

Usability Issues with Security of Electronic Mail

A thesis submitted in fulfilment of the requirements for the
degree of Doctor of Philosophy

by

Alexander John Anthony George

DeWitt

(0001921)

School of Information Systems and Computing
Brunel University

June 2007

Abstract

This thesis shows that human factors can have a large and direct impact on security, not only on the user's satisfaction, but also on the level of security achieved in practice. The usability issues identified are also extended to include mental models and perceptions as well as traditional user interface issues. These findings were accomplished through three studies using various methodologies to best suit their aims.

The research community have issued principles to better align security and usability, so it was first necessary to evaluate their effectiveness. The chosen method for achieving this was through a usability study of the most recent software specifically to use these principles. It was found that the goal of being simultaneously usable and secure was not entirely met, partially through problems identified with the software interface, but largely due to the user's perceptions and actions whilst using the software. This makes it particularly difficult to design usable and secure software without detailed knowledge of the users attitudes and perceptions, especially if we are not to blame the user for security errors as has occurred in the past.

Particular focus was given to e-mail security because it is an area in which there is a massive number of vectors for security threats, and in which it is technologically possible to negate most of these threats, yet this is not occurring. Interviews were used to gain in depth information from the user's point of view. Data was collected from individual e-mail users from the general public, and organisations. It was found that although the literature had identified various problems with the software and process of e-mail encryption, the majority of problems identified in the interviews stemmed once again from user's perceptions and attitudes. Use of encryption was virtually nil, although the desire to use encryption to protect privacy was strong.

Remembering secure passwords was recurrently found to be problematic, so in an effort to propose a specific method of increasing their usability an empirical experiment was used to examine the memorability of passwords. Specially constructed passwords were tested for their ability to improve memorability, and therefore usability. No statistical significance in the construction patterns was found, but a memory phenomenon whereby users tend to forget their password after a specific period of non-use was discovered.

The findings are discussed with reference to the fact that they all draw on a theme of responsibility to maintain good security, both from the perspective of the software developer and the end user. The term Personal Liability and General Use Evaluation (PLaGUE) is introduced to highlight the importance of considering these responsibilities and their effect on the use of security.

Publications

The following peer reviewed publications resulted from the work of this thesis:

DeWitt, A. and Kuljis, J., "Aligning Usability and Security: A Usability Study of Polaris," presented at the Symposium On Usable Privacy and Security, Pittsburgh, PA, USA, 2006 pp.

DeWitt, A. and Kuljis, J., "Is Usable Security an Oxymoron," in ACM interactions, vol. XIII, 2006, pp. 41-44.

DeWitt, A. and Kuljis, J., "Numeric Versus Alphabetic Passwords: An Empirical Memorability Study", IEEE Security & Privacy <In submission>

Contents

Abstract	i
Publications	ii
List of Tables	vi
List of Figures.....	vii
Acknowledgments	viii
1 Chapter 1: Introduction	1
1.1 Domain	1
1.2 Outline of Research Problem.....	2
1.3 Background and Previous Work.....	3
1.4 Aims and Objectives	4
1.5 Research Methods	5
1.6 Organisation of the Thesis.....	6
2 Chapter 2: Usability and Security	7
2.1 Introduction	7
2.2 History of Security	7
2.3 History of Usability	10
2.4 Aligning Security and Usability.....	12
2.5 Usable Security.....	13
2.5.1 Usability of Passwords.....	14
2.5.2 Transparency	17
2.5.3 User Education.....	19
2.5.4 Developmental Integration.....	21
2.5.5 Design Patterns	22
2.6 E-Mail Security	23
2.6.1 Public Key Infrastructures.....	24
2.6.2 The Importance of E-Mail Security	27
2.6.3 Problems with E-Mail Security.....	29
2.6.4 Getting a Digital ID.....	30

2.6.5	Interface Problems	30
2.6.6	Standards and Mental Models.....	31
2.6.7	Lack of Internationally Agreed Laws	32
2.6.8	Complexity of Managing PKI keys.....	35
2.7	Summary and Conclusions.....	37
2.7.1	Research Questions.....	38
3	Chapter 3: Evaluating the effectiveness of usable security principles	40
3.1	Introduction.....	40
3.2	Usability Study of Polaris: Experiment Setup.....	41
3.3	Participants.....	42
3.4	Procedure.....	43
3.5	Results	44
3.5.1	Usability Metrics.....	46
3.5.2	Users' Decision Making Responsibility.....	48
3.5.3	Users' Attitudes to Security	49
3.6	Discussion	51
4	Chapter 4: E-Mail Encryption: Adoption and Attitudes	53
4.1	Introduction.....	53
4.1	Individual E-mail Users.....	54
4.1.1	Pilot Survey.....	54
4.1.2	Main Survey.....	56
4.1.3	Summary	66
4.2	Organisational E-mail Users.....	66
4.2.1	Interviews With Users in Organisations	67
4.2.2	Results.....	68
4.2.3	Summary of Barriers to Adoption.....	79
4.3	Discussion	79
5	Chapter 5: The Dichotomy of Passwords	83
5.1	Introduction.....	83
5.2	Participants.....	83
5.3	Procedure.....	84
5.4	Results	86
5.5	Discussion	89
5.6	Summary	91

6	Chapter 6: Usable Security – A PLaGUE on Both Houses	93
6.1	Introduction	93
6.2	Research Findings	93
6.3	PLaGUE in Software Development	95
6.4	PLaGUE in User Interfaces	96
6.5	PLaGUE in Policy Development.....	97
6.6	Moving Forward With Usable Security	100
6.7	Summary	101
7	Chapter 7: Conclusions and Future Work	103
7.1	Introduction	103
7.2	Research Overview.....	103
7.3	Research Contributions	107
7.4	Future Research	108
	References.....	110
	Appendix A - Materials used in the usability study of Polaris (chapter 3).....	117
	Appendix B - Materials used for interviews in chapter 4.....	132
	Appendix C – Recent examples from the media on usability/security related issues	135

List of Tables

Table 3.1 Metrics used to measure the usability of Polaris in three categories	42
Table 3.2 Tasks as instructed in the usability study.....	44
Table 3.3 Summary statistics of participants who completed the usability tasks	45
Table 4.1 Survey questions relating to concepts from popular technology adoption models.....	58
Table 4.2 - Summary of results of e-mail encryption survey.....	62
Table 4.3 Perceived benefits of adopting e-mail encryption	62
Table 4.4 Reasons why respondents are not currently using e-mail encryption (self given reasons)	63
Table 4.5 Reasons why respondents are not currently using e-mail encryption (reasons selected from a list).....	63
Table 4.6 Reasons why respondents would not like to start using encryption	64
Table 4.7 Organisations interviewed on use of e-mail encryption	67
Table 5.1 Days on which participants were asked to log in with their password	86
Table 5.2 Successful recall of all passwords	87
Table 5.3 Successful recall of issued passwords (this includes all participants who had no option to change their passwords together with those who had but did not exercises this option).....	88
Table 5.4 Successful recall of self-chosen passwords (this includes only the participants who had an option to change their passwords and who exercised this option)	88
Table 6.1 Research findings of thesis	93

List of Figures

Figure 2.1 Example of a PKI hierarchy	26
Figure 2.2 Example of a PGP web of trust	26
Figure 4.1 A comprehensive adoption model (Gong and Yan, 2004)	59
Figure 4.2 The design model versus the user model, adapted from (Norman and Draper, 1986) ..	60
Figure 6.1 A Taxonomy of barriers to the adoption of e-mail encryption	99

Acknowledgments

Special thanks are due to my wife Claire, parents Sue and Alan, and all of my friends for their support and encouragement throughout the many hard times of my PhD. For my ability to survive the research office environment I owe a lot to Bobbi who offered relentless cheer and support.

Thanks to my first and second supervisors, Dr Jasna Kuljis and Dr Mark Perry, for their continual constructive feedback, and to Professor Ray Paul whose insight changed the way I view research.

The studies reported in this thesis would not have been possible without the invaluable data collected from volunteering organisations and individuals.

Thanks also to the researchers at HP labs, Palo Alto California, who allowed me to perform the first usability test on their Polaris software.

Chapter 1: Introduction

1.1 Domain

This thesis examines the usability issues surrounding computer security systems, with specific attention to electronic mail (e-mail). It identifies the extent to which the human factors aspect of security can influence the overall security of a system and discusses current trends and attitudes towards e-mail security. Current work in the emerging field of usable security is evaluated and new methods of lessening the security burden on end users is proposed.

In this thesis security is defined as the principle of ensuring the completion of a task without any unexpected or unauthorised access to, or modification of the data being used in that task. This definition fails to account for security breaches that occur outside the performance of a task, such as when an unattended computer is accessed by an opportune hacker. The focus of this thesis is on a task-oriented approach as it is assumed that security is an attribute of task completion rather than a task itself. Security exploits can include attacks on the network infrastructure in order to gain unauthorized access to the data streams, attacks on the operating system in order to compromise file security and passwords, and attacks on applications, including leveraging the Internet to use viruses, malicious software (malware), monitoring software (spyware), unsolicited e-mail (spam), and protocol attacks (e.g. HTTP compromises). These attacks are perpetrated to make either financial or social gain (e.g. the kudos gained amongst the 'cracker' community of breaking a large system).

Security for e-mails is vital in protecting the privacy of its users and their information from unauthorised viewing or alteration. E-mail was developed alongside the first wide area, packet switching network, ARPANET in the early 1970's. ARPANET evolved into the Internet of today and e-mail exploded into a fast and cheap source of global communication. According to a leading market research firm The Radicati Group (marketWire, 2006), the number of e-mail messages being exchanged daily in quarter 3 of 2006 was 183 billion, with 1.1 billion e-mail users worldwide. However, the same study by Radicati shows that only one third of these messages were legitimate, with the rest causing worry for security software developers and researchers. Spam e-mails can solicit business, promote obscene material, carry malicious code in the form of viruses and Trojans, or attempt to extract a user's valuable data such as passwords and personal information. Software houses have been responding to new virus threats as quickly as possible before too much damage can be done, but not always quickly enough. For example, the 'Blaster' and 'I Love You' viruses cost billions of dollars of damage by exploiting the massive user base of

Microsoft Outlook (Festa and Wilcox, 2000). The ‘Sobig’ virus and its variants are known as one of the fastest spreading and most financially damaging viruses in the history of computers, causing havoc between January and September 2004 before the patches to fix the problem became widely available (Foremski, 2006).

Digital signatures and message encryption are two technologies designed to counter some of the security threats mentioned above, and have been widely available since 1996. Digital signatures are comparable with hand written signatures that are used to prove you are who you claim to be. Encryption is a technique to scramble the data in a message such that it can only be decoded by its sender and its recipient.

1.2 Outline of Research Problem

Security is becoming increasingly necessary as widespread and high speed networks are used to connect more and more devices together. In this networked world, the cost of intercepting and modifying data is much cheaper than in the physical world, and the opportunities for doing so are far greater. This is why such a variety of security tools are available. However, recent literature has identified usability problems with security technologies that can have significant impact on the way the security is used. Users have been seen to avoid, bypass, or incorrectly use security mechanism, but it is not entirely clear why. The potential risks of doing so are apparently low in their priorities, until they themselves become the next victims of a security breach.

It is believed that a part of the problem is that users cannot properly use e-mail security, or indeed other security technologies. The field of research dealing with how humans interact with computers is known as Human Computer Interaction (HCI), in which much research is undertaken to improve the usability of software. The international standard ISO 9241-11 (1998) defines usability as comprising of the following three factors:

- Effectiveness - the ability of users to complete tasks using a system, and the quality of the output of those tasks
- Efficiency - the level of resources consumed in performing tasks
- Satisfaction - a user’s subjective reactions to using the system.

This definition of usability is used for the purpose of this thesis.

Typically, the design of security measures for computer systems has been technologically driven, rather than user driven: levels of security seen in the designers laboratory are very high, but in practice this is rarely achieved, with users finding it difficult to know when or how to implement good security (Dourish and Redmiles, 2002).

The aim of security is to make things hard to do (e.g. gaining unauthorised access to a system), whilst the goal of usability is to make things easy to do (e.g. writing a document). These apparently conflicting notions have contributed to the perceived difficulty of getting security and usability to work together in harmony. Many software developers as well as end users have come to assume that security software is inherently difficult to use, whilst they expect high levels of usability in other types of software.

Usable security is an emerging research field that attempts to reverse this undesirable trend. Its aim is to make software more secure simply by altering the way users interact with it; the aim is to make the natural way of using software the secure way.

To gain a better understanding of the problem, current progress in usable security research needs to be evaluated to gauge progress so far in solving some of the problems mentioned above. Exactly why security seems so difficult to correctly use needs to be identified and proposals put forward to remedy the situation. To facilitate the research it is necessary to focus on one of the many applications of security. E-mail seems the most fruitful choice as it has a massive user base, and is an area in which the security problems are rife, yet for largely unknown reasons users seem not to be using adequate protection.

1.3 Background and Previous Work

Johansson (2004) highlights the dichotomy between usability and security by noting that “the most secure system is one that is disconnected and locked in a safe”. In this extreme example, actual use of the system is sacrificed for total security. Previous attempts at combining security and usability have attempted to compromise these extremes, and have so far either sacrificed usability for improved security or vice versa.

Both Human Computer Interaction and Security have been extensively researched separately, but the newly emerging field of ‘HCI-SEC’ combines the two, and has seen a slow increase in popularity. The term HCI-SEC was popularised by Whitten, when she founded the HCI-SEC discussion group on Yahoo! Groups (Whitten 2000). HCI-SEC gained further attention in 2003 with a workshop titled ‘HCI and Security Systems’ at the ACM Computer Human Interaction Conference held at Fort Lauderdale, Florida, USA (http://sigchi.org/chi2003/cat_program.html). But research linking usability with security goes back further than that. One of the most well known studies in HCI-SEC was carried out by Whitten and Tygar in 1999 and showed how the poor interface of Pretty Good Privacy (PGP) encryption software impacted on users’ ability to properly use e-mail encryption.

Whitten and Tygar (1999) provided one way to measure the integration of usability into security software, by checking whether the people who are expected to use the software are:

- Reliably made aware of the security tasks they need to perform
- Able to figure out how to successfully perform those tasks
- Not making dangerous errors
- Sufficiently comfortable with the user interface

The researchers in HCI-SEC argue that security need not necessarily be poor in order to have good usability, but concedes that this opinion is dwarfed by the popular thought driven by many factors, perhaps primarily that security is a field of mathematics, which the average software user has neither the time nor the inclination to understand. Many software designers are of the opinion that improving security necessarily degrades usability, and vice-versa (Yee, 2002). Similarly, end users to have, since the first military uses of security, believed that being difficult to use was a part of being secure (Yee, 2002; Zurko and Simon, 1996). This problem is compounded by the fact that an expert will influence many software development teams either in usability, or in security, but rarely both. Furthermore, Whitten and Tygar (1999) suggest that even if this were the case there would still be problems because usability for security software is somehow different to that of other software, implying that a single expert in the joint field of usable security is necessary on the development team.

When the software leaves the development phase and enters the market, it often does not perform as securely as expected, perhaps because most users do not spend all their time thinking about security but rather, are concerned with accomplishing some useful task (Yee, 2002). There is also confusion over the level of security protection which is necessary for the task at hand (Dourish and Redmiles, 2002).

1.4 Aims and Objectives

The aim of this research is to investigate the extent to which the usability of security software can affect the level of e-mail security, perhaps leading to more general conclusions.

The objectives are as follows:

- To determine the place of this research within the published literature
- To evaluate efforts to align usability and security
- To investigate the security used in e-mail in more detail and discover its usage patterns and reasons for that behaviour

- Based on this investigation, to investigate the possibility of a taxonomy identifying the barriers to e-mail adoption, and if so to create one.
- To investigate if recommendations on how to better align usability and security for e-mail can be determined

1.5 Research Methods

A detailed literature review is conducted to understand the domain and support the work of the thesis, identifying any room for improvement in the knowledge. A cognitive walkthrough is also used to illustrate some of the difficulties with using e-mail security technologies.

In order to assess the impact of usability of security software a combination of qualitative and quantitative approaches is used in the thesis, with each methodology being chosen for its appropriateness to meet the aim of a particular chapter, and being discussed within the chapter itself. Such an approach, known as triangulation, allows grounding of the often vivid stories found in qualitative research with qualitative data, and is endorsed by (Dubé and Paré, 2003) and (Kaplan and Duchon, 1988). The approaches used are summarised below.

To evaluate the application of usability principles from current research to security software, a controlled usability study is performed. The ISO definition of usability given in section 1.2 is used to define metrics, comprising of both qualitative (e.g. interviews and observations to obtain user's opinion), and quantitative (e.g. number of errors, time to complete task) data. Usability studies are widely accepted within the HCI field, and have been shown to identify a high percentage of problems with a low number of participants.

To investigate the issues surrounding the adoption of e-mail encryption, a critical approach is used to form a social critique, and a case study is used to collect data. An initial quantitative survey gathers preliminary data to lead the main data collection, in which semi structured interviews were used to gather in depth qualitative information. Respondents are from two categories; individual e-mail users from the general public, and representatives of organisations. Semi structured interviews follow a series of discussion topics which gather the required data, whilst allowing the interviewee to lead the discussion into areas about which they have deeper knowledge or opinions. Within the public sector a large number of respondents from a varied group of demographics are used to represent the widest possible user base. Qualitative evidence was gathered on the need for, use of, and attitudes towards e-mail security, and analysed with a narrative approach, that is, building a story given by the respondents to understand its meaning. Each reason that has impacted on the adoption of e-mail security is identified and used to build a taxonomy. The

taxonomy is used to propose a set of guidelines aiming to improve the usability of e-mail security and thus increase the protection offered in practice.

The previous studies lead to the identification of a recurring problem in the use of passwords as a usable security authenticator. To investigate possible alleviations to this problem a quantitative approach is suitable. An uncontrolled longitudinal experiment is performed to gather data on the memorability of various passwords, after which statistical analysis is applied to accept or reject the findings.

1.6 Organisation of the Thesis

Using the literature, case studies and experiments, chapter 2 explores usability aspects of security software. Chapter 3 evaluates the usability of new security software, and demonstrates that it is not as easy to use as it perhaps could be. Chapter 4 narrows the focus to e-mail encryption; an area of security that has wide spread privacy implications. Interviews are used to examine the mental models of the public towards e-mail encryption, to determine its perceived necessity in society and to discover the extent to which it is currently employed. The business model view of e-mail encryption is also examined with interviews, and a taxonomy is formed to summarise the issues affecting e-mail encryption adoption. Chapter 5 addresses the difficulty of remembering secure passwords; an issue raised in the literature and in the interviews. An empirical study that investigates a possible solution to this problem is described. Chapter 6 discusses the research findings and finally, chapter 7 presents conclusions and future work.

Chapter 2: Usability and Security

2.1 Introduction

The research focus of this thesis is to examine the alignment of security and usability, with particular focus on e-mail security. The research related to security and usability is reviewed in order to organise the literature into a meaningful story, which can be used to identify similarities and disparities between research and gaps in the current knowledge. First, the history of security and usability are independently examined to give the reader a background of their application and importance. More recent work that merges the two fields together is then reviewed to highlight several issues which are important considerations for the studies of the thesis. The specific case of security for e-mail is then addressed in detail, highlighting problems with its current state of adoption. Finally, a summary is given to highlight the main points of interest relating to the problem at hand.

2.2 History of Security

In the context of this thesis, security is defined as the protection of data being used to complete a task, for example, protecting unauthorised access to a message you are trying to electronically send to a colleague. Such a desire to keep communications private is not unique to this era; perhaps the earliest example of a security tool to ensure secrecy of messages is the Caesar cipher. This simple encryption technique was used by its Roman emperor namesake around 80BC and worked by transposing letters in a message by a certain number (Suetonius, c.110). Each letter is replaced by the letter that is third after it in the alphabet, for example A is replaced by D. This offered rudimentary protection from the prying eyes of enemies. Over time, more advanced cryptographic systems were developed to increase the difficulty required to break the code and thus increase the secrecy of the message. In the 1460's, Florentine architect and mathematician Leon Battista Alberti described the first 'polyalphabetic cipher'; that is one in which a different Caesar cipher is used for each letter of the message (Singh, 1999). French diplomat Blaise de Vigenère developed this into a cipher. It used 26 different ciphers which were selected based on a keyword and was much more difficult to break than previous ciphers. This cipher was published in 'Traicté des chiffres' in 1586 and became widely used, known as the Vigenère cipher. More recently, encryption techniques have become extremely strong and have played vital roles in military campaigns. Perhaps the most famous such instance is the use of the Enigma machine during World War II. Patented in 1919 (Hinsley and Stripp 2001), Enigma was then revised and used extensively by the German military during World War II to communicate secret plans and information among troops dispersed around the world. Enigma worked on the same principles as

the Caesar cipher and other substitution ciphers that had gone before it, but was far more complex. The typewriter-like machine consisted of wheels which passed each letter through seven separate substitutions, allowing 17,576 different substitution alphabets. This presented a great challenge to the allied cryptographers attempting to break the code. However, Polish and French mathematicians made great progress by exploiting weaknesses in the encryption scheme such as the fact that a message key was repeated at the start of the transmission and that no letter was ever enciphered as itself. British mathematician Alan Turing eventually finished what the Polish had started and cracked the Enigma encryption scheme, allowing disclosure of German tactics, which helped to win the war.

As well as keeping messages secret it is also desirable to prevent them from being tampered with in transit, and to be able to prove the identity of the sender. For thousands of years, ink and wax seals have served both of these purposes. Wax seals have been used in the Far East since the invention of writing and later extensively throughout Europe and the rest of the world. Applied to envelopes, they are broken when the message is opened to prove it has not been read in transit. Applied directly to documents or to cords attached to the documents, they serve to identify the owner or issuer of a document and cannot be removed without breaking. These two features offered by seals are known as authentication and integrity; proving the identity of the sender, and ensuring that the message is not tampered with. The three factors mentioned so far (secrecy, authentication and integrity) combined with a fourth, non-repudiation; make the four pillars of modern cryptography. Non-repudiation describes the ability to prove a transaction has taken place; neither party can later deny that the transaction or communication has occurred. Throughout history, receipts have been used for this purpose. A receipt must bear a time stamp and some identifying information such as a signature. This protects both parties in a transaction or communication in that it is a record of what has taken place.

Today's cryptography is much the same as has been used throughout history, except the context for its use has changed. Secrecy is still very important for military operations, but encryption also has many uses in the public sector, such as protecting privacy and sensitive information during online transactions.

Today, perhaps the most ubiquitous of all authentication mechanisms is the password. The first timesharing multi-user operating system, Multics, in 1965, began the widespread use of passwords as an authentication device. Modern computer users must now remember dozens of passwords to gain access to web sites, computer systems, buildings and bank accounts. With so many passwords to remember, users of computer systems face increasing pressure to maintain good security practices. Although they have become widely accepted, passwords still have many flaws, most notably that due to the nature of human memory they are often forgotten. As such, there are

emerging new ways of authenticating yourself without having to remember a password. One such method is known as biometrics; authentication by recognising who people are rather than what they know. This idea has been in use since fingerprinting was used in ancient China, however technology advances in recent years have allowed computers to store and recognise fingerprints, the first digital use of which was adopted by the New York State Identification and Intelligence System in 1968 (Finn, 2005). As well as fingerprints, other biological features may also be used for identification, such as voices, facial features and more popularly, iris pattern recognition, which was first patented in 1989 (Leonard and Safir, 1989). Biometric technology is however, expensive and not entirely accurate, and as such has a long way to go to completely replace passwords.

As e-mail and the Internet have become more and more vital channels of communication for businesses and individuals alike, the sense of urgency to increase their security has risen sharply. As has been highlighted above, encrypting information has long been possible, but the Internet has introduced new threat models, mainly due to the fact that information in transit will stop at many insecure points before it reaches its destination. To combat these threats, symmetric encryption systems were developed, which require a single key that is used by the sender to encrypt and by the receiver to decrypt messages. However, sharing the secret key can be problematic as the Internet is insecure and using telephone is inconvenient. The only way to securely use symmetric keys is to communicate them offline, such as in a face-to-face meeting, which obviously is not possible when the sender and receiver are far apart. This inconvenience was overcome 1976 when Diffie and Hellman introduced their public key scheme (Diffie and Hellman, 1976). In this scheme there are two keys instead of one. One key is secret and need not be communicated, whilst the other is public and should be publicised. The use of the keys is interchangeable, so a message encrypted with one key can always be decrypted with the keys pair and vice versa. The public key system paved the way for Public Key Infrastructures (PKIs), which provide all of the four requirements for cryptography; secrecy, authentication, non-repudiation and integrity. PKI is discussed in detail in section 2.6.1.

All cryptography in use today is based on mathematical algorithms and as such has been developed by mathematicians. The average user of these cryptography products has little or no understanding of these algorithms and like users of most systems, has no need to understand them in order to use them. Because of the long history of development of security, consultation with usability experts has been rare and certain specialised terminology has become used in today's software. When the complex underlying workings of cryptography become apparent to the user it can dissuade them from using it. Their lack of understanding can also cause using the security to hinder and it slow down their work. To aid in software development models are often used to

clearly presenting complex ideas, however security models in themselves can be very complex and difficult for even experienced developers to understand and properly use. The well known ‘Bell-LaPadula’ model (1973) for example, only deals with secrecy and must be combined with other models for complete security. The 52 page ISO 15408 standard ‘Information technology Security techniques’ (ISO, 2005) is not comprehensive and gives a list of the security aspects it does not address. Shortcomings like these can cause a communication breakdown between the different stakeholders in the software development team. If the software is to be successful, significant amounts of time and expertise must be devoted to the analysis, design and implementation of security features in software.

The motivation to include security features in software is strong, as widespread and spectacular security breaches are becoming more and more common, many of which are well publicised in the media (see Appendix C). For example, US prosecutors allege that during 2001 and 2002 computer enthusiast Gary McKinnon committed "the biggest military computer hack of all time" by accessing classified information and causing disruption to Army, Navy and Air Force computer systems (Boyd, 2006). The Guardian newspaper described in 2005 how online credit card fraud and fake e-mail scams had risen dramatically, as hackers found the Internet an easier target than the newly introduced ‘chip & PIN’ system used in shops (Jones, 2005). In January 2006 fraudsters used fake e-mails from popular online auction site eBay to persuade sellers to send their goods, even though they had not received any payment (Stallwood, 2006). These cases represent the risks to every sector of society arising from poor security practices. However, security is about both keeping secrets, and exposing them; monitoring illegal communications can lead to the prevention of crimes such as drug trafficking, money laundering and even terrorist atrocities. This presents a good case for continued research into improving security practices.

2.3 History of Usability

Usability is a multi-disciplinary subject, comprising computer science, human factors and ergonomics (ISO 13407, 2005). The International Standards Organization defines usability as “The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use” (ISO, 1998). Within the context of this thesis, the term usability is used to represent the ease of use of computer systems, particularly security software. Usability is an important consideration for software design, because software that is difficult to use requires increased cognitive effort from the user and may result in user error, increased time to complete a task, frustration and disappointment. These factors will impact on the user’s productivity, as well as damage the reputation of the software house. In safety critical systems, good usability design can even mean the difference between life and death.

For example, during World War II, the military realised that complex cockpit designs were causing many air crashes, so they began to redesign them to better meet the pilots needs (Yank, 2002).

Usability, also known Human-Computer Interaction took a great leap in 1963 when Ivan Sutherland developed Sketchpad; the first example of direct manipulation; where a pointing device can grab objects on screen, move and resize them (Sutherland, 1963). This led to the common use of windows seen in today's operating systems. 1969 saw the first operation of the Arpanet, the world's first packet switching network. Born from research within the US department of defence, Arpanet was the predecessor to the Internet. Combined with the World Wide Web invented by Tim Berners-Lee in 1990, this sparked the massive growth of network communications. Instant electronic messaging, shared workspaces and cooperative working have increased the ease of getting work done immensely. In 1985 what was to become a highly respected journal, 'Human Computer Interaction' was launched to provide a platform to present the increasing number of academic research papers in the field of usability studies. In 1988 Boehm introduced a spiral model for software development (Boehm, 1988). This model introduced a highly iterative approach and could be applied to all types of software development. This pioneered the notion of integrating usability into the design of software from the very start, and continuing to re-assess the user's needs, making revisions where necessary. In the same year software giant Microsoft indicated that it was to take the issue of usability more seriously when it launched a usability group to improve the ease of use of their operating systems and document editors. This move was somewhat behind competitor Apple who had an active usability program since the early 1980s. Usability author Don Norman wrote about the bad designs of everything from light switches to computer systems and how they can be improved, in his books *The Psychology of Everyday Things* (1988), and later *Things that make us smart* (1988), showing the widespread reach and impact usability studies can have. In 1991 Apple showcased its new multimedia software QuickTime, which broke new ground in playing video and audio on computers, bringing the personal computer closer to the sensory abilities of humans.

It is now widely recognised that usability is a vital ingredient of any software product. Because processing power is rapidly increasing, whilst the cost of technology is decreasing, it is now commonplace to find extremely complex and powerful software systems such as computer-aided design, video editing and cryptography systems widely available, in a market where a substantial number of computer users are still very naïve. To address this mismatch there are many usability experts who publish design principles such as 'Designing Web Usability' by Jakob Nielsen (1999), and many experiments take place to assess the usability of products before release. However, despite the seemingly huge weight designers now give to usability, there are still many

instances of failure attributed to poor usability. For example, many automated air traffic control systems have failed because the computerised system cannot meet the usability standards that operators grew accustomed to when using the slips of paper in the previous system (Mackay, 2000). A further example is that in 1988 a US Navy ship launched missiles at what its computer systems identified as an enemy threat (Hogland and McGraw, 2004). It was actually a commercial flight on which 290 passengers were killed. The Navy blamed misleading output from its tracking software. It is not clear in this case whether the failure is attributable solely to poor usability, or inadequate quality testing, or both combined. Perhaps, as proposed by Gray and Salzman (1998), usability evaluation methods are inappropriate, leading to reduced findings of faults. In their review of usability testing methods, Gray and Salzman highlighted that previous papers, which recommended particular methods for usability evaluation, did not have a strong enough grounds to do so. Of particular weakness throughout the five influential papers that were reviewed, were the lack of statistical methods used to compare usability evaluation methods, failure to control for random events, problems with the setting, equipment and selection of participants for usability tests and the tendency of the authors to go beyond the observed results in their conclusions. It may then be the case that since recommendations on usability evaluation methods are flawed, that the outcome of usability evaluations themselves are also flawed, leaving usability problems in systems remaining undiscovered.

2.4 *Aligning Security and Usability*

Here the notion of usable security is introduced and its validity demonstrated. Previous research up to this point is presented, grouped by the following major issues: Passwords, transparency, user education, design patterns and developmental integration.

People use computers to accomplish some objective, whether that is to send a message to someone, to write a report, or to immerse him or herself in a 3D game. Anything that inhibits the attainment of this objective can cause negative perceptions on the user such as frustration, wasted time, or dissatisfaction. Security software often does exactly this because it requires extra time and effort to set up, monitor, update and use. Because protecting the security of a computer is not always a user's main objective, in many cases the user will prefer to bypass the security software, even if this means compromising the security of their computer. Security is like a seatbelt in the software car; provided by the manufacturer for your safety, but no car is ever bought for this feature alone.

In software design, the security of a software package typically receives less attention during than its functionality, perhaps largely because the ultimate aim of software houses is to make profit. This is traditionally accomplished by continually releasing updated versions of the software for

subscription or purchase. A limited budget will often be devoted to functionality, which users are seen to take more notice of, than security or usability. Software houses know that spending too much time on any aspect can lead to untimely release that misses the peak of consumer demand.

Insecure software is often breached deliberately to malicious ends, but recent research is showing that many security breaches are also caused inadvertently by legitimate users, who are commonly willing to take 'unsafe' shortcuts to get work done faster, or because they do not understand the security software (Besnard and Arief, 2004). If the usability of security is leading to lower levels of security in practice, improving the usability should therefore cause the system as a whole to become more secure as well as more pleasant to use because there will be less instances of security being de-activated, bypassed, or misunderstood. Sasse strengthens this argument with her 'users are not the enemy approach' which advocates better software design to culture of blaming users for security breaches even though the users are unable to fulfil the huge burden of security control placed on them by designers (Sasse, *et al.*, 2001).

Some research has argued that the goal of perfect security is set too high and may not be achievable without sacrificing usability. Rather than perfect security then, much of the research community has recommended 'good enough' security, which although not guaranteed to prevent any attack, will sufficiently protect the average computer user against most attacks (Gutmann, 2005; Saltzer, 1974; Sandhu, 2003; Sasse, *et al.*, 2001). Furthermore, due its higher levels of usability, it is argued that this type of software will provide far greater levels of security in practice than a technically more secure system with low usability.

2.5 Usable Security

As security is such a complex domain, it has been believed by developers and users that it is therefore necessarily difficult to use. Popular belief and media have fuelled this view that usability and security are antagonists for years. Even the respected usability expert Jakob Nielsen has stated that security considerations often *require* violating usability principles (Nielsen, 1993). This has led users to believe that being difficult to use is a part of being secure, and has cultivated a culture where usability for security is tolerably lagging behind whilst usability for other aspects of computing has been persistently campaigned for.

The first mention of security and usability having to work hand in hand is generally accepted to be in the 1975 paper "The protection of Information in Computer systems" (Saltzer and Schroeder, 1975). The authors proposed eight principles to guide the design of security products, the last of which was 'Psychological acceptability', which described the interface design to be essential. If the 'psychological acceptability' or usability of security products can be improved, it will encourage users to routinely use the security mechanisms in the correct way. However it wasn't

until 1996 that interest in usable security started to grow more rapidly, with Zurko and Simons' 'User centred security' paper (1996), which discusses usability as being the primary goal of security. In 1999 Whitten and Tygar's' paper 'Why Johnny Can't encrypt' (1999) described a study which showed that most users were unable to encrypt e-mails with PGP software, which was considered to be very usable at the time. This remains one of the most cited works in usable security. Whitten went on to set up the popular 'HCI-SEC' Yahoo group in 2000, which facilitates online discussion of usable security issues. HCI-SEC has since become an accepted and popular term to describe the research field of aligning usability and security.

Work from the HCI-SEC field has brought particular focus to the following subtopics:

- Usability of passwords – Passwords being the most widely used authentication mechanism has led to them receiving much analysis
- Transparency – the extent to which the user is aware of the software, and therefore the extent to which the software can impact on the user's tasks
- User education – there has been some disagreement over the effectiveness of simply instructing users on how best to use a system, and the proportion of blame which should be attributed to the users when these instructions are not properly followed
- Developmental integration – whether usability or security are considered during a software lifecycle, in what proportions, and at what times can impact their effectiveness
- Design Patterns – there have been some suggestions creating procedures which should lead to systems being both usable and secure

Each of these sub topics is discussed in turn below:

2.5.1 Usability of Passwords

Passwords are one of the most ubiquitous security mechanisms and as such there has been much literature about them, most of which has focused on the problems users have with remembering them. For a password to be secure it must to be complex (long, with a mixture of upper and lower case letters, numbers and symbols). Humans find it difficult to remember complex passwords so they often choose easier to remember alternatives which are very insecure (Adams and Sasse, 1999; Weirich and Sasse, 2001; Zurko and Simon, 1996). Henry Roediger, the chair of the psychology department at Washington University in St. Louis said "We are told to make them [passwords] meaningless and hard to guess, but that also means that they are hard to memorize" (Hébert, 2001).

Calum McLeod, senior consultant for security software producer Cyber-Ark, highlights some of the potential risks associated with passwords: “Administrator passwords are required for emergency and disaster recovery scenarios...[and] frequently need to be shared, [so] there is increased risk that they are just left lying around” (2005). A good password management policy and increased usability may reduce the cases of passwords being written down or shared, which create security risks.

Forgetting a password effectively causes the system to break down as we no longer have access to it. Ironically, this is not caused by some security problem, but to the supposed protection against security threats. Tactics used to avoid forgetting a password include choosing a meaningful word, or the same password for all systems/purposes. This makes the password easier to remember but decreases the level of protection against attacks and thus defeats the very purpose of the password. Alternatively, many people make a note of the password for future reference, often keeping it stuck to their computer monitor; the most easily accessible place for a potential attacker. To paraphrase renowned usability author Norman, without external aids the human memory is constrained (Norman, 1988 pp. 43).

In recent years the need to address the human factors aspect of security mechanisms with equal vigour as the technical aspect has received growing recognition for its potential to overcome downfalls such as those described above. Recent research such as (Brostoff and Sasse, 2000; Jermyn, *et al.*, 1999) has proposed the use of graphical passwords instead of text to facilitate easier learnability. Another study proposed taking advantage of human memory phenomena to enable users to easily remember their password (Weinshall and Kirkpatrick, 2004).

Sasse *et al.* (2001) identified that the majority of users have problems in remembering their passwords and reported that it is important to give users good motivation to choose an appropriate password. They also acknowledged that it is extremely difficult to create passwords which are easy to remember yet hard to break, but did not offer any specific advice on how to improve this situation.

Of interest when studying how to improve passwords is the type of information which is most likely to be remembered and the trigger for recalling the information. Tulving (1974) in (Eysenck and Keane, 1990) pointed out that the forgetting of information is sometimes due to the lack of a relevant cue. For example, in the context of computer security, a person might not be able to recall their password for a particular system until the login screen for that system is shown to them. Furthermore, a study by Godden and Baddeley (1975) in (Eysenck and Keane, 1990) has shown that the context a person is in can affect their ability to recall information. In their study [3] participants learned a list of words either on land or underwater and then had to recall the words from the list either on land or underwater. The retention of information was approximately 50%

higher when the learning and recall took place in the same contextual environment (those who learned on land recalled more on land).

In an article for the American Psychological Society's Observer magazine, Sternberg states the difficulty humans face in processing "strings of symbols from alternating categories" (Hébert, 2001), suggesting that it is easier to remember a string consisting either solely of numbers or of letters, rather than a mixture of both. Baddeley, *et al* (1962) carried out a post code memorability test with 42 postmen and found that the postal code type with the best recall was the code consisting of three letters followed by three digits (80% successful recall rate). This seems to suggest that in the case of postal codes at least, the two halves of the code are treated independently which may explain why a mixture of categories performed better in this experiment, contrary to the research by Sternberg (Hébert, 2001). When the choice was between a code consisting of either all letters or all digits, digits performed better, because similar sounding letters were confused with each other. Presumably though, passwords unlike post codes are treated as a single string / entity rather than being broken into parts for retention.

The study by Baddeley *at al* (1962) used an immediate recall; six characters were displayed to the participant one at a time, with 0.75 seconds per character to remember it and after all characters were displayed the participants had to write the entire sequence of characters as best they could remember it. This is clearly a different context to that of remembering a password, where usually the complete password is displayed at once and the user has as long as they need for memorising it. Furthermore, the study employed a limited vocabulary, using only the letters A-E and the digits 1-5, so further study is required to test the remaining vocabulary.

There are very few studies specifically researching the memorability of computer passwords. In December 2006, Schneier was fortunate enough to have access to data from a Phishing attack on popular website MySpace.com which allowed him to perform the analysis of 34,000 captured usernames and self-chosen passwords for use in a real system (Schneier, 2006). The analysis revealed that only 1.3 % users chose a numeric-only password and only 9.6% chose a password consisting only of letters, indicating a slight preference to the all-alphabetic passwords over the numeric ones. However, the majority of passwords (81%) chose a mix of letters and numbers, but 26% of these were lowercase letters followed by a single digit, usually 1 (presumably the user believed this tactic would make the password more secure). The words used were usually names such as the name of a band or a person.

Similarly, Grampp and Morris (1984) found that when asked to create a password consisting of at least six characters, where at least one should not have been a letter, many participants chose their name followed by a number, presumably because the participants found their name easier to remember than a random string. The problem with such passwords is that they are very easily

guessed by dictionary style attacks. It would be desirable to find a password which is not a dictionary word, but is somewhat easier to remember than a randomly constructed sequence of characters, however no such solution has yet been found.

The study perhaps most relevant to this problem was performed by Zviran and Haga (1993) who tested 106 students on their ability to remember one assigned random password and one self-chosen password after three months. Successful recall of self-chosen passwords was managed by 35% of the students, whilst only 23% recalled the assigned random password, and 66% of these recalls were with the aid of a written note. Although this experiment provides a frame of reference for the memorability of passwords, it does not accurately reflect reality because the students did not use their passwords during the three-month period, nor was the construction of the passwords analysed for their effect on memorability.

Some systems force adherence to strict and seemingly arbitrary rules when creating a password, and this compounds with the fact that modern users are expected to memorise dozens of passwords for various systems, making recall even more difficult. Sasse et al (2001) confirmed that most login failures were attributable to users confusing two different passwords and recalling the wrong one, or correctly recalling a part but not all of a password. PINs were found to be more frequently confused with each other than passwords which would seem to suggest that recall of alphabetic passwords is more accurate in cases where users already have many numeric passwords. The study by Sasse et al (2001) did not address a representative cross section of users, focusing solely on managerial employees of British Telecom. Furthermore, the context of use on which the above findings were based is solely the PINs for a telephone voice-mail system.

The widely held belief that randomly selected passwords are more secure than passwords based on mnemonic phrases, was disproved by an empirical study on password memorability by Yan et al. (2005). In this study random passwords were found to be significantly more difficult for the users to remember than those based on a mnemonic phrase, but were no more difficult to break. Yan et al. also found that users who had received advice on using mnemonic phrases chose passwords that were five times less likely to be guessed using simple dictionary style attacks than when no advice was given. In their experiments, user compliance and password policies were deemed to be crucial. Without good advice approximately 65% of users chose a sufficiently strong password, whilst with good advice, but not enforcement, this figure increased to 90%.

2.5.2 Transparency

Transparency is a usability concept that describes hiding complexity from users. Transparent aspects of software can be helpful to users with low computer skills who may get confused by excessive details. In the HCI-SEC field, there has been some disagreement over the level of

transparency that will induce better security habits from ordinary users. Several authors have proposed that the notion of making security as transparent as possible will not necessarily improve usability (de Paula, *et al.*, 2005; Dourish, *et al.*, 2003; Dourish and Redmiles, 2002). It is argued by these authors that software cannot make adequate security decisions on the users behalf and that if the user is to be empowered enough to make good security decisions they need to be presented with all the necessary information in a clear way. In this case it is advocated that security be visualised to the user and thus become apparent rather than transparent. Both Whitten and Tygar (2003) and Dourish et al (2004) emphasise user understanding and control, and appreciate that security systems are supplementary to the user's main task. Dourish and Redmiles (2002) suggest user understanding and control may be improved through the use of an event notification system; whenever an event (such as a security breach) occurs which will affect the users task, it can be brought to their attention through the use of notifications. Dourish (2002) suggests using event monitoring combined with visualisation to achieve this, although notifications may also be made through auditory or haptic feedback. McCrickard and Chewar (2003) also believe that higher understanding can be given to the user through notifications or 'alerts' and state that "the success of a notification system hinges on accurately supporting attention allocation between tasks, while simultaneously enabling utility through access to additional information". This statement describes a trade off between distracting the user unduly from their primary task and failing to alert them to an event which is urgent enough to warrant an immediate response. It is widely recognised within the Human Computer Interaction and Security (HCI-SEC) community that users grow accustomed to such alert messages and learn to quickly dismiss them without reading them (Gutmann, 2005).

Security software needs to be effective with minimal action from the user, however like all other types of software it should also provide feedback about what is actually being done to protect them and allow customisation of the settings. The problem is that users do not always know how to use customisation. For example, in Microsoft Internet Explorer 6, users can enter the options dialogue, where they are presented with a security tab offering them to choose between high, medium, medium-low or low security, but most users do not know what precise effect this will have on the security settings, let alone on their actual task at hand. The user is unlikely to set security so high that they are prevented from completing their primary task.

Sasse (2005) describes a paradigm of 'one-click security', meaning that the user should be able to set up their security settings with one mouse click. This complies with the guideline that security mechanisms will only be used if they are easy to use. Jon Callas, CTO and CSO of PGP Corporation, goes one step further in saying that the philosophy behind their new PGP universal product is 'zero-click encryption' (Callas, 2004). This makes the interesting point that sometimes

the best user interface is no interface at all. Callas describes this as allowing people with ‘average jobs’ to get on with their work without having to worry about setting up security, stressing ‘transparency is key’.

Although the benefits of a completely transparent security system are clear, there are also some reservations about its consequences. Providing completely transparent, automatic security implies automatic a prescriptive approach; removing the user’s ability to choose how to behave. Although if given a free choice of how to behave, it is questionable whether a user will choose to behave securely, or whether they know what is best for them, usability should be a means of assisting users to behave securely rather than forcing pre-determined behaviour. Automation may work for some scenarios (e.g. securing communication channels) but not others (e.g. setting access control policies such as when a user wants to share some files but not others) Whitten and Tygar (1999).

Gerd and Markotten (2002) state that maintaining high security is not the users primary goal, so security information will cause interruptions to their work flow, leading to frustration. They recommend security be hidden from the user so that the user need not make as many interactions with the security software. Jøsang and Sanderud (2003) propose offering the user as much information as they can handle in order that they are better informed to detect breaches in security, although they do not discuss how the amount of information the user can handle can be established. Straub and Baier propose a compromise whereby maximum transparency at first gradually allows users to take more and more control as they become more accustomed to the software (Straub and Baier, 2004).

2.5.3 User Education

Since security software is often based on complex algorithms and concepts, it is rarely of interest to the ordinary user. Consequently, users’ understanding of possible threats, risks and good security practices is often lacking.

In many cases, this lack of understanding has been used to pin the blame on the user for security failures. Researchers such as Sasse at al. (2001) have challenged this ‘blame the user’ mentality, asserting that user error is inevitable when the user is unfairly asked to adapt to the needs of the computer. Norman points out the difference in skills between humans and machines (Norman, 1988); people are good at improvising, creating, and using their senses, yet the computer asks for precise, accurate information and requires the same task to be repeated many times. To use the password example; complex passwords are difficult to remember, yet users are insisted to do so if they want good security. The limitations of humans are well known, yet people are still blamed for system failures. Adams and Sasse (1999) argue that improper, or absent use of security software is the fault of the software designer, not the users.

For these reasons there is often thought to be a need to educate the user to allow them to better understand their roles and responsibilities within the system. Schneier (2000;2003) argues that user education is key for good security decisions to be made and that the users must be taught how to make the right choices. The U.S. Department of Homeland Security recommends user education to prevent users from falling for Phishing attacks (see section 2.6.2) by enabling them to recognise tell-tale signs of such attacks (Emigh, 2005). Yan et al found that good education can help users to make better choices when creating passwords, leading to higher password security (2005). Adams and Sasse advocate user training to help users “do the right thing” (1999). Whitten and Tygar developed an approach known as safe staging to break down complex notions into easily digestible steps for novice users and provide continued support when it is needed (2003). In a similar vein, Dourish and Redmiles hypothesised that using visualization to keep users informed of security information can lead to users making more effective security decisions (2002), a hypothesis that seemed to be true under further investigation (Dourish, et al., 2003;Dourish, et al., 2004).

However not all research suggests that education alone will eradicate ‘human error’. Weirich & Sasse (2001) showed that education and training is not effective unless the users believe they are at risk. Sasse et al. confirmed this with studies that showed education is not effective in large organisations, but can and should be used along with motivation techniques to improve the security of the organisation as a whole (Sasse, et al., 2001). Sasse later strengthened this position by advocating that education be used in a cultural and social context, and in combination with other techniques such as improving the user interface (2003). Gutmann argues however, that user education is a waste of time, stating that “Computer security is simply too complicated, and the motivation for most users to learn its intricacies too low” for it to be a useful way of improving security practices (Gutmann, 2005).

Despite this, many new security features in software require the user to be trained to notice the presence of security indicators, or worse, to notice the absence of usually present indicators. Noticing that something is missing is more difficult for a user because they grow accustomed to seeing the indicator and eventually learn to ignore it. Studies such as (Schechter, *et al.*, 2007) have shown that authentication measures which require users to notice an indicator are ineffective (users continue about their task even though there is a security risk), seeming to support Gutmann’s stance that education and training are ineffective and that the problem lies in the complexity of the security itself.

2.5.4 Developmental Integration

The well known usability author, Nielson, has discussed in his 'Usability Engineering' book the importance of integrating usability before and during the software development cycle, stating that knowing the user's requirements is key (Nielson, 1993). Faulkner, in her later book sharing the same title (2000) goes on to stress the importance of usability engineering, and suggests that the usability specialists themselves should program the application, to avoid the misunderstandings that can occur when requirements are communicated from person to person. Mayhew (1999) describes the usability engineering model in detail, focussing on understanding the users, tasks and environment before implementation, and using iterative development to continually re-assess the usability goals throughout the process.

This type of iterative design is also used to improve the quality of security software. Kis (2002) states that security must be integrated into software from the outset, otherwise it will be ineffective. Kis suggests that software developers misconceive security to be a 'plug-in' to be dealt with after release. Yee (2004) also states that security cannot be added onto a system at any time, rather it must be integrated into the product from the start. Developers' views of security as a plug-in can be part owed to the perseverance of old security models, such as the perimeter protection model. This model describes protecting only the external link between a company's mainframe and the network, and came into use before the Internet, when the lack of global inter-networks and de-centralized computing made it a much more suitable model to employ than it is today. In today's networks the threats lie not only outside the company firewall, but within it as well. Perhaps if the perimeter protection model were updated to meet this environments needs, developers could better understand the necessity to develop security with equal importance to functionality. Halkidis et al. (2004) show that when security is not kept in mind throughout the development process, this in most cases leads to security holes which can be exploited by attackers. Anderson states that requirements engineering is the most critical task of secure system development (Anderson, 2001, p.503). Mouratidis et al. (2003) propose a process which integrates security and systems engineering throughout the entire development phase, guiding developers through the process. It is stated that this approach will reduce the number of security vulnerabilities in the finished product.

So it seems that previous research has reached a consensus with regards to the need to incorporate security and usability design throughout the development process, testing and evaluating against objectives to ensure that the product meets expectations throughout (Balfanz, *et al.*, 2004; Flechais, *et al.*, 2003). As demonstrated in chapter 3, the Polaris software designed to combine usability and security has highlighted the difficulties in doing so using a retrofit onto a pre-existing system where this iterative, integrated approach is not possible.

2.5.5 Design Patterns

Patterns have been used to apply solutions to recurring design challenges in software engineering and later were also applied to usability problems. Although concerns have been raised as to whether large sets of patterns will be comprehensible, shareable, or effective (Borchers and Thomas, 2001), patterns remain able to abstract the complex requirements of HCI problems and can effectively convey possible solutions to designers (Borchers and Thomas, 2001).

Since the innovative work of Yoder and Barcalow (1997), patterns have also been used as a way to apply known solutions to security holes in software. An example of a pattern used specifically for cryptographic software is the work done by Braga et al. (1999), which defines patterns to enforce the four pillars of security; secrecy, authentication, integrity and non-repudiation. The authors claim that using their pattern allows the user's needs to be addressed and allows cryptographic elements of software to be separated from functional elements. Thus it would seem that if these patterns were applied correctly, the task of developing the software could be correctly split between the two goals; security and usability. However, Kis (2002) warns that patterns allow developers with little or no knowledge of either security or usability to apply solutions in these areas, which may lead to inadequacies in both domains. More recently, Halkidis et al. (2004) made a qualitative evaluation of patterns for improving software security and found that no single pattern can provide perfect security, rather, patterns must be combined to leverage the features that each pattern offers.

Garfinkel's Thesis (2005) strongly advocates the use of patterns to align usability and security and presents a set of patterns that can be applied to make 'relatively minor' changes in the development process, resulting in dramatic increases in the alignment of usability and security. For example, the 'Key Continuity Management' pattern describes allowing digital certificates that are self-signed or signed by an unknown Certificate Authority to be used in a way that proves continuity of identity: When a digitally signed e-mail is received and the certificates are not signed by a recognized CA, the system verifies the signature, then consults a local database of identities. If the identity is not present, the identity and the certificate are added. If the identity is present and the certificate on file for that identity is different, a warning is issued. When an identity is received that is not digitally certified and the identity is on file with a matching certificate, a warning is issued. Sets of patterns such as this may help make e-mail encryption easier to use in the future.

HCI-SEC research has described the continual game of catch up that is played between virus writers and anti-virus software and suggested that although this provides a good profit model for anti virus vendors (as users subscribe to continual updates), it is not the most efficient or usable

method of combating the virus problem. To this end Yee (2002,2004) proposed ten HCI design patterns that can be used to improve the usability of security systems. The CapDesk software was created by applying eight of these patterns, with specific focus on The Principle of Least Authority (POLA). POLA aims to grant software only the minimum of permissions it needs to run to prevent unauthorised file access. A close cousin of CapDesk, Polaris, was later created as a retrofit onto Microsoft Windows, as a way to combine legacy, security, usability and functionality. As Polaris is a retrofit onto Windows, it was not able to take advantage of the developmental integration principle described above, so its design was limited to comply with the specifications of Windows, restricting the extent to which usability and security could be combined. A usability study carried out on Polaris is discussed in chapter 3.

2.6 E-Mail Security

Electronic mail or e-mail uses packet switching protocols to send messages from any Internet connected machine in the world to any other. E-mail is vulnerable to attack because the chunks of the message, or packets, make many stops at various servers along their journey. At each stop the message is in 'plain text' meaning it can easily be intercepted, viewed and altered, perhaps without the sender or receiver ever finding out.

Over the last decade the number of electronic messages being sent over the Internet has massively increased, so e-mail security has been seen as increasingly important. Common with other forms of security, e-mail security also revolves around four central tenets; secrecy, integrity, authentication and non-repudiation.

If information sent using e-mail is deemed to be secret, then only the sender and receiver should be able to understand the message. The secret information could be anything deemed by the sender to be sensitive, for example, personal communications with friends and family, bank account details or research findings. Apart from secrecy, it is also necessary to protect e-mail messages from being altered in transit without the sender or receiver noticing. Rather than preventing such changes to the message content, which can be difficult, e-mail security technologies usually alert the sender and receiver to these changes occurring. Checking alterations to the message in this way is known as its integrity and is important in the fight against fraud, where details can be changed to subscribe to services under a false identity. Another important aspect of e-mail security is that of proving the identity of the message sender, known as authentication. E-mail messages have message headers which show where the message originated, however many users do not realise that these headers can be falsified to so that the real sender of the message is altered. This can lead to trust being unduly placed in the message contents, whereby the receiver may be give away sensitive information without being aware of the senders'

true identity. Non-repudiation gives unequivocal accountability for messages sent and received, which is more important where messages must be legally accountable. Public Key Cryptography (PKI) has provided a means to enforce these four factors.

To uncover the usage patterns behind e-mail encryption, in 2004 Garfinkel conducted a survey of 469 Amazon.com merchants to ascertain their e-mail security capabilities and attitudes (Garfinkel, 2005 pp. 170-181). This was the first survey to address these issues since the less detailed 10th GVV WWW User Survey in 1999 (GVV, 1999). Garfinkel's results showed that most of the respondents were technically capable of sending and receiving encrypted and digitally signed messages, but most people thought that they had never received an encrypted or signed message. Some people claimed to have received a digitally signed e-mail from Amazon in the US, even though Amazon has never sent digitally signed messages to its US merchants. Conversely, some European respondents claimed never to have received a digitally signed message from Amazon, even though Amazon does send digitally signed messages to its European merchants. This portrays a deep confusion over e-mail security amongst users, the cause of which was not identified in Garfinkel's survey. Garfinkel pointed out that further research is required to assess the need, use and acceptance of e-mail security, and reasons behind this deep confusion.

The adoption of e-mail encryption, particularly PKI which will be discussed in the next section, has been reported to be far below expectations from its release in the 1990's. The reasons for this are largely undefined, but are thought to be due to the complexity of the technology, and the evidence is largely anecdotal e.g. (Garfinkel, 2005, p.202; Gutmann, 2002; OUT-LAW, 2006).

2.6.1 Public Key Infrastructures

Public Key Infrastructure is the infrastructure that allows for authentication and encryption of data over the Internet. PKI became seen as a very viable option after Diffie and Hellman introduced their ground breaking protocol for exchanging secret keys over the Internet in 1976 (Diffie and Hellman, 1976). However, even decades after the introduction of these cryptography techniques, for a variety of reasons they still remain underused. The evidence for this is mostly anecdotal, such as the messages posted on the usable security Yahoo group (Whitten 2000).

In PKI, each user is allocated a unique private key which must remain secret to them, and a unique public key which should be disclosed and published. The public and private keys encrypt data into an unreadable format and operate in such a way that the order in which they are used is unimportant (the public key can decrypt what the private key has encrypted and vice versa). To provide secrecy, the sender of the message can encrypt it using the recipient's public key, which can be looked up in a directory. The recipient and only the recipient can then decrypt the message into a readable format using their own private key. To provide authentication and integrity for

messages, a digital signature can be used. A digital signature requires that a short digest of the message called a 'hash' is created. Every message produces a unique hash and it is impossible to reconstitute a hash back into the original message. This hash is then signed with the sender's private key (thus encrypting it), and sent along with the original plain text message. This attachment is known as a digital certificate. The receiver can apply the sender's public key to the hash to decrypt it, then make their own hash of the plain text message they received. If the two hashes are identical it proves firstly that the sender is who they say they are, or their public key would not have decrypted the hash, and secondly that the message has not been altered in transit, or the hash would be different. Popular methods of encrypting data include Elgamal (named for its inventor, Taher Elgamal), RSA (named for its inventors, Ron Rivest, Adi Shamir and Leonard Adleman), Diffie-Hellman (also named for its inventors) and the Digital Signature Algorithm (DSA) invented by David Kravitz.

Within a PKI, one can use one of several systems for exchanging secure messages. The three most popular are Privacy Enhanced Mail (PEM), Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME).

PEM was developed by the Internet Activities Board's Privacy Task Force in 1987. PEM was revised twice, the latter and final revision being in 1993. PEM describes a way of digitally signing, or signing and encrypting an e-mail message, using public key cryptography and the RSA encryption algorithm. Today the PEM standard is largely not used due to its complexity and lack of commercial support.

PGP is another message encryption scheme released in 1991. PGP had the advantage of being open source and therefore free to use and develop. Once again, PGP did not gain wide spread or long lasting acceptance, due to not interoperating with popular mail clients. In 1997 PGP was released as a new commercial version which included plugins which allowed it to be used with popular mail clients. PGP message formats were eventually standardized by RFCs 1991, 2015 and 2440; however PGP never really picked up in popularity.

S/MIME was adopted by Microsoft in 1996, even before it was standardised in 1998 in RFC2311. Netscape responded by adding support for S/MIME into its Communicator and e-mail client. S/MIME is similar in implementation to PEM, except it integrates closely with the MIME e-mail standards. Today S/MIME is widely supported.

These systems all comply with a standard known as 'x.509'. This standard describes the hierarchical structure of PKI. In this hierarchy, digital certificates are issued by a Certification Authority (CA), which is a globally trusted entity which assures recipients of e-mail that the sender's identity is valid.

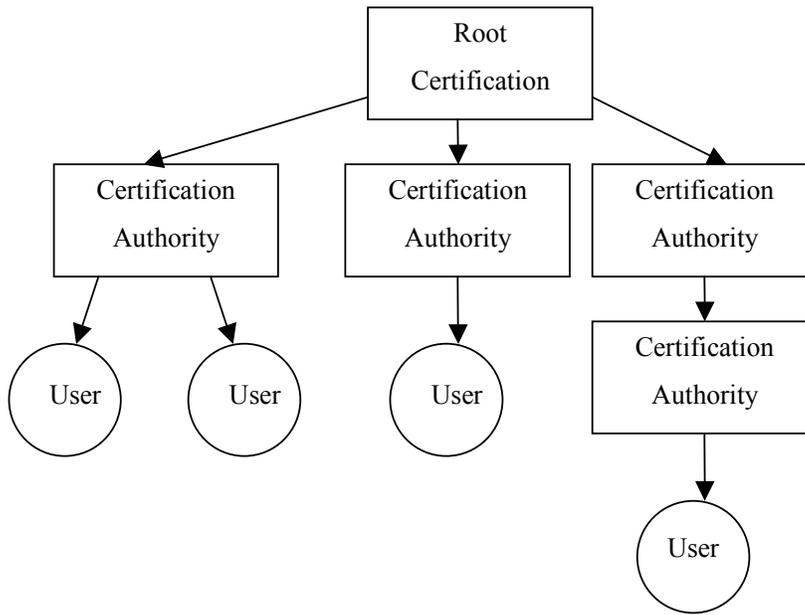


Figure 2.1 Example of a PKI hierarchy

In the hierarchy of a PGP system a CA is not necessary (although one can be used if desired). Instead, most PGP users operate in what is called a ‘web of trust’. In this model, any user can use their private key to sign the digital certificate of another user who they know personally. This is a way of declaring their certificate to be trustworthy without the need for a hierarchy with a CA at the top. Variations of PGP include GnuPG and OpenPGP which have met with approval from the public sector, although they are not used as widely as would be hoped to protect public privacy in online transactions.

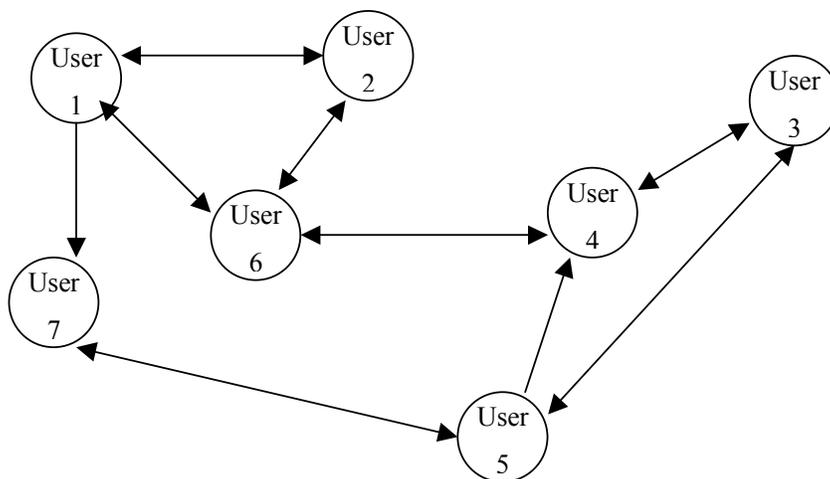


Figure 2.2 Example of a PGP web of trust

Nor has any implementation of PKI yet seen full integration into e-mail culture, despite the benefits it could bring to online commerce. Ellison and Schneier controversially argue that PKI is

not required for e-commerce to be successful, and that the propagation of PKI is merely a money-making exercise (Ellison and Schneier, 2000). This view seems a little cynical since although people are making vast amounts of money from PKI, security remains a crucial part of being a successful e-commerce company. PKI may not be the ultimate user friendly security solution, but it is a step in the right direction.

The reasons for the lack of adoption of e-mail encryption include legal fears, user apathy and the complexity of obtaining a digital certificate. These issues are discussed in section 2.6.

2.6.2 The Importance of E-Mail Security

There has been no published success in breaking a public key encryption system, such as RSA, and it is deemed so effective that some governments have put a limit on the strength of encryption that may be used. Bauer (2002) suggests that classical style attacks are still possible and the lack of published attacks serves to aid the cunning experts, who prefer to keep their skills and techniques hidden rather than brag. Nonetheless, public key encryption remains a proven way of upholding secrecy and authentication, which is of particular interest, simply because e-mail is a social and business phenomenon, with billions of messages being exchanged daily. The potential for harm is therefore great. E-mail encryption provides several methods of protecting security and has been established for many years, yet is for some reason is only minimally used.

Central information stores are becoming more and more common ways to use the Internet to facilitate administration of large systems. In such stores, the details of hundreds, or even thousands of users are stored in a central location where they can be accessed and modified by remote. The UK's National Health Service (NHS) is operating such a scheme, known as the National Programme for Information Technology, which has been in operation since 2002. Over the next ten years, the Programme will connect over 30,000 GPs in England to almost 300 hospitals. Benefits of this system are claimed to take the form of a 'Care Record Service' which will allow patients to track their personal health and care information online, however, potential security risks have been acknowledged with this system.

The Foundation for Information Policy Research (FIPR) undertook an independent review (2004) to assess the confidentiality implications of the NHS program. They suggested that the creation of valuable data repositories will create extreme temptation for exploitation in terms of unauthorised access, or the abuse of authorised access. They recommended that nobody in central government should have access to identifiable health information on the UK population, and that the NHS take measures to prevent social engineering attacks on patient confidentiality. E-mail security and its associated technologies such as PKI, are one viable option for securing such a system.

Proposed methods of maintaining security are to use smartcards and PINs for authentication, to implement an audit trail, and to enforce policies which will only issue patient information on a need to know basis and only in the best interests of the patient. A representative for the program indicated that e-mail would not be acknowledged as an important part of NHS communications, due to security concerns (Horley, 2006). In a separate statement, developers of the NHS IT programme said that e-mail will not be recognised as a valid or important form of communication, because 'it is not secure enough' (BCS meeting 10th Jan 2006, Bridge Hotel, Greenford). Although it is theoretically possible to secure e-mail communications sufficiently for this type of sensitive information, it seems the complexity of doing so has acted as dissuasion to its adoption.

Information passing, such as GP to GP record transfer, will instead be handled by messaging components within the internal IT network. These messages will be based on the health Level Seven (HL7) standards along with XML. HL7 is a standard for composing clinical data messages at the application level. The HL7 standard has many technical committees, one of which is the security committee. However, little of the exact specifications can be viewed by non-members of the working group; the only document that could be found (Kratz, *et al.*, 1999) was last updated in 1999. It could well be the case that e-mail with PKI would be equally if not more secure than HL7 and as e-mail is already well established, it should also be accepted with less resistance. The problem is that PKI is too poorly understood, too complex to set up and use and possibly seen as an old technology, even though it has in truth never seen its heyday. Furthermore, attack models have shown that most sensitive data leaked has been as a result of social engineering attacks as opposed to brute force hacking (Anderson, 1996), meaning that the way security is understood and used is of more importance than the level of security which can be theoretically achieved. Social engineering attacks involve people more than technology; an example is a private detective calling a GP or hospital and persuading them to release information. A cynical view would be that under the Health and Social care Act 2003, the Police and Government are able to access, and thus possibly misuse any information they wish.

Recently, so called 'Phishing' has been the social engineering attack in the media spotlight (see Appendix C). The term was first seen in January 1996 on alt.2600, the online hackers newsgroup (Anti-Phishing Work Group, 2005). It describes an attack which tries to 'fish' out valuable information from unsuspecting users. In the first Phishing attacks, this information was the password for an AOL user account, but now it is more likely to be credit card numbers, passwords to online e-commerce systems, or personal details, all of which can be used to steal identities and money. By February 2005, Phishing attacks began to originate from 'zombie' computers (Ilet and Hu, 2005), that is, computers that have been taken over with a Trojan virus, giving full control to the hacker. The attacker can then send Phishing and spam e-mails through the zombie computer's

Internet Service Provider (ISP), making them difficult to track down and block. By July 2005 it was estimated that 100 per cent of all Phishing attacks were sent through zombie machines, with 168,013 new zombie computers emerging every day (CipherTrust, 2005). There are many agencies set up specifically to combat cyber crime, such as the Anti-Phishing Work Group, the Council of Europe, the G8, Interpol, The European Network and Information Security Agency, The Internet Watch Foundation and The Joint Money Laundering Steering Group, but it is difficult to judge their impact on the vast number of crimes still occurring. A landmark law case saw Britain's first perpetrator of Phishing to be jailed for four years on November 1st 2005 (Campbell, 2005). The man conned users of Internet auction site eBay out of £200,000 by stealing their passwords and selling non-existent goods in their names. This shows the legal system is becoming more able and willing to deal with hi-tech crimes, but sadly, in response to the huge surge in such crimes occurring.

Even with seemingly non-sensitive data, users have a right to protect their privacy and uphold the security aspects of secrecy, integrity and authentication, described above. Unsecured personal e-mails and unencrypted website submissions are open to identity theft, whereby attackers can impersonate the e-mail sender in order to obtain financial products in their name. If these communications were encrypted, it would make them extremely difficult for an identity thief to interpret. Furthermore, according to the Joint Money Laundering Steering Groups guidance notes, digital signatures can and should act as a form of electronic identification, which can be used by financial service companies to verify an identity before a transaction is made. Due to the small proportion of e-mail traffic which currently uses encryption, those messages which are encrypted may draw more attention to themselves as containing important data and therefore become a prime target for hackers to attempt to crack. Phil Zimmerman, author of PGP encryption software said "it would be nice if everyone routinely used encryption for all their e-mail, innocent or not, so that no one drew suspicion by asserting their e-mail privacy with encryption" (Zimmerman, 1995).

2.6.3 Problems with E-Mail Security

Many problems have been identified which could inhibit the widespread adoption of e-mail security:

- The difficulty of obtaining a digital ID in order to use encryption
- Poor software interfaces
- User apathy
- Legal concerns

Each of these is discussed in turn below.

2.6.4 Getting a Digital ID

Garfinkel's PhD thesis on design patterns of usable and secure systems presents a survey that was carried out on the e-mail practices of 400 Amazon.co.uk merchants (2005). It shows that e-mail security (digital signatures and encryption) are hardly used, with users feeling that the effort involved would be wasted, that it is not necessary, or they just do not care. Also discovered was confusion whereby those who had not used security thought they had, and vice-versa. Garfinkel points out the need for a further in depth survey to be carried out to assess the need, use and acceptance of e-mail security, as well as identifying the source of confusion over it. Garfinkel recommends that automated mail sent from 'no-reply' e-mail accounts of large corporations should be digitally signed by default. This would allow their many thousands of recipients to validate the origins of their e-mail messages and would help to prevent Phishing and other social engineering attacks. In the same thesis, Garfinkel points out that one of the main barriers to adoption of PKI has shifted from the software interface to the difficulty of obtaining a digital ID. A digital ID is required by both the sender and receiver of an e-mail if PKI encryption is to be used, and the complicated process required could be responsible for some of the problems Garfinkel observed with the use of e-mail encryption.

The book 'PKI, a Wiley Tech Brief' (Austin, 2001) provides users with no prior knowledge of PKI with directions to obtain and set up a digital certificate. There are 34 step by step instructions and a further 14 warnings and side notes which may apply differently to each individual user, and which users must assess individually to achieve optimal security. The book claims this process will take a total of 30 minutes. Researchers at the Palo-Alto Research Centre (PARC) tested a similar procedure. They performed a study where they asked users to set up a PKI-based authentication system (Balfanz, et al., 2004). The eight users studied were given a detailed list of 38 steps to follow and they all had doctoral degrees in computer science or a related discipline, yet it took them an average of 140 minutes to complete the configuration after which many of whom described the process as the most difficult computer task that PARC had ever asked them to do (Balfanz, et al., 2004). This perfectly highlights the dichotomy between security and usability, where highly skilled and experienced computer users have difficulty configuring security systems. This seems to leave even less hope for the average home user to do so.

2.6.5 Interface Problems

The frequently cited 'Why Johnny Can't encrypt' study (Whitten and Tygar, 1999) showed that the interface of PGP encryption software was one of the factors that caused it to have low

usability. Due to this, many users were unable to adequately secure their e-mail communications. A follow up study in 2006 (Sheng, *et al.*, 2006) found that despite the awareness of such usability issues and the passing of time, many problems were still evident. Sheng et al. found that users struggled with the interface to complete tasks and were not provided with enough clues or feedback. A separate study also found problems with making the process of sending a secure e-mail transparent to the user and making decryption of messages foolproof (McNamara, 2005).

The interface can also confuse or mislead users. For example, all Public Key Certificates contain an expiry date for the certificate, but it is not clearly identified which date format is being. This can lead to great confusion as Americans (MM/DD/YY) or Europeans (DD/MM/YY) may interpret the date differently. Garfinkel (Garfinkel, 2005) also found that users were frequently confused by e-mail security, with users who had received digitally signed messages claiming to have never received them, while conversely, some users claimed to have received such messages when in fact they had not. The reasons for this confusion were not identified, however since the interface is designed to give clues about the security status of messages, it can be assumed that it holds at least partial responsibility.

2.6.6 Standards and Mental Models

Before being able to use digital signatures or encryption, it is first necessary to choose a standard to use. It has been noted that there are too many PKI standards to choose from, which can be worse than having no standards at all (Articsoft, 2003). Organisations cannot guarantee that their messages will be received without error if the recipient is using different standards to the sender. There are many choices to be made, such as choosing an operating system, mail client, encryption algorithm and underlying PKI standard. This is bewildering for the average user, who had little information on which to base their decisions. In a presentation at Infosecurity 2006 event in London, Andrew Lochart described the problem of too many incompatible encryption products and technologies with no clear market winner, with consumers taking a ‘wait-and-see’ attitude. Standards must be used to ensure compatibility so that users will not encounter errors when receiving mail from disparate clients.

Under the current PKI system, users cannot send a secure message to anyone; both the sender and the recipient must have digital IDs. Not many people have a digital ID because it requires a lengthy signing up process, which is not required to send unsecured e-mail. When given the option, users tend to take the easy route and just send unsecured mail. As Dingleline and Mathewson put it, “for e-mail encryption, security is a collaboration between multiple people: both the sender and the receiver must work together to protect its confidentiality” (Dingleline and Mathewson, 2005;Garfinkel and Cranor, 2005). Being an expert on security is not enough to

protect your mails, as each person with whom you communicate must also have the necessary skills to decrypt messages sent to them and to encrypt outgoing messages. The need for all parties to obtain and set up digital IDs is an added complexity which seems to have negatively impacted on the adoption of PKI. Even once users have their digital ID, the complexity continues; it has been shown that users find it difficult to know when they should secure a message (Dourish and Redmiles, 2002). Users also frequently forget to secure sensitive messages that they know should be secured (Garfinkel, 2005). Users also find it difficult to know whether they have successfully encrypted or digitally signed a message, and have mistakenly believed that a message they have sent is secure when in fact it is not (Garfinkel, 2005).

2.6.7 Lack of Internationally Agreed Laws

Computer users need to protect themselves from a legal standpoint from fraud attacks, as they may be held responsible for any sensitive data being extracted from their electronic records. This information was revealed in the report “Electronic commerce: who carries the risk of fraud?” in 2000 (Bohm, *et al.*). The report from the foundation for information policy research revealed that customers of some online banks face the prospect of unlimited personal liability as a consequence of fraud which may be caused by Trojans, viruses, eavesdropping or other similar means. A spokeswoman for Barclays Bank said that the most likely way of online banking fraud happening is if customers open e-mails from unknown sources (Moores, 2000). Widespread use of verification technology such as digital signatures may help reduce such occurrences of fraud.

However, the legal aspects of e-commerce and digital signature legislation are a complex web of documents, perhaps viewed by companies and individuals as a minefield best avoided. UK law defines a digital signature as a ‘signature incorporated into or logically associated with a particular electronic communication or particular electronic data’ (Electronic Communications Act, 2000), the Electronic Signatures Directive goes on to specify that the signature must serve as a method of authentication.

The Electronic Communications Act 2000 states that a digital signature is admissible as evidence in any legal proceedings where the authenticity or integrity of electronic data is under question. This may cause individuals and organisations to be fearful of using digital signatures, as every message that has been digitally signed may be used as evidence against them. In today’s suing culture, many companies are doing all they can to avoid costly court cases.

The Electronic Communications Bill describes the duty of the Secretary of State to maintain a register of approved providers of cryptography support services (Electronic Communications Bill, 2000). However, it is not a legal requirement for people proposing to offer cryptographic services to be assessed and included on this register; inclusion is only carried out upon their request. In

other words, the register should provide a list of approved cryptographic service providers, but it is impossible to tell if a provider who is not on that list has been rejected, or has simply chosen not to be approved. In a separate document, the Department of Trade and Industry's Achieving best practises in Information security leaflet, it is explained that the statutory approval scheme described above will not be officially used unless an industry-led scheme fails. It is necessary to read an array of documents to understand how the law applies to cryptography, and following the trail between them requires a great deal of active effort, something which many companies may not find feasible or desirable.

The Electronic Signatures Regulations 2002 states that it is the duty of the Secretary of State to monitor the activity of all certification service providers who issue certificates to members of the public. These certification providers will be kept on a publicly visible register and the public may be warned of any provider who the Secretary of State deems to be acting in a detrimental way to the public. The Electronic Signatures Directive (1999) introduced a uniform standard for legal recognition of electronic signatures, regardless of their origin in the EU. Its section on liability refers entirely to the provider of a digital certificate, rather than the person who uses it to sign electronic data and lays down provisions to ensure that the certificate provider is responsible for assuring the identity of the signatory and the accuracy of the data in the certificate. The Electronic Commerce (EC Directive) Regulations 2002 state that breaking its regulations could lead to imprisonment of up to two years and/or a fine of up to £5000.

Apart from the complexity of the law confusing potential users of encryption, government officials have also seemed to disfavour the introduction of widespread, strong encryption, over fears it may hinder their ability to combat crime. In 1997 FBI Director Louis Freeh, in his speech to US Senate Subcommittee on Terrorism, Technology & Government Information, stated:

'If we are unable to access and decrypt real-time... conversations of criminals and people who would commit horrible crimes... we will be hard up to defend the country in many respects... Unbreakable encryption will allow drug lords, spies, terrorists and even violent gangs to communicate about their crimes and their conspiracies with impunity.' (Freeh, 1997)

Two years later a similar standpoint was expressed by the UK Prime Minister Tony Blair, when he described what he believed to be a 'conflict' between economic and social benefits and national safety, brought about by encryption:

'On the one hand, business has delivered a clear message that encryption is essential for developing confidence in the security of electronic transactions. ... On the other hand, the

use of encryption by major criminals and terrorists could seriously frustrate the work of the law enforcement agencies' (Cabinet Office, 1999)

In the same document, The Performance and Innovation Unit Report, the opposite is said about digital signatures:

'Digital signatures do not pose the same problem to law enforcement. They could even bring significant law enforcement benefits, as they would help an individual sender or recipient to be positively identified and may also help cut down on fraudulent transactions.'

The Performance and Innovation Unit Report was the first step in allowing 'lawful access' to decryption keys or plain text for reasons of national security. In other words, the government, given reason, can and will decrypt and read any encrypted messages sent over the Internet, if they are believed to be linked to a crime. Similarly, the Health and Social Care (Community Health and Standards) Act (2003) allowed the Government access to all medical records in the UK, for the purposes of 'Health Improvement'. It removed many of the patient privacy safeguards in previous legislation. This too could be a hold-up to the adoption of encryption, as members of the public may believe there to be little point in enforcing secrecy if there is a chance the government will read their messages anyway.

When one of the first free web-based encryption schemes HushMail, was launched, FBI spokesman Frank Scafidi commented:

"It doesn't sound like it's illegal, but is it a law-enforcement problem? Sure it is," (Festa, 1999)

This statement highlights the fact that electronic communications must fulfil two requirements; secrecy and disclosure (Palen and Dourish 2003). These two requirements fall at opposite ends of the information protection spectrum, but are both key to an organisation. Sensitive data must be protected and kept secret, but there may be times when it is necessary to expose that same data, for purposes of policy or law enforcement, or to complete transactions.

Export laws control the export of goods and technology, including cryptographic and other security software between countries. Export laws, particularly in the USA place controls on the use of encryption, to ensure that the government always has the power to decrypt and read messages, if necessary, to protect military and commercial interests. The UK government has decontrolled cryptographic products if they are generally available to the public, their functionality cannot be easily changed, they do not require substantial support from the vendor and details of their use will be provided on request. However, there are still controls on

commercial cryptographic products and laws in other EU member states, and other world wide countries vary. Because electronic communication is inherently borderless, it can be difficult to ascertain whether encrypted messages are going to break any one countered laws, particularly if the message travels across borders. The DTI has provided new online search facilities ((Goods Checker, DTI, 2006;OGEL Checker, DTI, 2006)) which allow the searching of goods and technologies to assess the legality of exporting them to various countries, however this seems unpublicised, time consuming to use and does not always provide a definite answer.

2.6.8 Complexity of Managing PKI keys

When using PKI, there are many tasks related to key management which needed to be performed every so often, including obtaining a digital certificate, renewing a certificate, or revoking one. The process of renewing an expired certificate with Thawte has been documented using a cognitive walkthrough technique in order to examine its complexity. A user account was created with Thawte and each stage necessary to renew the certificate was completed as an average user would do. At each stage the process was carefully considered from the user's point of view to become aware of any difficulties as the user would experience them.

When a certificate is about to expire, the CA sends an e-mail warning to that effect, after which there is only a short period during which it is possible to send digitally signed e-mails using the expired certificate, but the receiver of these mails will be presented with a daunting looking warning about the invalid certificate. Thereafter, the mail client usually gives a warning if you try to send a signed message with the expired certificate. Upon visiting the CA's website, the certificate owner is asked to enter their password; this is another opportunity for the usability flaws of passwords to foil the procedure. The link for renewing certificates is not clearly visible but requires some searching through the website navigation. When the correct page is reached, the user is asked to choose between two certificate formats; 'X.509', or 'developers of security applications', which is a potentially confusing choice for users to make. After selecting the type of certificate, there are three more steps to click through before another choice is offered, this time between all of the e-mail addresses that belong to the certificate. It is necessary to choose just one of these e-mail addresses to include in the certificate, although, confusingly, the web page allowed multiple addresses to be selected. This presents some confusion to the user as to which address should be selected and whether it would still be possible to sign e-mails sent from the addresses which were not selected. Next, there is another decision to make; whether to accept the default certificate extensions, or to configure them. After this, a list of 11 different 'CSPs' to choose from is presented, with no explanation of what a CSP is. After selecting the default option, a dialogue box warns that only trusted websites should be allowed to request a certificate, with a yes or no

choice to continue. After choosing 'yes', a message informs the user that the certificate will not contain their name unless they joined the 'Thawte web of trust', but there was no further information on this. After this, a certificate state screen was presented which showed the state of the newly renewed certificate as 'pending'. It took eight minutes for this status to change from to 'ready'.

An e-mail confirming the request for a new certificate was issued to the certificate owner. This message also contained information about two ways of getting the owners name to appear in the certificate. The first is to become validated by a certified public accountant, a practicing Attorney, or a Bank Manager. The second was the previously mentioned 'web of trust'. The web of trust requires one to visit two separate 'notaries' with proof identity documents so that they may confirm your identity, many of whom charge a fee for this service. For users who happen to live somewhere remote, the chances of there being a notary nearby diminishes, for example there is only one notary in the Thawte web of trust in the Shetland Islands. Once verified by notaries, the certificate will contain the owner's full name. However if, they choose not to have their ID validated, users are still able to digitally sign e-mails, except the certificate will only prove that one is able to receive mail at the originating address, rather than proving identity. It may be the case that many ordinary e-mail users will fail to check the certificate on every e-mail they receive and will take the digital signature icon to convey immediate trust. This can give a dangerous false sense of authority if it is assumed that digital signatures unequivocally prove the identity of the sender, which is not necessarily true.

This cognitive walkthrough demonstrated the complexity of one task a digital certificate owner is likely to encounter. The entire certificate renewal procedure required a total of 41 steps, which included six points at which settings could be altered, one point where a password had to be chosen, four points where a password had to be entered and three points where the trustworthiness of a website had to be judged.

As well as expiring, the public key certificate can be revoked by the Certification Authority. Each time the certificate is encountered it must be checked to ensure it has not been revoked (and is therefore invalid). This process incurs extra time and can become very complicated if the revocation list is very large and is frequently updated. However, if the revocation status is not checked, there is a chance that the signature may be wrongfully trusted. As can be seen this can prove to be an extremely difficult and lengthy process, especially for users who are not IT literate.

Garfinkel performed a usability study on Key Continuity Management (KCM); software designed to minimise the complexity of looking up and authenticating correspondents' public keys and with generating their own key pairs. Although KCM improves key management, it also opens up three

new attack models, which Garfinkel's study shows users are still susceptible to, particularly social engineering attack. Additionally, KCM does not aid in obtaining a digital ID in the first instance.

It seems that users have formed a mental model in which computers are trustworthy and seen as a source of authority (Yee, 2005). They also tend to trust the e-mail messages they receive, especially when it appears to have come from somebody known to them. They may not realise how easy it is to forge the sender field in a message header. Persuading users to distrust every message they receive, which should be the case for utmost security, is a difficult task that would undermine the convenience of e-mail. If every e-mail sent were protected with PKI encryption, this trust would be well founded, but unfortunately, this is not the case.

2.7 Summary and Conclusions

The evidence gathered so far shows that e-mail security has not had as high an adoption rate as had been expected. One of the reasons for this is thought to be the poor usability of the security software. Users and in some cases developers too, have believed that being difficult to use is a part of being secure. This has meant that although theoretically a very high level of security is attainable, in practice this has rarely been met because users would rather bypass the systems to save time. It remains unclear how much of this theoretical security users actually want or need.

PKI has been shown to be a well established and technically sound scheme for protecting electronic communications, however there remain many barriers to its adoption such as confusion over multiple standards, legal concerns and difficulty in obtaining a digital signature. This is an extremely complex system in which a single change will have many ramifications, so more research is required to find a way to finally harness its power for the masses. The Performance and Innovation Unit Report (Cabinet Office, 1999) states that there has been 'remarkably little co-ordination' of encryption policy between international countries, resulting in 'misunderstanding and suspicion' over the rationale behind regulating or influencing encryption. The complex legal references to encryption and digital signatures seem to have caused confusion for businesses and cynicism for the public.

PKI can protect the secrecy of information in transit and in storage, if it usable enough to afford proper operation by its users. The authentication it offers can also help dramatically reduce social engineering attacks such as phishing, identify theft, card not present fraud and unsolicited e-mails.

The current literature shows that passwords remain a widely used security mechanism with usability problems that remain to be fully addressed. Transparency is a technique that has increased the usability of software, but it is still unclear as to how much transparency is the right amount when it comes to security software. Education has been used to increase the public's

awareness of security issues and has been successful to a certain extent; however users can not be expected to learn every aspect of security and should not be blamed for security breaches which occur due to difficulties using poorly designed systems. Design patterns have been used in software engineering to apply solutions to a set of problems and it seems from recent work that they can be used to help align security and usability, so long as they are flexible and understandable. It is clear that in their separate fields, both security and usability are known to be improved when they are tightly integrated from the start of the development process. Thus, it would seem logical that this would remain true for the combined field of usable-security; this aligns with the findings of HCI-SEC researchers Balfanz et al (2004). However, despite this research, this does not seem to have been adopted in practice. This may be because experts on development teams have either a great deal of knowledge on security or on usability, but not both, and collaboration between the two groups of experts has been lacking. Kis (2002) also rightly points out that software houses primary aim is to make money, which they do by releasing software where functionality, along with time to market are usually the most important factors. The 'time to market' means that software houses want to produce new versions of their software as fast as possible in order to keep a competitive position in the market, this leaves less time to devote to non functionality related issues, such as security and usability.

2.7.1 Research Questions

The literature review has highlighted several areas which require further investigation, four of which are presented below and addressed in subsequent chapters of the thesis.

- To what extent has recent research been successful at aligning usability and security in practice?

Security software has been observed to have lower usability in many cases than other types of software, but work on improving the situation is immature. The HCI-SEC research field has suggested ways to counter this, including transparency, user education, visualisation and integration. Although there are numerous studies evaluating the usability of traditional security software, none so far have done so for emerging software aiming specifically to be both secure and usable. It is therefore necessary to evaluate the effectiveness of principles aiming to align usability and security in practice so that future iterations of such software can be improved and refined.

- What proportion of e-mail users have successfully obtained a digital certificate?

It has been suggested by Garfinkel (2005) that problems previously identified with the user interface of security software have now been replaced with problems in obtaining and using a

digital certificate. Since it is mandatory for both the sender and receiver of a PKI encrypted e-mail to have a digital certificate, the accuracy of this will affect the uptake of encryption. A sample set of e-mail users drawn from the general public can give an indication of this.

- Is e-mail encryption as underused as the literature has suggested, and if so, why?

Mostly anecdotal evidence has suggested that e-mail encryption, although a mature technology, has not matched the widespread adoption of technologies in other domains at similar stages of maturity. The motivation to examine this apparently underused security for e-mails is the sheer volume of e-mail traffic travelling on the Internet, which is expected to grow further in coming years. The potential for malicious unauthorised use of these messages is therefore also vast. Because adopting the technology is technically feasible, it is assumed that usability problems are all that stand in the way of greater adoption; these must be identified so that they may be overcome.

- What mental models are held by the public and by businesses of e-mail encryption?

It seems from the literature that usability problems are not only manifesting as graphical interface issues, but also as psychological issues related to the way users think of security. This justifies further research to investigate the users' views and attitudes towards e-mail encryption to find if this has affected its use in practice.

- Is there a way to ease the memory burden on users of traditional passwords?

It has been observed that people find it difficult to remember their passwords, which in turn can directly affect the quality of the security offered by them; therefore it is worthwhile investigating ways of helping people to remember their passwords.

This literature review has moved from the general observation that security seems to be limited in some way by its use, to the specific questions outlined above. These particular questions have arisen by separately examining the issue of usability, and of security, before exploring anecdotes, media and research articles to investigate how the former can affect the latter. The above research questions aim to gain clarity and insight into why these phenomena occur with a view to issuing recommendations to counter them. This process is important to ensure that there are no delusions about the actual level of security which is offered by software once it has left development and entered the domain of the end user. This process begins in the following chapter by evaluating software which was specifically designed to be both usable and secure.

Chapter 3: Evaluating the effectiveness of usable security principles

3.1 Introduction

In the literature review substantial evidence was presented that the usability of security software was lacking which led to unsatisfactory levels of protection in practice. Section 2.5 established that a dedicated research area known as HCI-SEC has evolved to combat this problem. The usability of encryption software has already been tested and found to be poor, most notably by Whitten and Tygar's 1999 'Why Johnny can't encrypt' paper, subsequently in 2005 by Garfinkel, and in 2006 by Sheng et al. All of these analyses have been on software which the literature review has identified to be wholly in the security domain, with little consideration for usability. With very recent research from the HCI-SEC beginning to produce software specifically designed to combine usability and security, analysis on this software is now necessary to gauge the progress being made and the effectiveness of the techniques used. A user study was designed to assess the most recent application of usability principles to security software, which happens to be an anti-virus software named Polaris.

Polaris is an alpha release for Windows XP and being a retrofit onto Windows rather than a complete redesign of the operating system means Polaris must comply with design features of Windows. It was developed by researchers at HP labs in California, USA and has the specific aim to align security and usability. The primary goal of Polaris is to make Windows safer from viruses and malicious code, but it was specifically designed to be highly usable as well. The developers of Polaris had a specific usability goal; that 'the user shouldn't be aware that Polaris was providing protection' (Karp, 2006, personal communication), in other words, it should be transparent. It should offer protection without interfering with users tasks and according to theory should therefore offer higher security in practice.

Polaris is based around the Principle Of Least Authority, described in section 2.6. Like other anti-virus software the aim of Polaris is to prevent malicious code from reading, altering, or destroying files on the system. However the method used to achieve this goal is very different; rather than using a virus definition dictionary to look for viruses, Polaris severely restricts the authority of software so it can only access the files it needs to run. Using this approach, applications can be isolated in separated disk areas ('polarized'), so they cannot affect other files. This creates a separate 'tamed' instance of an application, which is immune to viruses and is known as a 'pet'.

The aim of the usability study was to measure its success in its goal to be highly usable as well as highly secure. This work represents the first formal usability study to examine Polaris.

3.2 Usability Study of Polaris: Experiment Setup

The methodology used in this study is similar to that employed in the ‘Why Johnny Can’t Encrypt’ study (Whitten and Tygar, 1999), in that it uses a laboratory test which asks users to perform tasks that include the use of security. This study employed a combination of qualitative and quantitative approaches.

Experimental usability studies were used because they enable the detailed inspection of a scenario in controlled conditions, furthermore, Cook and Campbell (1979) state "the unique purpose of experiments is to provide stronger tests of causal hypotheses than is permitted by other forms of research" in (Gray and Salzman, 1998).

Lab based experiments are those where participants come to an area under the control of the researcher, whilst in a field based experiment, the researcher will visit the participant in locations where they would ordinarily carry out their activities. Lab based experiments are convenient, can be faster to complete and offer a great deal of control over variables which may affect the result. However lab based experiments may also introduce bias by placing pressure on the participant to behave in a certain way, or to fulfil what they perceive to be the researchers requirements; this bias can be minimised by avoiding contact between the researcher and the participant. A lab condition may not accurately represent how the scenario would be carried out outside of the lab and this may also affect the results. Field based studies can get a truer picture of the experimental scenario as the observation is made in the most natural context possible. However the experiment may take longer to complete and is more difficult to control. External variables may inadvertently come into play and affect the result.

Both of the experiments used in this thesis were lab based. This decision was made to increase the control over the experimental variables and to make the experiments faster and easier to set up and carry out. It is recognised that true usability can only be accurately measured over a long time period by observing what the user ordinarily does, rather than what he feels he is expected to do, however, this would be very costly and impractical to carry out. Instead bias was reduced as much as possible by asking the participant to behave as they would in every day work. During the tests, participants were left alone to avoid any bias which could be introduced by the researcher’s presence. They were observed by the experimenter from the adjoining room using one-way mirrors. A standard Windows XP desktop computer was used. Keystrokes and screen activity were captured and stored for later analysis using freely available logging software. Virtual Networking Computing (VNC) software was used to enable the participants’ screens to be

duplicated in another room; this allowed easy viewing of both the participants' body language and screen activity during the test.

This study used three pilot tests to refine the testing procedure, followed by ten participants for the main study. Virzi (1992) found that 90% of all usability problems were discovered in a study with ten participants, whilst the usability expert Jakob Nielsen (Nielsen, 2000) advocates using only five participants in a study. Using more than ten participants would have a very low ratio of problems discovered to resources expended. Based on the exploratory experiment, the hypothesis was that the software would not provide a good experience for the users.

Usability was measured through three metric categories derived from the international standard ISO 9241-11 (ISO, 1998); the definition of usability given in the introduction of the thesis. Using this definition the usability metrics used are shown in Table 3.1.

Table 3.1 Metrics used to measure the usability of Polaris in three categories

Effectiveness (the ability of users to complete tasks and goals)	Efficiency (the level of resources consumed in performing tasks)	Satisfaction (a user's subjective reactions to using the system)
The number of references users make to Polaris documentation	The time taken to complete each task	Questionnaires and short semi-structured interviews to gather subjective data
The length of time spent referring to documentation	The number of mouse clicks taken to complete each tasks	
The number of users who remembered how to complete goals after a period of inactivity		
The number of errors encountered		

A summary of the collected quantitative data is presented in Table 3.3 Table 3.3 Summary statistics of participants who completed the usability tasks.

3.3 Participants

The ten participants were student volunteers from the department of Information Systems and Computing at Brunel University, and were recruited using an e-mail message asking for their help. The initiative behind e-mail only recruitment is that e-mail was to play a big part in the experiment itself, so by responding to the call for recruitment e-mail, potential participants were showing their ability to use e-mail in a timely manner. The participants all had a good working knowledge of computers, but no specialist knowledge of security issues or terminology.

From the respondents to the e-mail, a group of mixed sex and age were selected and allocated an appointment. There was no monetary incentive to the participants, but they were keen to assist regardless.

3.4 Procedure

The Polaris documentation was also included in the evaluation as it is considered a part of the software package. Users were asked to perform some tasks to simulate the configuration of Polaris. After this the tasks represented ordinary computer usage in which the security features were presented as a side-effect of the primary task. This testing scenario would be much the same as in real situations where users would first be required to set up the Polaris software, but thereafter, it is assumed, would be more concerned with getting their work done than with configuring security.

Before the test, participants were simply told “Polaris is designed to protect you from viruses by restricting the authority of applications to access your files”. Participants were not given any further instruction or training, but were able to consult the Polaris documentation in electronic format during the test. The participants understood that they were part of a usability study, but that they should use the PC as they would their own.

A list of the tasks users performed during the test can be found in Table 3.2.

At the end of the testing, participants completed a questionnaire to gather subjective opinions. The questionnaire measured results on the System Usability Scale (SUS) (Brooke, 1996). SUS has been shown to be a good overall guide to usability and has been used extensively within its originating company, Digital Equipment Co. Ltd., and in external studies such as (Roth, *et al.*, 2004). The SUS is designed to give a quick impression of the overall usability of a product. It consists of ten questions rated on a Likert scale and yields a number from 0-100, where 100 represents excellent levels of usability. SUS was chosen for this study because it is very short and quick to complete. It is believed that this would avoid user frustration that can occur with long questionnaires and as a result, ensure that the answers given are as accurate as possible. The SUS questions were slightly modified to replace the word ‘system’ with the word ‘software’ to relate more accurately to the study at hand. Additionally, the SUS was augmented with five extra questions, also rated on a Likert scale. These extra questions were designed to assess the effectiveness of the documentation and the results were reviewed separately from the main SUS score. Completion of the questionnaire was immediately followed by short semi-structured interviews to gain more in depth information.

Participants were asked to repeat a shorter version of the test after a period of one week, this time without the chance to refer to the documentation. This test was to investigate the learnability of the software.

Table 3.2 Tasks as instructed in the usability study

Task	Task Description	Purpose
1	Identify which of three applications have been polarized	Users need to know whether the application they are using has been polarized or not (equivalent to working in a safe environment or a non-safe environment). This task tests how well the software informs the user of their status.
2	Polarize Internet Explorer	Test the process of making an application safe through Polaris
3	Browse an Internet banking website	Observe behaviour when using secure and trusted web sites
4	Check e-mails and follow hyperlinks	Observe behaviour when using insecure and not trusted web sites and e-mails
5	Manually add some buttons to the toolbar of Microsoft Outlook which will let you safely open and save e-mail attachments using Polaris.	Test the procedure for adding functionality to safely open e-mail attachments, which must be manually configured in the current alpha release of Polaris.
6	Check e-mails and try out attached files	Observe what security precautions are taken when trying attachments of unknown origin.
7	Download an application from the Internet and try it out on your system.	Polaris includes several methods to safely try out applications, this task tests which one users tend to take (if any) when they want to try out a potentially dangerous application.
8	De-Polarize Microsoft Word and open a document in the normal, unprotected version of Word.	Test if the user can correctly go back to using the normal version of applications after using Polaris.

3.5 Results

Polaris is different from traditional anti-virus software in that once installed it does not require updates. Once the one-off polarization procedure is completed, the virus protection is integrated into the application itself and the protection offered is independent of virus versions. This would seem to instantly offer greater usability, however this effect may have been negated by the burden on the user to make other security-related decisions.

After the tests, all participants showed an understanding of what Polaris was trying to achieve, but only two participants understood the idea of having multiple pets for a single applications.

Table 3.3 Summary statistics of participants who completed the usability tasks

Task	Average number of...				Average time taken (minutes:seconds)	
	Participants who completed the task (out of ten)	References to documentation	Mouse clicks	Errors encountered (cumulative)	To complete task	for each documentation lookup
1	7	5	31	4	11:56	1:41
2	10	2	15	0	4:40	1:01
3	10	1	12	2	5:17	0:16
4	10	0	14	0	4:32	0:00
5	4	15	56	25	15:22	0:20
6	4	0	14	15	4:51	0:16
7	10	2	30	6	6:05	0:40
8	10	1	12	7	3:00	0:32

The designers of Polaris wanted total transparency, but participants in this study did notice its presence. Polaris required initial configuration, required users to make decisions as to how to open files safely and produced error messages. It is possible that the transparency may increase over time, as the users configure it to suit their needs, but as this study took place over a short time scale, this cannot be determined.

3.5.1 Usability Metrics

Several usability problems were discovered with Polaris, and these have been categorised under the three usability metrics discussed in the introduction to the study:

- Effectiveness (the ability of users to complete tasks and goals)
- Efficiency (the level of resources consumed in performing tasks)
- Satisfaction (a user's subjective reactions to using the system)

Each is discussed in turn below:

Effectiveness

Some participants had difficulty in identifying whether the application they were using had been polarized or not. This was made evident in task 1 when three out of the ten participants were unable to discern between polarized and normal applications. A further two participants were unable to discern when tested in Windows XP service pack 1, but were able to correctly identify the difference in XP service pack 2. This is due to a bug in the software which prevented the visual differentiation from working in service pack 1. The remaining five participants were unable to identify the difference immediately, but had to take long measures such as examining the list of polarized applications in Polaris. Many participants commented in the interviews that the visual difference between normal and polarized applications was not apparent enough. The participants who could not identify whether applications had been polarized suffered from further ramifications in later tests, because they assuming they were being protected by Polaris, when in fact they were not.

The number of references to the documentation, and number of errors encountered were distributed fairly equally across all the tasks but one. In task 5 users were asked to customise the toolbar of Microsoft outlook so that it included options to use Polaris on e-mail attachments. Instructions on how to do this were in the documentation, however only four out of ten users ultimately managed to complete this task. This task required referring to the documentation five times as often as was the average for all other tasks, and produced three times more errors. This demonstrates the problems encountered when users are asked to set up software themselves. The

Polaris development team is making efforts to automate this process as much as possible for the beta release.

The average length of time spent referring to the documentation for the first task was eight minutes 25 seconds, as users familiarised themselves with the software. During subsequent tasks users looked at the documentation rapidly for brief periods of around 15 seconds, which shows their need for detailed guidance when first using the software.

Polaris displayed error messages sometimes with no apparent cause and frequently with no explanation of how to resolve the error. The participants were seen to quickly dismiss these error messages, especially if they had already seen the same error at least once. For example, the following error was given when trying to open a downloaded application using the 'Icebox' feature of Polaris:

Application has generated an exception that could not be handled.

Process id=0xf38 (3896), Thread id=0fx3c (3900)

Click OK to terminate the application.

Click CANCEL to debug the application.

This could have been better communicated to the user; the meaning of this error message is as follows:

This application cannot be opened in the Icebox. Try polarizing it, or if it is from a trusted source, open it without Polaris.

The participants completed a shortened version of the test after one week in order to test the learnability of software. This time there no documentation was made available. This test had mixed results, with some users being able to quickly complete tasks that others could not remember how to do and vice-versa. Some users commented that it would be easier if there were a context sensitive menu from which they could choose several Polaris options when right clicking files and hyperlinks. Polarizing an application was a task that was widely successful, it is thought that this is due to the interface being simple and intuitive (select an application and click 'Polarize'). However trying out an application downloaded from the Internet was a task with a low success rate. This is a task that required the participant to perform actions above and beyond what is normally required to run a downloaded application. These actions are not obvious, must be repeated very frequently, take extra time and hold no apparent advantage for the user, as they can run an application (albeit unsafely) without any additional steps. In these situations the participants chose to run the application in the normal way rather than use Polaris. Learning and

using Polaris presents barriers to getting work done quickly, the benefits of which hold too little value for the participants to put in the extra effort. Participants put emphasis on the speed of doing things and did not like to be slowed down. The participants' apathy towards security and willingness to compromise security is further discussed later.

Efficiency

Task 5, that required customizing the Outlook toolbar, took significantly longer (up to 15 minutes) and required up to four times as many mouse clicks as the other tasks. Users struggled with this task and exerted more effort than with other tasks. This task required much more customisation of the software than any other. Placing this burden on the user appears to decrease the usability of the software. All other tasks required an average of between 12 and 30 mouse clicks and took on average between three minutes and six minutes to complete, except task one which took 11:56, due to the initial reading of the documentation. This seems quite reasonable considering the users had never used the software before.

Satisfaction

The SUS scale gave a mean average score of 44.2 out of 100 (most of the scores ranged 20-50, two were around 70). Most users indicated that the software was cumbersome to use, and that they would not like to use it frequently. The participants showed frustration at nonsensical error messages and thought that the various features of Polaris were not well enough integrated. Some participants commented that more context sensitive menus would make Polaris easier to use.

One participant assumed that Polaris was automatically protecting their files at all times, when in fact some of the applications they were using were not under the protection of Polaris. This user had a high expectation of the security software in that they did not expect to have to take any explicit action in order to be protected.

3.5.2 Users' Decision Making Responsibility

The most serious usability problems arose when a considerable responsibility in decision making was passed onto the user. The most noticeable instance of this was when participants were expected to polarize an application multiple times for different uses. The Polaris documentation states:

"Each Pet has permission to read and write any files opened by that Pet. So, if you've opened one spreadsheet received as spam and another spreadsheet containing critical information, a virus running in the spam spreadsheet could destroy the information in the critical file. In order to prevent this attack, you may create more than one Pet for the same application"

It should be noted that malicious files opened in pets only present a security risk to other documents that are open in the same pet. Polaris provides protection over the system area of the registry and the Windows directory, which are often targets for attack.

The participants were presented with a scenario to test their use of multiple pets. They were given several hyperlinks to open in a web browser. One was a secure Internet banking site they had to log into and the others were unknown sites on publicly editable domains, which were engineered to appear untrustworthy.

When interviewed, just six out of the 13 total participants claimed they knew that it was possible to create multiple pets for one application, and only two of these knew why this would be desirable.

One of the participants who knew why multiple pets might be desirable created a pet browser to log into a secure internet banking website, and after using the site, indicated that he thought it was secure, safe and trustworthy. He was then sent two unknown hyperlinks via e-mail, which he believed to be insecure, unsafe and not trustworthy. He was aware that any malicious code from the distrusted site may be able to affect information from the secure banking session, but despite all of this, he still did not create multiple pet browsers. Instead, he opened the un-trusted links in the same browser pet as was used for the secure banking session, thus knowingly compromising the security offered by Polaris.

In fact, none of the participants used multiple browser pets.

3.5.3 Users' Attitudes to Security

When asked to download an application from a website and try it out securely, most participants considered the goal here was opening the application, rather than protecting their security. As such, nine out of 11 (82%) of the participants (this includes one pilot participant-the other two pilots were discounted due to technical difficulties) simply double clicked the application and opened it without Polaris, compromising the security of their PC. Some of these then went on to use Polaris to protect their security, but by this point the damage could have already been done, had the application been malicious.

During the experiment the participants were asked to judge the safety, security and trustworthiness of the hyperlinks before visiting them and in the interview they were asked to do the same after having visited the sites. The results showed that they were all able to distinguish between sites that should and should not be trusted. They based their decisions on previous experience, the appearance of the e-mail that contained the hyperlink, the reputation of the web sites (e.g. Yahoo) and by identifying the padlock symbol in the browser for the secure site. Although the participants

had a high awareness of the security risks of the Internet and knew the possible consequences of their actions, they were not any more protective of the PC's security; in fact they showed total apathy towards the protection of files and knowingly compromised their security.

The apathy encountered during the tests seems to be due to the users' persistent attitudes towards security. When questioned, the two users who did know the purpose of creating multiple pets did not put their theories into practice because they simply did not care about the consequences. Some participants also indicated that their data was not important to anyone but themselves and therefore not worth taking effort to protect. Participants also indicated that completing the task at hand was more important than protecting their security and it was observed on several occasions that they would try to use Polaris, but if they were unsuccessful in their first attempt they would bypass it to open files without protection. The experimental conditions in which the participants were observed may have affected their behaviour and would agree with the data from Weirich & Sasse (Weirich and Sasse, 2001), which showed that users will not make good security decisions unless they believe they are at risk. In any case, given that users will knowingly compromise their PC security, it is unreasonable to expect them to make continual security related decisions, such as when to use a different browser pet, in everyday life.

If the user set up the Polaris software, but subsequently did not use it properly, as was observed in these tests, their level of security would be comparable to ordinary Windows users. An exception to this would be the cases where users believed they were being protected by Polaris when in fact they were not; this may lead to complacency over security and increased risk of attack. If, however, Polaris is imposed on the user, for example by a corporate security policy, they would have to work through the usability difficulties outlined in this report. These include confusion over when protection is being offered by Polaris, annoying error messages, difficulty in customizing the software to work with e-mail clients and the inability (or lack of motivation) to decide when to use multiple pets for a single application. These problems would hinder the user in their work and may render the protection offered by Polaris ineffective.

The visual distinction between polarized and non-polarized windows needs to be much stronger, as users are likely to have a large number of applications in a mixed state of polarization and need to know immediately and intuitively whether they are being protected or not. Polaris should be more tightly integrated with the operating system so that context sensitive menus can be used. The need to have a separate pet for each trust category seems an impassable problem for the average user and one which is inherent to the application of the POLA principle. As such, the solution to this problem requires more thought than the simple interface changes which can remedy other difficulties. Perhaps each instance of an application pet could store its temporary data in a separate disk area which is cleared after the instance is closed. This would remove the risk of different

application instances interfering with one another's data, and remove the need for the user to make continual trust decisions, but at the expense of not allowing long-lasting data such as cookies to be stored and used.

3.6 Discussion

The above study used a controlled usability test with a task-oriented approach to collect data and observations on users' interactions with software. The software was specifically designed to offer security whilst reducing usability problems, but the evaluation found that usability problems remained, which in turn affected the security level offered in practice. In this respect, HCI-SEC principles have so far been unable to alleviate the usability problems with security software.

Some of the usability problems can be attributed to the fact that the operation of the software was not as transparent as its designers had hoped it to be. Furthermore, in accordance with the findings of (Dourish and Redmiles, 2002), participants did not know when or how to make security related decisions. Such usability problems may be alleviated by removing the decision making responsibility from the user, thus making the software more transparent. However, care should be taken to only remove this power from the user where the system can do a better job (make better decisions). Removing control from the user at times when only they can effectively decide when and how to share information can become problematic (de Paula, et al., 2005).

Polaris specifically could be improved by having pets automatically created for programs upon installation. Furthermore, if each pet uses a separate temporary disk area to store information, which is cleared after the pet is closed this could prevent the user from having to make decisions as to when to use multiple pets, however this would be at the expense of facilitating permanent data such as cookies and cached files. The goal of usable security in this case seems partially to owe its failure to the post-hoc nature of the software. This strengthens the argument made by other HCI-SEC researchers (e.g. Balfanz, et al., 2004; Flechais, et al., 2003; Yee, 2004), that security and usability must be developed in unison from concept right through to development as an integral part of the system if they are to align perfectly.

More generally, the participants were willing to compromise security; a worrying discovery and one which is not identified in the software designer's model of the system. This behaviour is rationalised by declaring the speed and ease with which tasks were completed to be more important than the protection of their files. This apathy may be counteracted by ensuring that the secure way of doing things is the fastest way. It would also be valuable to increase users' sense of worth for their data and increase their motivation for protecting it. It may at first seem that education is the best way of achieving this, but previous research has shown that education was rarely effective for such matters. The upcoming Internet Explorer 7 uses a colour coded address

bar to convey the authenticity of the website. In a similar vein, the eBay Toolbar (eBay, 2006) alerts users when they are about to submit their password to an unverified web site. Such visualisation techniques may be valuable to increase the user's sense of worth for their data, although it is likely that over time users will grow accustomed to these alerts and will learn to ignore them.

The participants also perceived security as an attribute of task completion rather than a task itself. This again conflicts with the designer's model which asserts that the users are liable for security threats if certain specific actions are not performed.

The participants quickly dismissed confusing error messages, in corroboration with the findings of (Gutmann, 2005; Zurko, *et al.*, 2002). The messages are not seen as helpful, once again conflicting with the designer's intention. The habit of clicking away messages before reading them raises doubt that message boxes are an effective way of alerting the user to an event.

First thoughts of the applicability of these findings to the more general domain lead to the introduction of personal liability as a core issue. It has been seen above that software designers and developers are responsible, or liable, for accurately meeting the users' needs, but have not yet achieved this. The users on the other hand, are seen as liable for protecting the security of their own data, but do not appear to do this adequately, perhaps due to the insecurities still not handled by the designers. This seems to create a loop whereby one inadequacy influences another; developers view users as responsible for the security of their data whilst users have the same view of developers. To assist in discussing further investigations of this phenomenon, the term Personal Liability and General Use Evaluation (PLaGUE) will be used as shorthand. PLaGUE describes how the liabilities and responsibilities felt by and implied onto users and developers affect the way software is used, and implicitly suggests that evaluation may be necessary to find out the Personal Liabilities.

The possible benefits if the problem is successfully addressed is a strong motivation to further examine why security software seems to be so difficult to use, and the implications of liability, perceptions and attitudes on this. This is particularly relevant when the target user group consists of widely varying levels of demographics such as age and computer literacy. To deepen the understanding of the impact of usability issues on security in practice it was decided to examine one specific application of security. E-mail encryption has been chosen simply because it has a sufficiently large user base with widely varying levels of technical expertise. The next chapter explores the use of e-mail encryption, with the particular aims of applying PLaGUE to understand its users' mental models, and ascertain the reasons for its apparent low usability as reported in section 2.6.

Chapter 4: E-Mail Encryption: Adoption and Attitudes

4.1 Introduction

Chapter 2 pointed out that the need, use and acceptance of e-mail security is still largely unknown and needs to be investigated. To gain an understanding of the current state of adoption of e-mail encryption, two surveys were carried out. E-mail encryption was chosen in particular over other security technologies because it is well established and technically sound, but seems to have low adoption. It is also a technology which if correctly implemented and used could combat the widespread threats of the Internet such as spam (unsolicited e-mail) and identity theft. This study aims to uncover the usability problems which, as with all security technologies, can impact the adoption rate and effectiveness of e-mail encryption.

The method employed for data collection was case study. Although the interpretation of data from case studies is potentially open to variation from individual researchers, it is considered to be the most widely used qualitative data collection method (Darke, *et al.*, 1998) and is flexible in its approach. Data collection was made from both individual e-mail users from the general public, and from persons of authority in various organisations. Interviews were used to collect the data in both cases. Interviews provide in depth information on people's individual attitudes not available in other data collection techniques, but for this reason are also difficult to validate as respondents views are subjective and may be influenced by the wording of the questions. Nevertheless, interviews provide a fast and flexible way to build a picture of each respondent's mental models and attitudes towards e-mail security. The interviews with individual users from the general public were semi-structured, fairly short, and the results were not analysed until the end of data collection. This is because recruitment was made on an ad hoc basis and respondents were willing to donate only a limited amount of time. Interviews with authority figures in organisations were longer and more in depth. Analysis was made after each interview, as recommended by (Glaser and Strauss, 1968), the results of which could be used to inform future interviews and in this way to question on topics that the researcher was previously unaware of, or those which seemed to warrant further investigation.

The results were analysed using a narrative approach to build a story of the respondents' views. As the question of why e-mail security seems so underused was important elements of mental model theory and adoption theory were used to investigate the barriers to adoption. The most prominent areas of interest were organised into a taxonomy in order to better present them in the summary.

4.1 Individual E-mail Users

Members of the public were asked to describe their views and use of e-mail encryption through the use of semi-structured questionnaires administered face to face. The aim was to highlight the factors which have caused the limited adoption of e-mail encryption identified in the literature. A pilot study was conducted at first to assess what types of responses would be given. These areas were then investigated in more depth during the main phase of study.

4.1.1 Pilot Survey

A pilot survey was constructed to ask a wide array of questions relating to security practices and attitudes, so that an initial hypothesis could be formed and subsequently used to inform the main study.

Procedure

The pilot study comprised a questionnaire asking respondents if they use e-mail encryption, providing reasons pro and con in free comment fields. Subsequent questions sought to identify the need for encryption by asking the types of data most commonly sent by e-mail, attitudes towards e-mail security and demographic information such as the technical expertise of the respondent.

The survey was administered online via a website in order to quickly reach a large audience. The survey was sent to 746 level 3 undergraduate and postgraduate students across four schools at Brunel University, and 124 responses were received (16.6 % response rate). Responses were aggregated and analysed numerically to show average trends.

Results

Only 12% of survey respondents had no idea what the terms digital signature or encryption meant. These were from varying age groups, but they were almost exclusively from non technical disciplines. However, most of these people claimed to be very comfortable with sending and receiving e-mail, perhaps an indicator that digital signatures and encryption go beyond what most people would think of as normal use of e-mail.

Most respondents do not use e-mail encryption, the most common two reasons being “I don’t care who reads my e-mails” and “I don’t know how to set up and use encryption”, despite 82% of respondents claiming to have the necessary technical abilities to set up e-mail encryption, perhaps an indicator of their level of education. The former reason for abstention from e-mail encryption suggests that the respondents do not feel that it is necessary, although other questions in the survey seemed to show the opposite. The most notable indicators of this dichotomy were that 54% of respondents send passwords over e-mail occasionally, frequently, or very frequently, 64%

exchange contracts or official documents over e-mail and 55% regularly give out personal information such as full names and addresses, date of birth etc. Statistically, the security risk becomes greater the more frequently sensitive information is sent unencrypted, however even a single unencrypted e-mail can become the weakest link in the chain of a user's security protocol and expose valuable information which can be used for identity theft, for example.

Furthermore, the level of environmental risk appeared high, as 54% of respondents have knowingly received e-mails likely to be phishing attacks (purportedly from an organization asking for web links to be followed and information such as a password provided). The threat of such attacks could be minimised through the use of digital signatures to prove the identity of the mail sender. The survey suggested a good level of awareness of this and other types of risks inherent to sending unencrypted e-mail; 44% of respondents correctly identified that plain-text e-mails are 'quite vulnerable' to being read in transit and a further 15% indicated that they do not place any trust at all in plain text e-mails. Overall, 81 people showed distrust towards plain-text e-mails, 77 of whom rated themselves as being either an expert, or very comfortable with sending and receiving e-mails, and most of whom studied a more technical discipline. Those with more technical knowledge tended to display more distrust towards e-mail, whereas those less technical tended to trust unsecured e-mail more. When asked their trust towards *encrypted* e-mail, 24% did not know what effect encryption would have, 10% trusted encrypted e-mails enough to send credit card numbers and the majority (39%) thought encrypted e-mails were 'probably safe', with a slim chance of being read in transit.

The awareness of risk was juxtaposed with the low adoption rate of e-mail security. In fact only 18 people (15%) stated that they had a digital ID necessary to send either digitally signed or encrypted e-mails. When asked for evidence of their understanding of digital IDs, in the form of describing their issuing Certification Authority (CA), seven respondents could not provide an accurate answer. Because obtaining a digital ID requires investing substantial effort, it seems unlikely that these seven respondents could obtain digital IDs without knowledge of its CA.

Of the people who had no digital ID, four claimed to send digitally signed e-mails and two people claimed to send encrypted e-mails, which is not possible without a digital ID, unless a special service such as HushMail or Secured e-mail is being used.

The survey asked how often e-mails had been sent and received that used digital signatures and encryption. Just 14 respondents indicated that they used digital signatures on outgoing mail and eight respondents indicating the use of encryption. These respondents declined to give an explanation of how they knew their mails had been encrypted, so their level of understanding of the question remains unknown. The most frequent usage of e-mail security was in receiving digitally signed messages, with 57% claiming to have received such a message, although most

indicated that this ‘hardly ever’ happened. Only one explanation was offered to prove the existence of digital signatures in outgoing mail: “You see your signature”. It may be that many respondents confused a digital signature with what is commonly called a ‘signature’; a pre written text block which many e-mail clients can be configured to append to messages. Just one explanation was offered to explain how digital signatures were present in incoming mail: “My operating system lets me open them. If it is not recognised by the system it wouldn't let me open it”. These comments clearly show some confusion over what exactly a digital signature is. The lack of comments from other respondents could be attributed to apathy over answering the question, or confusion as to how to answer it.

Summary

Most respondents were very comfortable with using e-mail and most had heard of the terms digital signature and encryption, although the extent of their understanding of the terms is unclear. Most respondents showed high awareness of the security threats of the Internet, and correctly identified risks associated with sending plain text e-mails. Despite all of this however, e-mail security is rarely used in practice, and where it is claimed to be used no supporting explanation was offered. Some respondents claimed to use digital signatures and encryption without having a digital ID, to have a digital ID without knowing where they got it from, or could not explain how digital signatures or encryption affected their e-mails. This shows a deep confusion in corroboration with Garfinkel's (Garfinkel, 2005) findings.

In free text response fields many respondents commented on their openness to adopt the technology, if only they knew how to set up and use it. Conversely, many also believed there was no need for them to use security because they felt their e-mails were not sensitive enough to warrant protection. However, many respondents indicated sending sensitive data such as their name and address, or a password at least occasionally, which warrants protection against threats such as identity theft. A few respondents showed cynical views such as ‘the war against evil will never end’, and ‘the government checks all mails anyway, why make their life harder’.

4.1.2 Main Survey

A second, more detailed questionnaire survey was conducted to identify the level of use of e-mail encryption, reasons for non use and perceived usefulness of the technology. A specific goal of the survey was to discover the actual level of use of security and any barriers to adoption of the technology. By its nature, no large system can through its operations ever know the number of abstainers. Yet these abstainers may be of key importance in discovering the usability problems with the system. The survey therefore aims to discover what, if any, usability problems or perceived problems are impacting on the adoption and use of e-mail encryption.

Respondents

The survey was administered to 87 members of the general public. Respondents' ages ranged from 16 to 70, with a gender split of 59% male and 41% female. The survey was not targeted towards any specific demographic as the aim was to gain insight into the entire potential and actual user base of e-mail security, i.e. the general public. Therefore any person who could be persuaded to complete the survey was chosen, regardless of their age, gender, or technical experience. Respondents were recruited in the streets of popular shopping towns at various times of day to avoid biasing the results with any one type of person.

The respondents were asked whether they knew what the term encryption means. Those who gave a positive response were asked to give a brief verbal explanation to confirm their understanding, whilst negative responders were read a brief definition of encryption. The respondents were then asked whether they used encryption on their e-mails and if so, for what reasons. If they did not indicate a use of encryption, they were asked whether using encryption would be desirable to them and why. Finally, the interviewees were asked what was stopping them from using encryption (the barriers to its adoption). They were given some time to provide their own answers, following which they were shown a card stating several possible barriers to adoption that have been identified in chapter 2, and asked if any applied to them.

Although encryption provides several categories of security - namely authentication, non repudiation, secrecy and integrity - the survey questions focussed solely on secrecy. The reasons for this were two-fold; firstly, a questionnaire covering all four aspects would be very long and likely receive fewer willing respondents using this recruitment method. Secondly, from the literature and the responses to the pilot survey, secrecy seems to be the most important and well known aspect of security to the average user, perhaps due to the heavy media attention it receives compared with other aspects of security.

Procedure

The data collection was made using brief, structured face to face interviews. Respondents were recruited in person in popular shopping districts in West London, UK. Three shopping districts were visited twice each, once on a weekday and once on a weekend. Each visit lasted around two hours. A large poster was created and mounted on a stand to solicit respondents and a free bar of chocolate was offered as an incentive. The respondents were asked questions which were filled out by the interviewer in their presence. The survey was only administered to respondents over the age of 16 who had not already completed the questionnaire.

The survey questions were constructed primarily to discover the actual usage of encryption and reasons given for use or abstinence of the technology. As well as discovering usability issues and

mental models, the survey also addresses an adoption problem identified in the literature; ‘why is e-mail encryption so underused?’ Adoption theories are the subject of much research, most of which is outside the scope of this thesis, but the most widely accepted adoption models amongst the research community are the Technology Acceptance Model (TAM) and the Theory of Planned Behaviour (TPB). A comprehensive model was developed by Gong and Yan (2004) to take into account factors from TAM, TPB and other models (figure 3.1). Some of the survey questions were designed to fit with concepts of this comprehensive model with the aim of finding factors which may influence the adoption of encryption. Table 4.1 shows how these adoption concepts have been reflected in the survey.

Table 4.1 Survey questions relating to concepts from popular technology adoption models

Adoption Model	Concept	Description	Example of related survey question
Comprehensive model	Domain specific Knowledge (DK)	The amount of existing knowledge of e-mail security a respondent has which can affect their decision to use the technology.	“Do you know what the word encryption means?”
TAM	Perceived usefulness (PU)	The degree to which the respondent believes using the technology is beneficial to them.	“Is encryption beneficial to you?”
TAM	Perceived Enjoyment (PE)	The degree to which the respondent believes using the technology is enjoyable.	Not Questioned
TAM	Perceived Ease of Use (PEOU)	The degree to which the respondent believes using the technology is free from effort.	“Do you think encryption would take too long to set up?”
TPB	Subjective Norms (SN)	The perceived influence of peers including friends, family and colleagues on the decision to use the technology.	“Do any of your friends, family or colleagues use encryption?”
TPB	Self Efficacy (SE)	The respondents self judged ability to operate the technology successfully.	“Do you think you would have enough technical knowledge to install and operate encryption?”
TAM	Intention To Use (ITU)	Whether the respondents is using, intends to start using, or would like to use the technology.	“Have you tried using encryption?” “Would you, if you could, want to have encryption for all of your e-mails?”

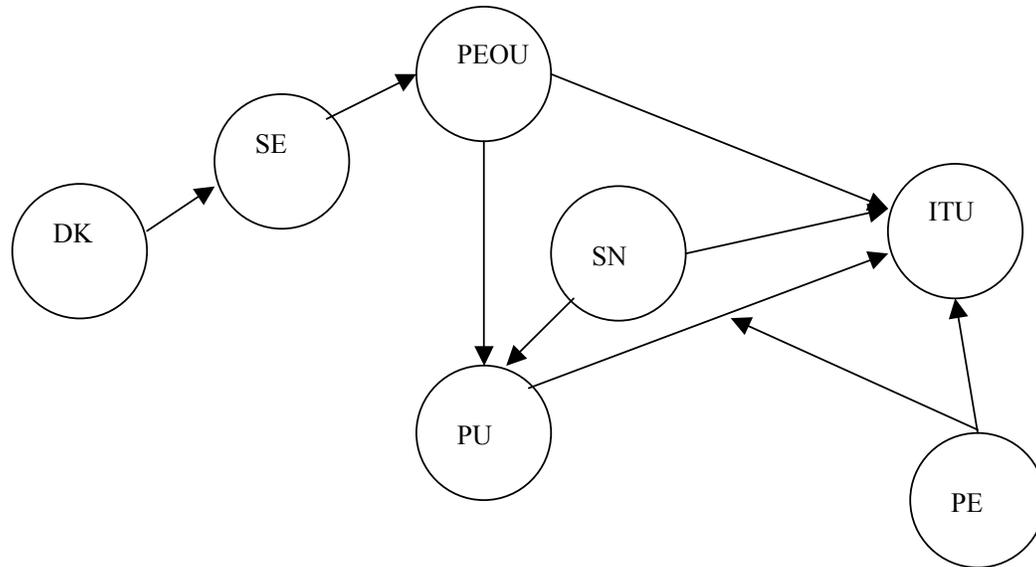


Figure 4.1 A comprehensive adoption model (Gong and Yan, 2004)

These adoption models all include an element of usability which can affect a person's decision to use that technology; The TPB model states that users' actions are partly guided by 'perceived behavioural control' beliefs, including the perceived difficulty of using the technology (Ajzen, 1991); TAM models how users come to accept a new technology and includes the perceived ease of use (the degree to which a person believes using the technology will be free from effort) of the technology (Venkatesh and Davis, 2000).

Usually adoption model questionnaires require two or three questions from each concept to confirm its impact, but this survey tested most of the concepts with a single question. The reasons for this are twofold; firstly adoption questionnaires can be long and time consuming and it was felt that this would severely affect the willingness of respondents to participate, their honesty and depth of answers during street recruitment. Secondly, the use of adoption models only make up half of the aim of the survey, the other half being to more generally examine the respondents use of and attitudes towards e-mail encryption.

As well as using adoption theories to analyse the results, mental model theory will also be used. Johnson-Laird (1980) describes the mental model in relation to cognition as:

'A mental representation formed through images or sets of propositions, which takes this evidence and uses it to draw a conclusion or make a judgement'.

Norman and Draper (1986) note that a system should be designed so that the user can develop a mental model of it which is consistent with the design model (the mental model of the systems

designers). If the user model is not consistent with the design model then usability problems arise because the user is not behaving in the way the software designers expected. Similarly, in what is considered the first article to discuss usability in relation to security, Saltzer and Schroeder state that the user's mental image of his protection goals must match the security mechanisms he must use in order to avoid failure (1975). Yee (Yee, 2002) also argues that there is a fundamental mismatch between software capabilities and users' mental models. Figure 4.2 demonstrates that the system is designed to follow a consistent conceptualization, but the mental model the user develops of the system either before or during use of it can become inconsistent.

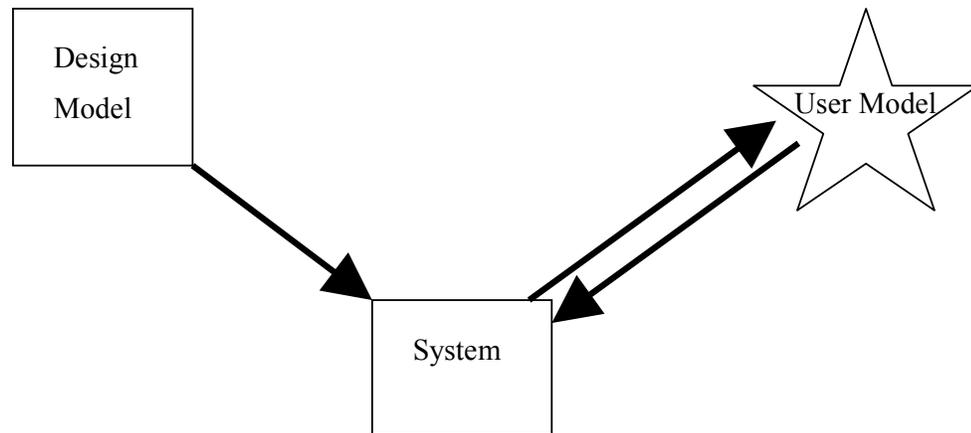


Figure 4.2 The design model versus the user model, adapted from (Norman and Draper, 1986)

One of the survey's aims was to build a picture of users' mental models towards e-mail encryption. As most of the surveyed users had not actually used e-mail encryption, their mental models must not have been developed from first hand experience with the system, but rather from other sources, in Johnson-Laird's terms; 'images and sets of propositions'. The images are communicated through the look, feel and behaviour of the system, whilst the propositions can come from the media and through word of mouth, filtering information about what encryption is and how it works through society.

Results

Developers of security products have seemed to have the opinion that security is a forefront concern to users; however this survey dispelled that belief. Results indicated that to most people computer security is important, but it is not actively thought about unless it is first brought to their attention. Even then, security will only be used if it incurs no costs to the user in terms of time to set up or use, effort to learn, or monetary costs. In other words, e-mail encryption must have extremely high usability to see widespread adoption in the public.

Perhaps unsurprisingly, most respondents said that they were not using, nor had ever used e-mail encryption. One respondent was told by a technical friend that it had been set up on their PC, but could not discern what impact this had on their e-mail. Another said that e-mail encryption came supplied with their Internet Service, although upon investigation this service could not be found offered by any mainstream ISP. Two respondents indicated that they had previously set up encryption but abandoned it after realising they did not know anybody else with a digital ID to enable encrypted communication. One respondent said that they have previously used encryption at work and university; however they have come to dislike all technology and now rely on offline methods of communication. Only one respondent seemed to fully understand the use and application of e-mail encryption, due to the fact that he has been the head of an IT department for 8 years and uses encryption both at work and at home.

Unexpectedly, most respondents had no idea what the word encryption meant, highlighting the dichotomy between the extensive media coverage of security problems and the very low awareness of established counters to these threats such as e-mail encryption.

Clearly if an individual is not exposed to a technology they cannot make any decisions on it. The Diffusion of Innovation Theory has five stages of decision making which influence whether a new technology will be adopted (Rogers and Scott, 1997), the first of which is awareness of the technology. The next stage - gaining additional information in order to make an adopt or reject decision – cannot be reached with prior awareness of the technology. Amongst the sampled users lack of awareness was a major factor for the non-use of encryption, indicating that the technology would benefit from significant promotion in the public sector. It is only after the initial awareness phase that the presence of any usability problems with the software will affect a person's choice on long term use of the technology. Thus it is important that in parallel with promoting encryption work is continued to identify and correct usability problems with the software.

When asked if they would like to use encryption (or for those who already are using it, whether they see it as beneficial to them), 64 responded positively, one was unsure and only 22 respondents said they would not like to start using encryption. The majority of people saw encryption as being able to protect their privacy, which they indicated to be of great importance to them. However, when asked if their e-mails were worth protecting, most respondents indicated that only 'business' or 'banking' e-mails are worthy of protection, whilst their personal messages are not. Furthermore, these respondents were speaking hypothetically as most of them never send any business or banking e-mails. Tables 3.2 - 3.4 show reasons why respondents would like to start using e-mail encryption along with reasons why they are not doing so. Table 3.5 shows reasons why people would not like to use encryption (some respondents listed more than one reason in each table).

Table 4.2 - Summary of results of e-mail encryption survey

Use of encryption	#
Do Not use	80
Use	7
Understanding of encryption	
No understanding	39
Full understanding	38
Some understanding	10
Attitude towards encryption	
Would like to adopt	64
Would not like to adopt	22
Unsure	1

Table 4.3 Perceived benefits of adopting e-mail encryption

Benefit	#
To increase or protect personal privacy	36
Because I have been made more aware of security threats recently	4
To protect against viruses	3
I don't want my account/system to be hacked	3
To help overall security for all of my e-mails	4
To allow me to send bank details over e-mail	4
To stop getting spam	2
Because you never know who's reading your work e-mails	2
To protect my identity	2
Because it seems safer	1
To protect confidential research that I send by e-mail	1
Because I work for a law firm who do not use encryption but send potentially sensitive data	1
Because Big Brother is watching us	1
To combat marketing and spying technology	1
Because it is used at work	1
A technical friend set it up for me	1

Comments expanding on these answers stipulated that encryption must be automatic, free, uncomplicated, require no extra effort and go unnoticed; all demonstrating the very high usability levels expected. 28 respondents thought that e-mail encryption was only necessary for business or

banking e-mails, but not for general e-mails. However when asked, very few respondents actually use e-mail for business or banking purposes.

Table 4.4 Reasons why respondents are not currently using e-mail encryption (self given reasons)

Reason	#
I didn't know it existed	17
I don't want to use it (see table 4.6)	16
I don't know how to set it up	15
My ISP /e-mail provider doesn't provide it as standard	6
I cant be bothered/it would take too long	6
I'm not sure where to get it from	5
I don't know much about it	4
I've never thought about it before	3
I didn't know it was something that is accessible to me	3
It's not provided at work	2
I'm not serious about using it	2
It sounds complicated	2
It would be difficult to get others to understand how to decrypt my e-mails	2
My PC is too old/I don't have a PC at home	2
I don't know anybody else using it	2
I am sick of technology and want to go low tech	1
I tried to obtain a digital ID but got stuck because it is too complicated	1
I thought it already happened automatically	1
You can always be hacked no matter what you use	1
PCs crash too much already – there needs to be as little software being used as possible	1

Table 4.5 Reasons why respondents are not currently using e-mail encryption (reasons selected from a list)

Reason	#
I don't know where to start.	60
I am using some other way to secure my data.	40
I think I won't have enough technical knowledge to install or operate it.	37
I have too many passwords / have difficulty remembering passwords.	33
I think my information is not worth protecting; I don't care if anyone can read my e-mails.	31

Reason (continued...)	#
I was not aware of its existence.	29
I think it will be expensive to set up.	25
I think it will take too long to set up.	25
I don't think my information can be accessed by others over the Internet.	10
I have set up encryption but don't know anybody else who has, so can't send any encrypted e-mails.	4
I have tried using it but cannot use the software.	1
I have started to set up encryption but got stuck with getting a digital certificate.	1

Where respondents said they did not know whether a statement would apply to e-mail encryption they were asked to make an assumption. Most respondents said they had trouble remembering passwords because they have too many. Lack of awareness was a big problem. Other security methods used were cited as being passwords, anti virus or anti spy ware software which do not protect information in e-mails, although it was not ascertained whether these respondents believed their current security measures to be adequate to protect their e-mails. Most people believed that encryption would be free to use and quick to set up, and would be willing to adopt it if this were the case and they knew what first steps to take. Many suggested advertising campaigns on television and newspapers, or training schemes in the workplace to raise awareness.

Table 4.6 Reasons why respondents would not like to start using encryption

Reason	#
I never send anything that needs to be secured./ I do not think anyone would be interested in my e-mails./ I do not care if anyone can read my e-mails./ I do not care about my personal details	17
I do not use e-mail enough to warrant it.	3
I have never been hacked before so don't see the need.	2
I have been sent digitally signed e-mails before and Outlook forces me to copy and paste every message in order to reply.	1
My work e-mails are protected by the work server anyway, and my hotmail account is just for junk	1

Many survey respondents expected that if e-mail encryption were necessary it would be provided as standard by ISPs and other e-mail providers, but an example of this occurring cannot be found in reality. If this were the case, it would satisfy the desire expressed by respondents to use e-mail encryption whilst removing one of the main barriers identified with sourcing the technology. Another frequently encountered reason for non use of encryption is that respondents did not deem their personal data worthy of investing effort to protect, despite claiming personal privacy to be

important to them. The proliferation of encryption may influence others to enter the trial phase of adoption, as described by the subjective norm factor of adoption models.

In the survey perceived usefulness was generally high, although adoption remained low, shifting the blame for non use onto other factors such as perceived ease of use, subjective norm and perceived enjoyment. Gong and Yan noted a chain effect within their comprehensive model of adoption (2004) whereby one concept directly affects others. Specifically, they found that users' self efficacy strongly increases the perceived ease of use, which in turn significantly increases the intention to use the technology. 43 % of respondents said that they believed they would not have the necessary technical skills to use e-mail encryption unaided indicting a low self efficacy. This suggests that within this group the perceived ease of use is also lower, which itself impacts on adoption. Perceived enjoyment was not measured, but within the subjective norm factor, respondents rarely knew any peers who used the technology.

Users form mental models of security by asking the question "is this system secure enough for what I want to do?" (Dourish, et al., 2004). When asking this question of sending e-mails, this survey has shown that most people have found unencrypted e-mail to be secure enough, as they have used it regularly. The most popular reason given by respondents for not using e-mail encryption is that they do not believe their information is worth protecting, whereas the design model for e-mail encryption software is that people need high levels of protection for their e-mail. This is an example of the user's mental model not matching the design model.

The survey also showed that many people thought encryption to be irrelevant to their personal lives and more appropriate in a banking, or business setting. Where this opinion originated from is unclear, but it does support the notion that the user's mental model of encryption does not match the design model (that encryption should be used by everyone to protect any kind of data).

These disparities between user and design models could be addressed by increasing users' sense of worth for their information, or making encryption seem more relevant and appealing to them, or both. Both of these are solutions revolving around education of users which the literature review has shown to be not wholly effective. An alternative is to mandate the use of encryption so that all e-mails are secure regardless of their perceived worth, but for this to be successful, the cost of using encryption must be very low so as not to incur extra cost to the user.

Since very few respondents had used encryption, mental models formed through images, often metaphors encountered during system use, are not discussed for their effectiveness.

4.1.3 Summary

In the pilot survey most respondents knew the meaning of the word encryption, whilst in the main study the opposite was true. This highlights the bias that was placed on the initial study by recruiting only university students, whilst the results from the main survey were more representative of the general public.

It has been established that the sample of respondents need e-mail encryption because they often send sensitive information such as their name and address, passwords, or documents relating to their work/research etc., all of which can be used for identity theft or targeted spam/Trojan attacks. It was also found that the majority of respondents want to use e-mail encryption because they value their privacy and are aware of the number of possible attacks over the Internet. However many respondents had no prior awareness of encryption, highlighting its lack of presence in the general public sector. Of those who knew what encryption is, most had never used it. Most respondents expressed a strong interest in using encryption for their e-mails if they could, but simply did not know where to begin.

There seems to be a disjoint between the high value people placed on their privacy and the extremely low effort they are willing to make to protect their privacy. Despite expressing a desire to use encryption for all e-mails to protect personal privacy, respondents said in practice they would only use encryption for business or financial e-mails, even though most do not send this type of message.

Expected usability standards for e-mail encryption are very high, with many respondents indicating that it must be transparent, free to obtain, fast and easy to use, and provided to them as standard (for example by their ISP).

Analysis of the data gathered has led to the following recommendations:

- Increase the awareness of the advantages of e-mail encryption amongst users in the public
- E-mail providers should issue digital signatures by default

As most respondents had not used encryption it was not possible to analyse their interaction with encryption software, nor to identify specific usability problems with it; work questioning only respondents who have used encryption can be used to accomplish this.

4.2 *Organisational E-mail Users*

The international standard ISO 17799 recommends that organisations should develop and implement a policy on the use of cryptographic controls to protect the confidentiality, authenticity and integrity of the data it handles. The data collected from the public showed a low awareness of

e-mail encryption, but high perceived benefit. The information on attitudes to e-mail encryption gathered by survey is extended by gathering data from the corporate sector using interviews in order to gather more in depth information.

4.2.1 Interviews With Users in Organisations

The aim is to offer a snapshot picture of the extent to which e-mail encryption is used in a selection of organisations. It is intended to show the potential effect that encryption could have on these businesses, attitudes towards the technology, barriers to the proper use of e-mail encryption and any particular usability issues which can be identified.

The organisations chosen for these interviews are shown below, in descending order of the amount of data which was collected:

Table 4.7 Organisations interviewed on use of e-mail encryption

Organisation	Date of Interview, Interviewee
The National Health Service (NHS)	September 2006, Keith James, the new Information Security Manager. May 2006, Ravi Rao, Information Security Manager to the Hillingdon NHS trust. September 2005, Kimon Kontronis and Gay Bineham, research centre directors, Hillingdon Hospital.
The Metropolitan Police Service (MPS)	August 2005, Tony Troy, Head of Information Security Assurance Unit DoI 2, Metropolitan Police.
The Royal Bank of Scotland (RBS)	November 2004, manager, NatWest (subsidiary of RBS) head office.
The Financial Standards Authority (FSA)	September 2006, e-mail communications with an FSA representative.
A large American petroleum corporation, UK office	September 2006, IT security manager, Anadarko.
A University	September 2006, Policy Development and Quality Manager, University Computer Centre.
A secondary school	September 2006, head of the IT department, London based Secondary School.

Organisation (continued...)	Date of Interview, Interviewee
A large national retailer	September 2006, security administrator, head office, anonymous national retailer.
A large stock broking organisation	August 2006, head of IT.
A small IT consultancy	September 2006, manager.
A legal firm based in Hong Kong	March 2007, business manager

All of these organisations were chosen because they potentially handle sensitive data. The term ‘sensitive data’ is used within the meaning of the data protection act; any information which can be used to identify the racial background, political or religious beliefs, sexual activities, trade union status, or alleged commission of any offence of a person. For the purpose of this study, this definition is extended to include any information which may be used to harm the financial or personal well being of a person, for example, the name and address of a vulnerable minor, or details of a financial transaction.

The interview questions were designed to identify the need for information security, the actual use of security and any barriers to adoption of encryption. The interviews were semi structured to allow interviewees to direct the questioning somewhat when an interesting issue was raised. Interviews were conducted using a combination of face-to-face, e-mail and telephone methods. E-mail was found to be an efficient method of gathering data, particularly to follow up points raised in face-to-face interviews as and when they were raised without the need to schedule a further appointment.

The study faced some difficulty in the form of non response from some of the organisations. Ironically, it was difficult to gain information which could be used to improve the security of organisations because the organisations were weary of this information being used for harm rather than good. Consequently, the level of information gathered varied widely between organisations according to their willingness to discuss security.

4.2.2 Results

The information gathered from the interviews was categorised by the following issues:

- Need for Security
- Use of Security

- Cost of using Security
- Software Usability Problems
- Social Factors
- Knowledge and Belief Factors

Each issue is discussed in turn below:

Need for Security

All of the organisations dealt with some form of sensitive information and often exchanged this information using e-mail. The most sensitive information was exchanged by the Metropolitan Police, and details offences committed, personal details of vulnerable persons, etc. This information is often required to be shared with social services, the NHS and the government. The Metropolitan Police also emphasised the need to share information between themselves, health trusts and local authorities. In order for this to occur, all NHS trusts should be using the NHSmail secure system (as described in section 4.2.2) however this is not always the case. Similarly, most local authorities are not using any secure e-mail system, however the Criminal Justice Information Technology government department is driving them to adopt a system called Criminal Justice Secure Mail (CJSM) to enable secure communicate with police forces. This system is currently undergoing implementation.

Within the NHS there is a frequent need for sensitive data to be shared and transferred outside of a hospital. Sharing information across boundaries is absolutely vital to the smooth operation of the whole health care system. The boundaries include those between the various divisions of the NHS (acute care, primary care, research centres, social services and mental health), between hospitals and between the NHS and the Metropolitan Police. Such data may include patient identifiable records, digital X-Ray images, or details of mental health cases for example. Sharing information with the police is also required in cases involving children at risk. In such a situation, electronic communication is not deemed secure enough to be used, so the police would be telephoned and would make a personal visit to the hospital. One shocking exception to this rule was observed, in which a London borough's child protection register is e-mailed in an unencrypted Excel spreadsheet to hospitals, putting the data at risk of being exposed and the children on the list at even greater danger.

At the university data security is said to be taken very seriously due to the perceived threat to business continuity and the university reputation if data were to be disclosed inappropriately. It is the university policy that e-mail is not an appropriate medium for sensitive information to be communicated. It is assumed that this policy is being followed by all staff and students and that

therefore there are no sensitive data travelling in e-mail, however this policy is not actively monitored or enforced.

The stock broking organisation, along with the petroleum company ('Anadarko') both handle data of extreme financial importance. At the stock brokers, customers trade in financial products such as stocks and shares. Each trade is recorded in what is known as a ticket. The ticket contains sensitive information such as details of the buyer, the seller, the price and the product. In order to make the trade legal, a record of the ticket must be entered into and stored on the system and sent to both buyer and seller. These records are communicated using a fifty percent mix of fax and e-mail. E-mail is also used to respond to queries with trades. The integrity of these e-mails must be absolute to ensure that there can be no disclosure of clients contact details, or the altering of legal ownership of the product, however without proper encryption this cannot be guaranteed.

Anadarko handles sensitive commercial data which can represent extremely large financial investments, so it is imperative that this data is only accessed by authorised persons. It is the company policy that sensitive information is not sent by e-mail, because e-mail is assumed to be insecure. Although the policy is not actively enforced, e-mail is assumed to only carry non-sensitive data, therefore no encryption is applied. The sensitive data is sent by means of fax and other 'unknown means' which could be ascertained during the period of the interview.

The stock broking organisation creates most of its policies inline with the FSA, the UK's national financial services and markets regulator. The FSA aims to maintain efficient, orderly and clean financial markets. The FSA was asked to comment on its attitude towards recommending security to other organizations, rather than its own internal use of security, but proved to be one of the organisations unwilling to enter extensive dialogue. Instead, a catalogue of online resources was provided, presumably representing all publicly available FSA documents. These documents were analysed to find pertinent information on security policies.

The Royal Bank of Scotland when approached identified that their e-mails do contain a large amount of information they consider sensitive, mainly relating to classified research projects into new technology and banking devices. However RBS declined to give a full interview, despite repeated attempts at allaying their concerns.

The remaining three organisations all indicated that they use e-mail for the communication of sensitive data; clients' personal data and financial data at the IT consultancy; pupils' personal and medical data and data on exams and coursework at the school; confidential data on the legal proceedings of clients at the legal firm. All of these organisations used the ubiquitous Microsoft Outlook e-mail client software, and sent e-mail frequently both internal and external to their own networks.

Use of Security

The Metropolitan Police Service (MPS) appeared to use the highest security protocols out of all the organisations studied. The MPS is linked to the Government's Secure Intranet via the Criminal Justice Extranet (CJX), which is suitable for transmission of material up to 'RESTRICTED' protective marking. The CJX is essentially a Virtual Private Network (VPN) which makes the security transparent to the end user. Routing via the CJX and subsequent security measures automatically occur whenever a '.pnn' e-mail address suffix is used, whilst all other e-mails are routed via the normal Internet. Secure VPN traffic is also facilitated for communication with the NHS and the Local Government Secure Intranet (LGSi). It is estimated that 90% of e-mails travel over this secure VPN and the success of this is the main reason why a full Public Key Infrastructure (PKI) has not been implemented as yet. PKI is currently being used in limited situations to administer smart cards for remote access control. A larger implementation of PKI is underway and is expected to be operational late in 2007, at which time it is envisioned that digital signatures will begin to be placed on e-mails. The PKI programme is seen as not being strictly necessary to communicate securely with those outside the criminal justice community; however it would make increased network and workstation security easier to control. Ad hoc transmission of sensitive material over the Internet is allowed using the encryption built into WinZip (256 bit Advanced Encryption Standard), though for documents no higher than 'RESTRICTED' marking. This type of encryption relies on passwords in a way PKI would not. For documents which are above 'RESTRICTED' marking, several communications methods are used, including secure telephony and fax, which are approved by the Communications-Electronics Security Group (CESG) Assisted Products Scheme (CAPS), from the Government's Technical Authority for Information Assurance

Information security in the NHS is covered by a set of in-house guidelines known as the 'Caldecott principles' which aim to ensure ethical and secure processing of data. A member of staff is appointed as the 'Caldecott Guardian' and is responsible for upholding these principles, yet there are currently no formal methods for reporting incidents relating to breaches of security and confidentiality (such as sharing of log on IDs, or the leaking of data which can cause financial loss, embarrassment, legal penalty, or identification of patients). However in October 2007, a policy will be in place to report, though not to actively seek out such incidents. This policy will be linked to the NHS Trusts disciplinary policy to reprimand individuals responsible for the incidents. The Caldecott committee recommends that sensitive data which is to leave the hospital by means other than e-mail should be encrypted onto a CD-ROM, but this process was found to be so time consuming that it has been abandoned. Instead such data is usually stored on a CD-ROM

and either sent by courier, or given to the patient to take with them if they are transferring to a different hospital.

In 2002 information security at the NHS was developed with the introduction of an encrypted web-based e-mail system for NHS staff called NHSmail; all NHS staff are issued with an '@NHS.net' e-mail address as standard, but using this address is optional. NHSmail uses 128 bit encryption if it is sent to another NHSmail address, but is insecure if sent to a non NHSmail e-mail address. Another '@org.nhs.uk' suffixed e-mail address is issued which is insecure and carries a disclaimer advising against sending sensitive data. The British Medical Association advises that NHSmail should be used for all electronic communications which contain Personally Identifiable Data (PID), and the NHS Trust policy is that staff should not send sensitive or patient identifiable information using other insecure e-mail systems. The Trust security managers believe that it should ideally be used by every member of the Trust; however, they indicated that it actually sees extremely limited usage.

NHS recommendations also exist stating that all PID being sent electronically must be sent either via the NHSmail system, or encrypted using Advanced Encryption Standard (AES) provided by Utimaco SafeGuard, WinZip v9 or PGP. The NHS Connecting For Health Information Governance guidelines state that it is not acceptable to exchange identifiable information over unencrypted e-mail, in a password protected file (e.g. Word document), or using WinZip encryption lower than version 9. These policies are trust based and are not monitored or enforced. Interviews with the security managers for one of the NHS trusts indicated that the secure NHSmail system sees very low usage. Although the official method of exchanging confidential patient records is paper based (face-to-face using internal courier, royal mail, or more rarely, secure fax), it was revealed that most information communication is actually done electronically because it is faster and cheaper. The information security managers believe that internally there is a low security risk to these communications as there are few access points into the network and no wireless network access points. No mention was made that e-mails are not 'internal' but in fact travel over the Internet.

In RBS it was estimated that about 90% of the e-mail sent was internal to the company and so does not travel over the Internet, so it was felt that e-mail security was not a large concern. However RBS does have a dedicated department called Trust Assured that is actively marketing solutions in this area. One such example is a new project in conjunction with American Express to use the established encryption scheme Pretty Good Privacy to encrypt confidential documents, but no further information was offered on these developments. There is currently no use of e-mail security at RBS.

The IT consultancy use Microsoft Outlook Exchange clients to send e-mails, but do not employ any type of data encryption. There was reported to be a trial use of encryption in the past; however its usage rapidly declined due to many technical problems.

The university's many policies are addressed by the computer centre (Brunel, 2006) and are guided by external bodies such as Joint Information Systems Committee (JISC) and relevant Acts of Parliament. No security is employed on e-mails because it is assumed that the university policy of having no sensitive data transmitted via e-mail is adhered to. Internal e-mail does not leave the university servers but is routed via a Microsoft Exchange server, whilst e-mails sent elsewhere travel unencrypted over the Internet.

The stock broking organisation does not employ any kind of security of its e-mails. The main reason given for this was that no such requirements were imposed by the Financial Services Authority, which regulates UK financial companies. It seems that the organisation in question bases their security policies solely on the compliance with FSA regulations.

The FSA has not produced any available policies or guidelines specifically relating to the use of encryption for e-mails. The only mention of information security was relating to amendments to the Interim Prudential sourcebook for Building Societies (IPRU (BSOC)) to reflect the possible use of electronic communications between societies and their members. These amendments were made under section 157 of the Financial Services and Markets Act 2000 (FSMA) and were made because of recent changes to the Building Societies Act 1986 (Electronic Communications) Order 2003 (SI 2003 No: 404) ('the Electronic Communications Order'). The effect is that building Societies can, if they wish, communicate electronically with their members on constitutional matters, such as the business of annual general meetings, including election of directors and mergers and transfers of business. In all cases the member must consent to the means of communication (FSA, 2003). The Electronic Communications Act 2000 applies to all UK companies and generally permits electronic communications (e-mail, or CD, fax, WAP etc) as an effective alternative to paper based methods, but with no mention of security.

The FSA also state that disclosures or requests for disclosures between Inland Revenue and the FSA must take place in writing or 'secure electronic communication' (FSA, date unknown), where the level of security will vary depending on the protective marking of the document. 'BRENT' secure fax is later mentioned as an example, but no mention is given to e-mail. Requests for disclosures must also comply with the data protection act 1998 - Schedule 1 – Data protection principles, which state that appropriate technical measures shall be taken against unauthorised processing of personal data. But once again there is no specification of any specific security measures, just general guidelines such as taking 'reasonable steps' and offering more security for more sensitive data.

At the secondary school, there is no security employed on any e-mails. There are no short term plans to adopt any further security technologies. There was cited to be more interest in adopting a more rigid security system if there was more awareness of encryption technologies and if there was more perceived risk to the data being sent. The e-mails are handled by Microsoft Exchange Server 2003, with Outlook XP for client access inside the school and Microsoft Web Access (OWA) outside. Connection to OWA is secure using the HTTPS protocol. Exam and census data is sometimes needed to be set externally, which is accomplished using School Information Management System (SIMS), an externally developed package supplied by Capita Education Services and used by many schools. School staff believe SIMS to have 'secure connections', but upon investigation with Capita Education Services it was found that SIMS does not include facilities to electronically send information to other agencies, secure or otherwise. Such transfers use the normal e-mail system of the host school. The school has an acceptable use policy for pupils and staff, and a document in the staff handbook with guidelines for e-mail use, discouraging the transmission of sensitive pupil information by e-mail.

The national retailer does not employ any e-mail encryption because it is thought to be too complex to implement. The company has an internal policy and a computer user agreement which states that no sensitive data should ever be sent using e-mail. Some form of secure storage is used for static documents to prevent compromise, but no considerations are made for e-mail messages.

The legal firm forms policies in response to recommendations by the Law Society of Hong Kong, which introduced a voluntary e-mail encryption scheme in September 2005 but has since withdrawn support for unknown reasons. The legal firm has never used any kind of e-mail security and does not intend to unless clients specifically request it. This client led approach relies on the knowledge of the clients to actively request e-mail security, without consideration that the clients have no knowledge of e-mail security, or that they wrongly assume measures are already being taken.

Cost of Using Security

The information security manager at the NHS believes that there is definitely a need for more security than is currently in use within the trust, but states that the main obstacles to this are cost and usability. For example it is estimated that password management software would cost £53,000 to implement for a single Trust. In a cash-strapped organisation such as the NHS the monetary cost of implementing a new system is a very important consideration, especially when funds are required for other projects which have a greater impact on public image, such as staff training or medical equipment. The possibility of adopting a public key encryption scheme has not been

examined because NHSmail has already been implemented as a partial solution, although it sees limited usage.

In common with many organisations, the Metropolitan Police desire the ability to inspect encrypted e-mail traffic for malicious code and to detect staff misuse. Ideally, traffic should be decrypted at the e-mail gateway, inspected, then re-encrypted, but this is a complex process that would best work with PKI. There are some products around such as SecretSweeper from Clearswift, which allow inspection of encrypted content but there are currently no plans to implement this technology. The costs in terms of monetary outlay, processing overheads and time to implement and send individual messages are thought to be too large to tolerate in current solutions.

Similarly, inspection of messages is important for the university, who would require detailed investigation of the time overhead problem before any investment would be made in encryption. It was believed that the encryption of e-mails would impede access to them too much to tolerate. In order for an e-mail encryption scheme to begin at the University, e-mails would have to be comprehensively retrievable and decryptable by an authorised discovery agent, with manageable effort. There would also need to be full and un-tamperable audit trails of any encryption and decryption with manageable reporting tools, which currently incur unacceptable time overheads.

Software Usability Problems

The FSA has a policy of technological neutrality, meaning that the FSA will not discriminate on the basis of the delivery channel alone (unless its statutory objectives would be otherwise compromised). Nor will they advocate a particular method of communication, or security for that communication (FSA, 2001), leaving the choice of software up to its member organisations. The variety of software available to implement encryption, and the different standards and levels of security each offers can be a confusing choice for organisations, especially when no recommendations are given by policy makers.

Flaws were reported with the NHSmail system which covers the entire NHS, including GPs. One of the most noticeable of which is that the software is much slower to use than the alternative desktop e-mail clients such as Microsoft Outlook. The North Hertfordshire NHS Trust ran a trial in which all its staff used the NHSmail system, but they soon returned to using the previously used Novell client due to the many difficulties encountered. During its limited use throughout the various trusts, these same problems recurred again. Staff complained that they had to keep up to date with two sets of e-mail addresses, so they abandoned their NHSmail e-mail account and focused on their original e-mail address. Staff were also frequently locked out of their accounts due to the high level of security; even the IT manager and the Information Security manager were

both locked out of their accounts on several occasions and found it difficult to regain access due to the high security required to reset them; some of the less technical users found this process impossible. The passwords used have stringent quality controls to increase their security which has caused many problems with staff forgetting their passwords and has placed a large burden on administrators to reset them. Problems have also been identified with systems being left logged on in public spaces to avoid the inconvenience associated with multiple secure login sessions.

NHSmail is incompatible with the current Novell group ware system which is in wide use and does not provide as good a diary system as Novell, which staff use extensively to plan meetings and events. Furthermore, contacts must be imported from the desktop mail client, typically resulting in staff trying to keep two separate systems up to date.

Significantly, the system was not well promoted and awareness of it is very low. In fact the security manager believes that most hospital staff would not know what NHSmail is if asked. The system was designed to be used mostly by doctors so other staff that would benefit from using it are not aware enough about it. As it is optional to use and requires signing up, it requires a strong motivation to use. Although the system could be made mandatory, this is not seen as a priority because the current set up has never been cause for alarm so there is not seen to be a need to change current practice. Additionally, a complete transition to NHSmail is estimated to take around 4 months for every 5000 users. Staff resistance to such a change is thought to be very high as there would be a need for staff to be retrained and have new passwords issued.

Forgotten passwords account for 20% of the NHS Trust IT helpdesk's annual calls, representing over 4800 calls. Most users have dozens of passwords for the various NHS systems, including Novell and NHSmail, in addition to even more passwords for the sub systems they use such as clinical systems. One possible solution that has been looked at is provided by Imprivata and is called 'SSL Single sign on'. This will store users passwords in an AES 128-bit encrypted server so they can use a single sign on and their other systems will automatically be logged in for them. Another password related problem is that users have been observed to share passwords, in order to avoid the hassle and waiting time required for continually logging in and out of the same shared PC throughout the day. The impact of this practice is two-fold: Firstly, it means that if a user is left logged on there are many opportunities for unauthorised access to restricted information. Secondly, it makes auditing difficult, for example, in a case where a blood test is misdiagnosed on the system, the person responsible for this mistake cannot be reliably traced because many people have used the same login ID.

There is currently a trial ongoing of an open source on the fly encryption software called TrueCrypt, which seems so far to be much easier to use, than NHSmail. However other problems have emerged, such as members of staff forgetting to encrypt a message and sending it in plain

text, but thinking it had been sent encrypted. Keith James believes this system would not see widespread use other than occasionally encrypting data onto CD-ROMs.

PKI is also on trial and currently available for use within the trust, but it is rarely used by a limited group of people. This system uses Novell Network to generate its own certificates; however both the sender and recipient must have been set up to communicate securely. This process is time consuming and confusing and is only used for the most sensitive data for example if a secretary needs to send sensitive patient identifiable information to a consultant.

For Anadarko, the main identified issue with e-mail encryption is key management; there are concerns that whatever system is chosen must work with a variety of e-mail clients both under the control of Anadarko and of other companies, and must also cope with secure key management when people join and leave. This is seen to be problematic, but if this issue could be easily overcome, then Anadarko would implement an encryption scheme as well as Digital Rights Management (DRM) systems and utilise these to protect access to and use of sensitive data over e-mail. Anadarko examined the possibility of using a DRM system, but found that a small software installation was required on the client in order to read a document. This is not always possible on other companies' machines where policies dictate allowed software, nor would it be possible on non-Windows machines. Anadarko feels that for this reason the technology is not yet mature enough, and extends this belief to encryption technologies. It is felt that the benefits of adopting e-mail encryption are outweighed by the costs of doing so, however if this situation were to be reversed, encryption would certainly be considered.

The legal firm have never used e-mail encryption but did indicate that they would adopt the technology if requested by a client, and if the software was easy to use.

Social Factors

Within the NHS, many of the staff have very low IT skills with many requiring basic training, such as that offered in the European Computer Driving License when first beginning their job. However it is still easy for them to get confused over new technology and to forget passwords and procedures. Many staff are also resistant to change, especially if they have been working with paper based records for many years. The national project for IT in the NHS is the world's biggest IT project and is phasing in many new computer systems. The introduction of such complex new IT systems means that staff require re-training, and often results in changing working practices. The introduction of e-mail encryption is one example in which the security manager believes the staff are expected to be more pro-active and quickly learn new skills. This combined with the low usability which has been observed has impacted on the overall security of e-mails.

It seems that many companies develop their policies to comply with their regulatory bodies recommendations, such as those issued to financial organisations by the FSA. The FSA seems to make policy amendments to comply with UK law; however there have been no specific provisions for e-mail security. As such, it is left down to each institution to enforce their own information security policies, if they exist at all, without specific guidance from the FSA. As was observed in section 2.6.3, the legal requirements relating to information security can be confusing and do not always exceed the bare minimum for secure communication, so without specific guidance from regulatory bodies it is understandably difficult for organisations to implement effective information security policies.

As the stock broking organisation has reached a large size, they have now considered the option of using security in the future; however they noted that encryption is very rarely used by any similar organisations in the industry.

Knowledge and Belief Factors

In the MPS, staff have various methods available to send electronic messages, one of which is the CJX. E-mails sent to an address with a '.pnn' suffix are automatically and transparently secured, an excellent step towards removing the burden of security decisions from the user. However not the entire burden is removed, as staff must understand that they should not e-mail "protectively marked" (sensitive) material over the internet unencrypted. This requires staff to judge firstly whether their e-mail messages are sensitive and secondly whether the message will travel along a secure route. The fact that the encryption process is transparent but only occurs when .pnn suffixes are used can make this job difficult as staff without the correct knowledge may assume that all messages will be sent securely.

In the IT consultancy, the technology was seen by staff as difficult to use and unreliable. There is currently a review to decide on the future needs of data encryption, but the main barrier that was foreseen was the effort required on both the client and the customer side of the communication to set up a digital identity, and the technical and social problems which have been experienced in the past with this process. Furthermore, the perception that zipping and password protecting data is completely safe (although it is not) has resulted in a lack of interest in using widespread encryption.

There is a belief in the stock broking organisation that e-mail security is not a necessary requirement and that secured e-mails could be potentially unreadable by the recipient's software. Little understanding was shown of the nature of encryption, or how it could be implemented to their advantage.

At the secondary school the IT staff did not fully comprehend what encryption is, whether or not it was needed, or how to implement it. However they expressed a desire to learn more about security and an inclination to implement it where feasible. It seems that lack of awareness played a large factor in this setting, as it did with the general public. The only e-mail security policy in force is one which encourages staff to mark sensitive e-mails with the word 'CONFIDENTIAL' in the subject line. It is believed that this somehow increases the recipient's diligence with handling the mail although obviously it does not affect any external security breaches, in fact it may even draw the attention of potential hackers to the messages in question.

In the Hong Kong legal firm e-mail security is not used because it is believed that the e-mails will not be attacked in transit. The source of this low perceived risk is based on assumptions about technology and on the lack of incidence in the past. This illustrates that experts in a particular domain (law in this case) should not be expected to hold expertise in the threat models of e-mail in order to secure their communications.

4.2.3 Summary of Barriers to Adoption

When comparing the information discovered in these interviews with the data collected in the surveys with the public, the issues fall into very similar categories, but with a different focus and level of importance. Lack of awareness was a big problem on both sides, with many people not even knowing of the existence of e-mail encryption. Amongst organisations monetary cost was an oft-cited concern, whereas this was of little concern to most individuals. The belief system of individuals and organisations shared many similar issues, but highlighting their differing needs. Many individuals stated that their information was not worth protecting and that they did not care if anyone could access it. Amongst organisations this was not often the case, although they did believe that security is not always necessary within the organisation and that most security threats lie outside the organisational network. Social factors play a large part in an individual's decision to adopt a technology, for example, how many of their peers use it and how prolific it is in society. Organisations, particularly the smaller ones, were seen to use similar reasoning, such as examining how many of their peer companies use the technology and whether use of the technology is deemed necessary by policy or law.

4.3 Discussion

The data collection from some organisations was partially unsuccessful in that the organisations were reluctant to allow access to, or divulge data sources related to security. This presents a type of feedback loop whereby when analysing security, the things people are worried about are the security of the analysis. For example, the RBS although providing some useful information on

their security policies, would not allow interviewing of their staff, instead responding to subsequent e-mail enquiries with “Unfortunately, we are unable to assist you with your research.” This type of response again illustrates the issue of personal liability (see section 3.6) where the necessity to examine the use of sensitive information is hindered by the respondents’ concerns for and uncertainty of the consequences of their actions. This is a factor which is slowing the improvement of security technologies.

The information gathered from UK organisations shows that large quantities of sensitive data are handled electronically, giving a strong case for the widespread use of e-mail encryption. However, in practice the use of e-mail encryption that has been observed is extremely low across the board. The metropolitan Police Service in particular however, have adopted good security measures despite the lack of a PKI implementation. This is reassuring considering the large amounts of highly sensitive data that is dealt with. A variety of reasons were offered for the low adoption of encryption, from lack of awareness, to lack of faith in the reliability of the technology, to awkwardness in using the software. Although encryption technology is very well established, it seems to be met with a high level of resistance across the board.

It was found that for organisations, the major barriers to adoption were cost and usability issues, such as the complexity, speed and reliability of the system. Whilst for individuals, the main barrier was a lack of awareness of the technology. According to the Diffusion of Innovation Theory (Rogers and Scott, 1997) , awareness is the first of five stages of adopting a new technology. If the user is not aware of a system, they cannot gain interest in it, evaluate it, or use it. Certainly the technology of e-mail encryption needs to have greater publicity to increase its awareness, as the survey also showed that most people were keen on the notion of encrypting their e-mails. However, it may be that if the stage is reached where e-mail encryption is being used widespread by individuals, they may then begin to encounter some of the usability problems which have been identified by organisations and in the previous literature. As cost was one of the major barriers to adoption for organisations, so it may be for individuals, as most people indicated that they did not know what the cost of encryption might be, but that they would assume it to be free.

Within the NHS, NHSmail sees significantly less use than was expected despite being in its 4th year of operation. The information security manager believes that there is a definite need for more security than is currently used within the NHS due to the sensitivity of the data involved, as well as compliance with regulations such as the Data Protection Act and the Cauldicott principles. The current use is believed to be so low due to the low usability of the systems causing confusion amongst staff who have limited I.T. knowledge. The acceptance to new systems also tends to be low due to lack of I.T. skills, lack of understanding and resistance to change of working habit. It is believed that the perfect security solution would be totally transparent, with no extra actions for

the users to take. Security requirements are very high for the hospital; however a compromise resulting in less security for more usability expressed as preferable. Secrecy is the most important aspect of security for the hospital, authentication and non-repudiation are not considered very important, but integrity is important for sensitive data. The NHSmail system is technically very secure, but not very usable with frequent lockouts requiring help desk to reinstate users. Having excellent security is technically achievable and has proven and widespread benefits for an organisation such as the NHS, but being the UK's second largest employer the implementation project would be massive, the cost could be high and importantly, the usability is believed to be too low for it to achieve success.

The IT consultancy cited low cost and ease of deployment as the two key factors which would initiate further interest in deploying encryption.

Many Companies seem to be unaware of standards (e.g. ISO 17799; The British Standards Institute releases information security policies relating mainly to access control) and legislation (e.g. (Export Control Act 2002), Sarbanes-Oxley Act) regarding the use of e-mail encryption, which is unsurprising considering the vast myriad of documents available and the difficulty in accessing and understanding them.

The security practices of the organisations sampled are based on assumptions, including:

- E-mails are inherently secure
- There is no threat of attack
- Connections are already secure (e.g. SIMS)
- An organisations clients understand security and will request it when they want it (e.g. the law firm)
- If a security technology is introduced it will be used by staff (e.g. NHSmail)
- Policy makers will advocate security if it is necessary

This final assumption may be leveraged to improve the problem by encouraging external policy makers such as the FSA to create policies advocating the use of e-mail security, giving instructions on how to do so. It is likely that organisations would follow this advice if the cost of doing so were not restrictive.

The above assumptions, along with the general observations of this chapter strengthen the relevance of PLaGUE (introduced in section 3.6), which is that people's liabilities, responsibilities and attitudes affect the way they use security. Firstly, some of the organisations examined felt a responsibility to protect the security of information about their security policies, which

paradoxically hinders the potential to develop and improve their security. Secondly, users in the public domain clearly expressed that they did not feel liable to provide strong protection of their own data, instead placing this responsibility on others including ISPs and employers. This contradicts the beliefs of security software developers, to the extent that the security software they develop seems to require the users to accept full liability for protecting their data. Furthermore, some of the issues which were attributed to the low adoption of e-mail encryption were traditional user interface problems, and as such definable in traditional usability terms. Other problems, such as the very low awareness of encryption, stem from the mental models created by users and developers, and whilst they affect the usability of the software they do not accurately fall into traditional usability terms, hence the use of the term PLaGUE to conceptualise such problems. The users interviewed seemed not to accept or be aware of responsibility on their part to increase their awareness, and since e-mail encryption has such potential to combat security threats it is unclear why it has not been promoted sufficiently by software houses or the government.

As was previously elaborated, this chapter has identified several usability issues with the use of e-mail encryption. Of these issues, it was chosen to further investigate that of remembering passwords. Passwords are ubiquitous with wide spread applications; yet suffer from the well-reported usability problem that a secure password is difficult to remember, whilst an easy to remember password is not secure. Little research has been performed to suggest ways of improving this situation, so the following chapter suggests one such method and evaluates it.

Chapter 5: The Dichotomy of Passwords

5.1 Introduction

Passwords are one of the most widely used security mechanisms and to be secure they must be complex. The notion that users find it very difficult to remember complex passwords and therefore compromise security by choosing weak ones has repeatedly emerged in both the literature review and interview case studies.

The premise behind this study was to find out if passwords constructed in a certain way would be easy for users to remember in the long term, and whether numeric only passwords had better memorability than alphabetic only passwords. To balance usability and security the 'Chip & PIN' (Jones, 2005) system introduced to UK banking was used as a frame of reference for applying the 'three attempts and you're out' approach.

Although there are many software tools available which offer users the chance to have their passwords automatically recalled, such as that built into Microsoft Internet Explorer, or Just1Key from HushMail, these can pose a big security threat in that breaking this one system would yield passwords for many systems. These memory aids can also be inconvenient given that the user is not always allowed to access to their passwords when travelling or using a different computer.

An experimental approach to investigating alternative ways of producing passwords which may be easier to remember is reported below. It is hypothesised that being easier to recall (thus easier to use) will increase the effectiveness of the password in practice.

A pilot study was run with five participants to gauge any unforeseen complications and to improve the subsequent main study. The pilot study made it apparent that participants may not all login on the day the e-mail is sent to them, so a calendar was used in the main study to carefully monitor the login timings and ensure they were correct for each participant.

5.2 Participants

The study used an independent subjects design with 50 volunteer participants, 20 of whom were postgraduate computing students at Brunel University in London, with 30 having been recruited through word of mouth from outside the University. There was no desired demographic for the experiment as the test group should represent password users in the wild, having a range of experience and age. The age range was 19-53 and the gender split was 65% male and 35% female. The participants were informed that the nature of the study was to assess how memorable different types of password are. They were split into two groups, each consisting of 25 participants.

Passwords in group 1 consisted solely of digits from 0-9. These passwords are referred to as numeric passwords. Passwords in group 2 were constructed solely of lowercase alphabetic characters from a to z. These passwords are referred to as alphabetic passwords. For fairness of test all passwords were pseudo-randomly chosen to form a unique password for each participant. Four participants in group 2 failed to participate, so only the remaining 21 participants were included in the study. The option of changing passwords was introduced to half the group to see if a self-chosen password really performed better at retention than an issued password. Therefore each group was further subdivided into two halves; those who were given the option to change their password at the beginning of the study (groups 1a and 2a), and those who were not (groups 1b and 2b). Gender and age groups were assigned evenly to each group. In group 1 (numeric) the gender split was 65% male 35% female with an age range of 21-53 and in the group 2 (alphabetic) the gender split was 67% male 33% female, with an age range of 19-53. Participants in groups 1a and 2a were only allowed to change their password, if they wished to do so, when their password was shown to them, on day one of the study. Self-chosen passwords were constrained to be exactly six characters in length and of the same category as their original password (either all numbers or all letters).

5.3 Procedure

The main experiment was designed to test the differences in memorability, if any, between the two types of specifically constructed passwords.

The null hypothesis for this experiment is that there is no difference in the durability of retention between numeric and alphabetic passwords. The hypothesis is that numeric passwords will be more memorable.

Passwords consisting solely of numeric or alphabetic characters have lower entropy than a password that uses a mixture of letters, numbers and symbols and would therefore be much faster to crack using a dictionary style attack. However, this threat can be greatly reduced if used in conjunction with a 'three strikes and you're out' approach. It is arguable that such a system would incur significant unnecessary support costs for resetting accounts in cases where users would have correctly entered their password on the fourth or fifth attempt, but were not allowed the opportunity to do so. However, should a particular type of password turn out to be more memorable, it should follow that most users will not exceed three login attempts, in which case support costs will not be higher than those currently seen for forgotten passwords. Furthermore, it has been documented (e.g. (Orgill, *et al.*, 2004)) that social engineering attacks (leveraging trust to obtain information) have recently become a greater threat than technical attacks. In these

situations, long and complex passwords do not offer any more protection from being socially extracted than shorter, simpler passwords.

The study by Zviran and Haga (1993) asked participants to login only once at the end of a 90 day period. This makes it impossible to determine the exact point at which participants forgot their password as it could have been at any point during the 90-day period. Furthermore, the password use in real world applications is likely to be at various more frequent intervals, so the study by Zviran and Haga did not accurately represent real use of passwords. To improve on this multiple logins were used in this experiment at various times over 108 days.

Rather than spacing the logins equally apart, the periods of time between each login were made successively longer. The reason for choosing such time intervals was to allow analysis of how the length of time of non-use of passwords impacts the password retention. This timing was also used to avoid the memory phenomenon known as the recency effect, whereby frequently recalled items are easier to remember than infrequently used ones, whilst retrieval of very frequently recalled items becomes 'automatic' (Sasse, et al., 2001). This phenomenon may have been encountered if the login periods were more frequent and equally spaced. The timings used are shown in Table 1.

To facilitate this study, a bespoke web site was created using HTML and the server side scripting language ASP, which linked to a Microsoft Access database. Mail merging was used with Microsoft Outlook to automate the sending of customized e-mails to the participants. A website was made to mimic the context for logging in which is felt to be more representative of similar websites today than the voice-mail system used in the study by Sasse et al (2001).

At the beginning of the study, an e-mail was sent to each participant asking them to visit a sign-up web page where they had to enter their age, gender and e-mail address and indicate any learning or memory difficulties which may affect the experiment. After this, each participant was shown a password on screen and was instructed to memorise it without writing it down and to treat it as they would any other of their passwords. In the case where participants usually write down their passwords, this would be identified in a follow up questionnaire. All of the passwords were dynamically created using a pseudo-random JavaScript generator.

The participants were sent e-mails after the time periods indicated in Table 5.1, with the first login being within one day of the password being issued. Each login request asked the participant to visit a URL and enter their password. To simulate the 'three strikes and you're out' scheme described above, participants were not allowed more than three attempts to correctly enter their password. Each login attempt was clearly labelled on the web page so that the user was well aware of how many attempts they had remaining. If they were unable to correctly enter the password in three attempts, they were thanked for their help and disqualified from the remainder of the study.

The number of attempts taken to correctly enter the password, the period of time which had elapsed since the last login and disqualification data were automatically recorded in the database for later analysis.

Table 5.1 Days on which participants were asked to log in with their password

Number of days from start of study	0	3	10	24	45	73	108
Number of days since last login	0	3	7	14	21	28	35

As the database recorded both the length of time the password was remembered for and the number of attempts required to correctly enter the password, both the durability of retention and the accuracy of retrieval can be measured. The speed of password entry is not considered important for this experiment and was not measured. The amount of effort participants put into memorizing their password may affect the outcome of the study, for example, if a participant is apathetic to the cause of the experiment they will take less effort to memorize the password. Although this factor is outside the control of the experiment, it was measured using a short exit questionnaire, which was also used to gather qualitative data on the ease of learning of the password and the technique used for memorizing the password (including the use of written notes).

5.4 Results

Only four participants managed to remember their password for the whole duration of the study (108 days). Interestingly, five participants failed the first login, which was issued immediately after they were given a password. In the exit questionnaire, three of these participants indicated on a four-point scale that they tried their very best to remember the password. One participant used moderate effort and one used low effort. A four-point scale was used to remove the neutral option and force either a negative or positive answer regarding the amount of effort used to remember the password.

Of the 23 participants who were allowed to change their password, only 11 chose to do so. There seemed to be a tendency to choose easily guessed passwords. Four passwords were changed in the alphabetic category, of which three were changed to dictionary words and one was changed to the participant's first name. Of the numeric passwords, one was changed to '111111' and one was changed to the date on which the participant first received their password, but the rest had no discernable pattern.

As the login requests were issued in increasing time intervals, it is impossible to determine the exact point at which a password is forgotten. For example, if a password was successfully recalled after 10 days, but the recall was unsuccessful on the login on day 24, then the password was

forgotten at some point between 11th and 24th day after it was issued. Therefore, when calculating the average successful password recall times the mid point was used, which in the example above would be 17.5 days.

Using this method, the mean number of days passwords were successfully recalled for is 28.4 for alphabetic passwords and 31.1 for numeric passwords. The immediate recall was more successful for numeric passwords, with 96% of numeric passwords being successfully entered on the first login, versus 81% of alphabetic passwords. The Mann-Whitney U non parametric statistical test was used to calculate the significance of this result. The Mann-Whitney test yielded a U value of 280.5, which is above the critical value of 173 at the $p \leq 0.05$ level, therefore the result is not significant and the null hypothesis cannot be rejected.

In the following table the % refers to the percentage of participants remaining in the group after disqualifications from the previous round.

Table 5.2 Successful recall of all passwords

Days since password issued	Days since last login	Number of successful logins	Success %
Passwords Issued	Passwords Issued	46	-
0	0	41	89
3	3	35	85
10	7	26	74
24	14	24	92
45	21	7	29
73	28	6	85
108	35	4	66

Despite the lack of statistical significance for the main hypothesis, the experiment yielded some interesting findings. Tables 24 show the successful password recall across all groups where the first row in each of these tables shows the total number of passwords issued for the category. The first login was immediately after the password was issued. Of the 23 participants who had the opportunity to change their password, only 11 did so. In all groups the recall success dropped dramatically between the logins on days 24 and 45, highlighted in bold in the tables, from 92% of all remaining participants to 29%.

As the time intervals between logins grew increasingly longer, it was possible to analyse how non-use of a password affects the recall. At the point of login on day 24 of the study the password had not been used for 14 days and only two participants failed to login.

Table 5.3 Successful recall of issued passwords (this includes all participants who had no option to change their passwords together with those who had but did not exercises this option)

Days since password issued	Days since last login	Number of successful logins	
		Alphabetic passwords	Numeric passwords
Passwords issued	Passwords issued	17	18
0	0	13	17
3	3	11	13
10	7	8	7
24	14	8	7
45	21	3	3
73	28	2	3
108	35	2	2

Table 5.4 Successful recall of self-chosen passwords (this includes only the participants who had an option to change their passwords and who exercised this option)

Days since password issued	Days since last login	Number of successful logins	
		Alphabetic passwords	Numeric passwords
Passwords issued	Passwords issued	4	7
0	0	4	7
3	3	4	7
10	7	4	7
24	14	3	6
45	21	0	1
73	28	0	1
108	35	0	0

At the next login on day 45 of the study, when the password had not been used for 21 days, the number of login failures rose to 17. The participants who did successfully login on day 45 required an average of 1.7 attempts, up from an average of 1.1 attempts on day 24. The success

rate dropped considerably between days 24 and 45, but then increased again after this period. This indicates that for most participants the successful recall of the password becomes much more unlikely after 15 to 21 days of non-use.

With casual observation, it seems that those who did not change their password performed better, as four people using the issued password were able to recall it after the full 108 days, versus 0 people using self-chosen passwords. However, as would be expected, participants who were allowed to change their password at the start of the study to the one of their choosing (within the constraints for their group – i.e., numeric or alphabetic) performed better overall. Statistical analysis showed that self-chosen passwords were remembered significantly longer than issued passwords ($U=118.5$, $N_a=11$, $N_b=35$; Mann-Whitney U test). However the number of successful logins dramatically dropped from 9 on day 24 to 1 at the next login on day 45 (see table 4). In interviews it was indicated that the reason for this was that the password was confused with one of the many other passwords in use, so it would have taken more than the three allowed attempts to successfully guess the correct one.

For both alphabetic and numeric password groups, the female participants consistently performed better at each login than the males, remembering their passwords for an average of 35.4 days versus 27.0 days for males, although this was not statistically significant. Participants aged 25 or younger, performed better with alphabetic passwords than those over the age of 25. Their success rate for the first login was much higher than for over 25s and they were able to recall the password for an average of ten days longer, although again not significant in the Mann Whitney analysis. There was no such age related disparity in the performance for numeric passwords.

5.5 Discussion

In the exit questionnaire 23 of the 46 participants said they found the password quite easy to remember, which is surprising as only four participants managed to remember their password for the full duration of 108 days. Only eight participants found their password very difficult to remember. The main cause for login failure was said to be confusion and transposition with other passwords or strings such as telephone numbers, rather than complete failure to recall the password.

When asked to identify the method used to memorise the password the most popular answer, with 16 responses, was that no method was used. Eight participants used an acronym system whereby they made up a phrase using the characters of the password – six of these participants had alphabetic passwords, whilst two had numeric passwords. Eight participants, all of whom had a numeric password, said the password just ‘stuck in their mind’.

Participants were asked to indicate how much effort they put into memorizing their password in order to gauge whether apathy could have affected the results. 18 participants said they tried their very best and a further 17 participants said they used moderate effort. Only eight participants said they used little effort and three that they used no effort to remember their password.

As has been widely observed elsewhere, participants in the study had great difficulty remembering passwords for long periods of time. Numeric passwords were remembered for three days longer on average than alphabetic passwords and all eight participants who said their password stuck in their mind had a numeric password. Recall was slightly more successful across both groups where the participants were female under the age of 25. The lack of statistical power for this result means that there is no evidence for password issuers to change their current password allocation methods.

In corroboration with previous literature (e.g. [10]), the main cause of login failure was reported to be confusion between passwords, for example, entering all or a part of a password from a different system, or transposing digits with those from familiar phone numbers.

The period of non-use, which had the greatest impact on recall, was between 15 and 21 days, during which time 70% of remaining participants forgot their password. This was an unexpected result, which extends current research into password retention. Systems where users login infrequently, such as websites that require registration, may benefit from using a memory jog specifically aimed at users who have not logged in for 15 to 21 days to increase long-term retention of the password. Further research can be used to narrow down this period and to test the effectiveness of such a memory jog system.

When given the opportunity to change their password to one of their choosing, but fitting within the constraints of their category, few participants did so. Of those who did, many chose an entropically weaker password that would be easier to guess, particularly those in the alphabetic group. Recall of self-chosen passwords was significantly better, despite the fact that nobody with a self-chosen password remembered their password for the full 108 days, versus four participants using issued passwords. Participants using self-chosen numeric passwords remembered their password for 10 days longer on average than those using self-chosen alphabetic passwords. As only 11 participants chose to change their password, further studies are required with more participants to confirm these results.

Participant recruitment was found to be difficult. No incentive was offered because an incentive based on performance at password recall would provide excellent motivation to memorise the password, but would not be appropriate as it would also increase the motivation to use 'cheats' such as written notes to ensure receipt of the prize. An incentive offered at the end of the study

may seem too far away to offer immediate benefit, or may result in apathy towards memorizing the password, as the reward is sure regardless of performance. Although lack of incentive impeded the recruitment of participants, it did not seem to affect their motivation, as most participants indicated that they tried their very best to remember the password and only one person admitted to using a written note as a prompt.

Although future work into usable authentication may focus on emerging alternatives such as biometrics and graphical passwords, it felt that traditional passwords remain worthy of equal research due to their maturity and penetration into our culture, and the possibility of usability improvements with have yet to be discovered.

Using more participants in future studies would confirm these findings as statistical power is increased with higher numbers of results. Setting up a similar experiment can easily be done using a web site to recruit and test participants over the Internet, if the methodology of using participant honesty to monitor 'cheating' (written notes etc) is acceptable.

The difficulty in participant recruitment for longitudinal studies can hinder similar studies, and it is necessary to assess how best a framework of incentives can be applied to such a study without biasing the results.

5.6 Summary

The purpose of this experiment was to discover if passwords constructed in a specific way would be easier to remember. All-numeric passwords were found to perform slightly better than all alphabetic, but not significantly so.

A strong link was found between recall success and the period of non-use – many participants in all groups of the experiment forgot their password when they had not used it for between 15 and 21 days. It therefore seems a good idea to issue some kind of reminder if users do not login for 15 days.

When given the option to change their passwords few participants chose to do so, but those who did, performed significantly better than those who were using issued passwords, even though their chosen passwords were constrained to be either all numeric or all alphabetic. This improved performance for self-chosen passwords was not evenly distributed. Specifically, successful recall using self-chosen passwords was excellent to begin with, but nil after the full 108 days, whereas in the issued password group, overall performance was very low, but four participants still managed to recall on day 108.

At a conceptual level, the issue of PLaGUE (see section 3.6) is relevant to the password problem discussed in this chapter as it can be used to identify the liability placed on end users to remember

their passwords, or else risk undermining the security of their data. But as we have seen in chapter 4, not all users place sufficient worth in their data to warrant the effort required to remember numerous complex passwords, despite valuing their security. This increases the difficulty of the developer's job in securing data that they know to be valuable but which the data owner does not. This study has suggested and evaluated a low level method of improving password use to improve overall security, based on the notion of PLaGUE which has identified that the balance of responsibility between developer and user should be altered to make the use of passwords easier and therefore increase overall security. It is suggested that thinking in terms of PLaGUE will eventually allow a higher level solution to be developed that can address the balance of responsibility to more accurately reflect the actual responsibilities implied or perceived in real use.

The usability problems with security have now been identified at a broad level in chapter two, principles to improve them evaluated in chapter 3, the specific case of e-mail encryption addressed in chapter 4, and a method to improve the usability of passwords proposed and evaluated in this chapter. The following chapter synthesises the findings of this research as a whole.

Chapter 6: Usable Security – A PLaGUE on Both Houses

6.1 Introduction

In section 3.6 the term PLaGUE was introduced to stand for Personal Liability and General Use Evaluation. The literature first hinted at the importance of considering each party's responsibilities to achieve usable security; early research accused the users of doing something 'wrong' which caused them to fail to keep their systems secure. Later, the addition of usability principles to the security sphere recognised this blaming mentality as wrong since the software did not allow the users to perform well. But still lacking is research that identifies and analyses the liabilities and perceived liabilities of both developer and user, to understand how these may affect the use of security in practice. Without this, the expectations placed on both the user and the developer in how to address security may be inaccurate, leading to usability problems.

The thesis comprised three studies, each leading from the previous, which viewed the problem from different angles. Each of the studies used a different methodology to highlight evidence of the importance of usability in achieving good security. The relevance of PLaGUE was identified in each case, along with other usability issues. This chapter will synthesise the findings of the thesis in order to apply them to the research questions formulated in chapter 2, discuss recommendations to the general domain in terms of PLaGUE, and conclude with a summary.

6.2 Research Findings

The findings of the research are presented here in relation to the research questions posed in section 2.7.1.

Table 6.1 Research findings of thesis

Research Question	Related findings
To what extent has recent research been successful at aligning usability and security in practice?	<ul style="list-style-type: none"> • Both security and usability must be considered from the beginning of the development of software or it is unlikely that they will both be equally effective. • Pop up error messages do not aid users in completing tasks. • Users like visualisation to increase their awareness of the state of security. • Users find it difficult to complete customisation of software. • Users find it difficult to make trust decisions

	<ul style="list-style-type: none"> • Users have an incredible amount of apathy towards the security of their data. Education would not seem to improve this because users will even knowingly compromise data to get tasks done faster. • Polaris may be improved by automatically creating a segregated disk area for each new application, and subsequently deleting that area after use. • Collaboration between functional and security software developers using a combination of use case and threat model is needed to address the task-attribute nature of security.
Is e-mail encryption as underused as the literature has suggested, and if so, why?	<ul style="list-style-type: none"> • Very few members of the public sampled have ever used encryption, or know someone who has. • Most do not consider themselves technically proficient enough to use encryption.
What proportion of e-mail users have successfully obtained a digital certificate?	<ul style="list-style-type: none"> • The public value their privacy yet very few have digital certificates. Interest in adopting encryption is high, but knowledge of how to do so is low.
What mental models are held by individual e-mail users, and businesses of e-mail encryption?	<ul style="list-style-type: none"> • A majority of the public expect that digital signatures should be issued by default by providers of their e-mail service. • There is a very low awareness of the meaning of encryption, or how it can apply to e-mails. • Organisations tend to be reluctant to implement e-mail security unless it has first been recommended by external policy making bodies. • Organisations show confusion over how the law applies to secure e-mails, and see abstinence as the safest option. • As with the public, organisations see speed of completing tasks as paramount and are unwilling to invest extra time for extra security. • Some organisations see the divulging of security information to be dangerous when in fact it can be used to improve security to a much greater extent than to launch an attack.
Is there a way to ease the memory burden on users of traditional passwords?	<ul style="list-style-type: none"> • Social engineering attacks are becoming more prevalent and cannot be prevented by high entropy passwords. So it may be favourable to use easier to remember non-dictionary passwords even if these are less complex. • Self-chosen passwords facilitate better recall in the long term than passwords which are not chosen by the user. • Most users forget their password after 15-21 days without using it.

The recommendations resulting from these findings are presented below, grouped by the issue that they address. Each recommendation is accompanied by a recap of how it came about

6.3 *PLaGUE in Software Development*

Perhaps the most striking discovery of chapter 4 is that despite impressions to the contrary in HCI-SEC research, people generally do care about security, but do not feel completely responsible for it. However most security software is not designed with this in mind: Polaris (evaluated in chapter 3) mandated certain actions of the user to ensure that they acted securely; E-mail encryption has not been promoted and suffers very low awareness considering its maturity, the reasons for this are unknown, but it is plausible that it is not seen as desirable to the public. Evidently security software developers did not expect people to care about security, underestimating the fact that acting insecurely is not necessarily an indicator of contempt for security, but an indicator that the responsibilities of security have not been properly allocated. In many cases it is not that people do not want security; it is that they do not want it to hinder their task completion. To compensate for this, it is recommended that usable security research considers a PLaGUE style approach to understand the user's mental models of security, including those formed before use of the system, and their perceived responsibilities to security:

Identify the user's perceived liabilities and compare with the developers perceived liabilities

An objective of the thesis was to evaluate how successful the application of usable-security principles has been in practice. To accomplish this, a usability study was made of software using these principles with the specific aim of being simultaneously usable and secure. Several usability issues were discovered, one of the less superficial of which was that the software had been designed post-hoc and thus was restricted to operating in pre-defined ways. Previous research has shown that security (Halkidis, *et al.*, 2004;Kis, 2002) and usability (Faulkner, 2000;Nielsen, 1993) individually benefit from being considered early in the software lifecycle, and continually assessed from that point onwards. However the same findings have not been applied to both security and usability in the same piece of software. The usability study of Polaris showed that although best effort was made to formulate usability and security into a post hoc add on for Windows, this end result did not satisfactorily meet the goal of being highly usable and secure. The developer should therefore be liable for assessing the unique needs of usable security throughout the entire software lifecycle:

Integrate security and usability into software throughout development

To support the previous two recommendations in accounting for user behaviour, it is necessary to be mindful of the evidence collected during the usability study in chapter 3, and the interviews in chapter 4 which identified that although users understand the importance of security they are unwilling to invest much effort for this security. Users see the liability of file protection as lying

outside of their responsibility. By making the default mode of operation as secure as possible the amount of investment in security required by the user is minimised:

Where possible the secure mode of operating should be the default mode

6.4 PLaGUE in User Interfaces

The issue of personal liability can also be applied to user interface issues identified during the evaluation of the software in chapter 3. During the study, participants were observed to quickly dismiss error messages without reading them. Even where the message contained useful information on how to correct the problem, the participants were seen to ignore this information, preferring to rapidly try several of their own ideas for fixing the problem. Such behaviour has previously been identified, but not fully explained. When thought about in terms of PLaGUE, it can be seen that the developers place liability on the users for reading ‘important’ system information, whereas this is of no concern to the users, who find speed of task completion to be paramount. In this way, the assumed responsibilities of software users have affected their use of this software. Participants became frustrated when several error messages were encountered in a session because it interrupted their flow. This evidence, in conjunction with similar observations from the literature (Gutmann, 2005; Zurko, *et al.*, 2002) leads to the recommendation that error messages be reduced in security software as they have little benefit:

Reduce the number of pop up error messages

The problem remains of how to communicate to the user when a task they have attempted to perform is infeasible, and this requires further research. Possible solutions include the use of default values where none are supplied, the use of integrated rather than pop up error messages to decrease the disturbance to the user’s workflow, or the use of visualisation such as colouring to indicate the success or failure of a task.

In the usability study participants seemed to find the use of visualisation useful in identifying the security state of the application. When a different version of the software without this visualisation was used, most participants were unable to identify the status of the application. Visualisation may be a way to communicate the developer’s perceptions of user liabilities, whether they are correct or not, to the user, thus helping them to understand what is expected of them. Visualisation may also be helpful to improve the situation identified by Garfinkel (2005), and the survey and interviews in chapter 4, in which some respondents indicated having sent or received secure e-mail messages, but were unable to describe how they knew this had taken place. It was evident that some of these respondents were mistaken in their beliefs as they did not have

the necessary digital ID to send such secure messages, but something had made them falsely believe their messages had been sent securely.

Use strong visualisation techniques to convey the state of security to the user

When thought about in terms of PLaGUE, it seems that software developers have assumed the conveying of security states not to be important to users. This seems to follow with previous evidence that security software should be transparent and not interrupt the user, however it can cause problems with the user's ability to identify the security state of e-mail messages, for example. In fact it seems that users require this information, not because it interests them, but because without it they create inaccurate models of security; e.g. the e-mail was sent encrypted when it was not. This is a case where users should be liable for knowing the level of security of their system but are not.

Many of the difficulties faced by participants in the usability study emerged in the task which required a great deal of customisation. This task took much longer, required more mouse clicks and produced more errors than any other task. Forcing customisation of software means that the users are thought to be willing and able to create a decision making responsibility, contrary to the findings of Dourish and Redmiles (2002), and the observations of user behaviour in the usability study of chapter 3:

Ensure customisation of security is optional rather than mandatory

This makes the responsibility of customisation optional rather than compulsory, and can be fulfilled in some cases by using default values that advanced users may change if they wish.

6.5 PLaGUE in Policy Development

It is not only the way software is designed that affects how it will be used, but the policies of software developers, system administrators, regulatory bodies and the government. Since much of this section is relevant to e-mail encryption discussed in chapter 4, a taxonomy of the barriers discovered to e-mail encryption has been built to summarise the main issues, this is shown in figure 6.1

As can be seen from the taxonomy, part of the rationalisation process for using e-mail encryption was to look to peers and leaders. Within the public this constitutes friends colleagues and family, whilst in the business domain the need to adopt technologies is strongly driven by regulatory bodies such as the Financial Standards Association, the Law Society of Hong Kong and the Joint Information Systems Committee. Interview respondents made it evident that the recommendation to use e-mail encryption by any such bodies would strongly swing their opinion in favour of adopting the technology. It is evident that the feeling of personal liability to use the technology is

increased when that peers express that view. Since none of the regulatory bodies examined currently endorse e-mail encryption, and since all of the organisations interviewed send sensitive information via e-mail it is recommended that they do so, also providing instructions on sourcing and implementing the technology:

Internal and external policy makers should endorse the use of e-mail encryption

Some organisations feel concern over the legal implications of adopting e-mail encryption, for example, whether e-mails can be accountable as evidence in a court trial with or without digital signatures attached, or whether sending highly secure messages across international borders is legal under export control laws. Since the literature review has shown that legal documents relating to e-mail encryption are ambiguous and difficult to locate it is very difficult for organisations to find the answers to these questions, thus:

Laws relating to encryption should be clarified and centralised

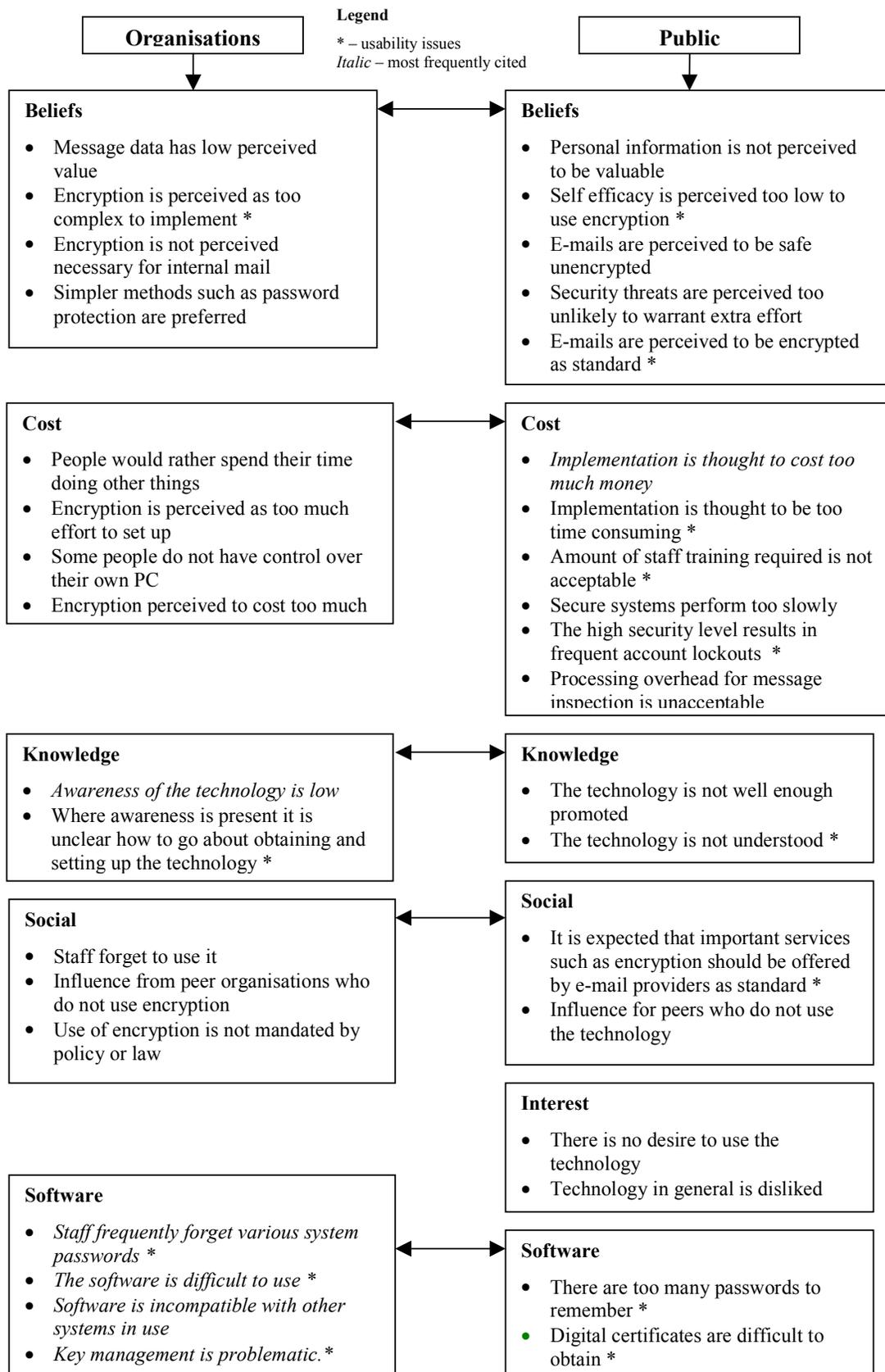
Clarification and flattening of the structure of documents relating to e-mail encryption would facilitate organisations understanding of their consequences.

One of the most frequently encountered reasons on figure 6.1 was the absence of knowledge about the existence of e-mail encryption. The potential user base for e-mail encryption is essentially any person who uses e-mail to send sensitive information; a user base which chapter 4 suggests will be vast and widely differing since most people questioned send sensitive information and therefore would benefit from the protection of e-mail encryption. However, the term ‘encryption’ seems only to be discussed in technical books, journals and websites; areas never reached by a majority of people. As can be seen in adoption theory models such as the Diffusion of Innovation Theory (Rogers and Scott, 1997), awareness must be present if a user is to trial and eventually adopt a technology:

Increase awareness of e-mail encryption

When asked how awareness could be improved, many of the respondents suggested using publicity in mainstream media such as Internet adverts, newspaper and television campaigns. Others suggested that more training be offered on the subject in the workplace.

Figure 6.1 A Taxonomy of barriers to the adoption of e-mail encryption



Within system security, the most popular choice for authentication is the password for its low cost and high convenience. Rules for password selection are also widely variable, such as the length, allowed characters, and whether the password is self-chosen or pre-designated. The study in chapter 5 statistically tested the long-term memorability of various passwords and found that cases where the user had selected their own password had greater recall success in the long term than those where the user was issued a random password. These results apply where certain constraints were applied to password selection in both cases, in other words the password can be self-chosen but must follow certain rules:

Users should choose their own passwords

It is a sensible policy for system administrators to allow users to choose their own password, even if constraints are given on its composition. This recommendation shifts the liability for password creation from the system administrator, or automatic password generation tool, to the user. This is not a universal practice, especially amongst websites where users are often e-mail a password upon registering. Excessive constraints should be avoided unless security is paramount, and guidelines should be provided on how to choose a non-dictionary password, which is easy to remember by using mnemonics for example.

The same password memorability study detailed in chapter 5 found that users tended to forget their password after a specific time of non-use. There are no known previous studies that have used a similar methodology of staged recall tests that could therefore obtain this data. The passwords were forgotten after they had not been used for between 15 and 21 days, and this occurred with all types of passwords, and with both issued and self-chosen passwords:

A reminder should be issued after 15-21 days of password non-use

Most participants who did survive this period without failure could recall their password until the end of the study. Therefore it is recommended that users are encouraged to sue their password if they have not done so within the first 20 days of receiving it, for example by sending them their password via e-mail.

6.6 Moving Forward With Usable Security

The studies in this thesis have identified many cases where the usability problems with security extend from user interface problems as are traditionally identified in the usability field, to problems stemming from the user's underlying attitudes, perceptions and liabilities, illustrated by the following five examples:

Respondents to the interviews in chapter 4 said that they place their personal privacy in high regard, but later they paradoxically explained that they feel their personal information to have

very low value, often making comments along the line of ‘nobody else would be interested in this’, which from an attackers point of view is untrue. This suggests that they do not understand the attacks which can take place using the information they send in their e-mails, and that they are complacent in protecting themselves from attack.

Participants in the usability study were seen to knowingly compromise security, their justification for this being that was easier that way. There is a perceived trade-off between immediate gratification (spending time and effort on some desirable task at hand) and long term risk hedging (spending time and effort on security).

The notion that security is as an attribute of task completion rather than a task of itself was assumed in chapter 1, and was later supported by the qualitative findings of the thesis during the usability study reported in chapter 3 and the interviews in chapter 4. Participants showed high value in the notion of security, yet placed greatest importance on the completion of tasks unrelated to security. This emphasises the approach that security should be designed to be effective with minimum involvement from the user.

Some survey and interview respondents believed that even encrypted e-mails remain vulnerable to attack to the Internet, which although cannot be rules out altogether, remains highly unlikely.

Some Interview respondents believed that e-mail sent internally within an organisation does not require any security protection as it cannot be attacked. This is untrue because this threat model incorrectly assumes that there is no hostility within the organisation.

These issues demonstrate that in addition to traditional usability testing where users’ behaviour with software is examined to identify interface problems, it is also necessary to separately examine users’ mental models to identify any pre-existing perceptions or attitudes that may affect their interaction with the software. PLaGUE is presented as a model of thinking in this way – by identifying personal liabilities, perceived and actual, of the user and developer and using these to evaluate system use.

6.7 Summary

E-mail security, although well established, had been reported to see very limited usage, which was not effective in the battle against online security threats. Clearly e-mail encryption has the potential, if used widespread and consistently, to dramatically reduce these threats; eavesdropping; unsolicited junk mail; identity theft; phishing. The HCI-SEC community has made good progress in developing research into further aligning usability and security, and promoting the importance of such issues. However the studies of this thesis identified much room for improvement. Usability problems were found in essentially two categories, those arising from user

interface problems, and those arising from poor estimation of the user's mental model. This mental model includes beliefs and attitudes about security, and perceived responsibilities as described by PLaGUE. These beliefs can be formed before as well as during system use, and have seen to be overlooked by the software developers in many cases as evidenced by the findings of the thesis.

Chapter 7: Conclusions and Future Work

7.1 Introduction

This thesis addresses the intersection of two fields; usability and security. The former is essential if humans are to successfully interact with machines, whilst the latter is equally important to ensure that data is only used for authorised purposes. The aim of this thesis was to investigate the extent to which the usability of security software can affect the level of security in practice. Particular focus has been given to e-mail, because it is a hugely popular technology, but one which suffers from many security ailments. The motivation of the research was to work towards every e-mail being sent over the Internet having high security so that the numerous threats currently posed to personal and business data could be significantly reduced. Previous chapters have explained the underlying domain, highlighted the apparent disparity between usability and security and investigated ways to improve the situation. This final chapter will summarise the findings of the research and report on their limitations and areas that still require attention.

7.2 Research Overview

Chapter two

The literature review highlighted a comprehensive set of usability issues applying to security software, including legal complexities, social phenomena, software faults and logistical problems with the encryption scheme. Also highlighted, were the many advances made in recent years to promote principles aiming to overcome these issues for the development of usable security.

Chapter three

A usability study was chosen to evaluate the effectiveness of the application of these principles because the value of usability studies in finding large proportions of problems with low cost is widely accepted. It was found that this either these principles were not effective, or not properly implemented in the software examined. The software examined, named Polaris, was the most recent and novel in the field and was, by chance, anti-virus software. The usability study performed found that although there were problems with the software interface, the majority of problems arose from the user's behaviour. Users found it difficult to break habits which they have formed over long periods of use (for example opening windows applications in the standard manner), they found it difficult to feel passion for protecting their data because their value system is different to that of the attacker, and they found it difficult to make trust based decisions. Keeping mindful the principle that users are not the enemy, this poses a difficult problem in how to alter either the software, or the users' attitudes to improve their security habits, without seeming

to place blame on the users actions. Furthermore, there were some cases where users were aware of the risk of dangerous software, but knowingly ran it in an insecure fashion. This evidence strongly corroborates the notion put forward by some in the literature that the 'normal' way to perform a task should be the secure way; therefore the users choices or attitudes will be inconsequential because they are perhaps unknowingly acting in a secure manner by default. Some heuristics related to the software interface were also put forward; that error messages should be minimised because users ignore them, and where present should allow users to understand and recover from the error; strong visualisation seems to be an effective way to communicate security information to users. Polaris specifically could be improved by using segregated disk areas which are automatically created and subsequently deleted for each new application launch; this would make secure behaviour the default, without imposing difficult decision making responsibility on the user.

Overall, it seems that support Whitten and Tygar's early prediction (1999) that security software has in some way different usability needs to other software. This also seems to support the assumption made at the beginning of the thesis that users perceive security as an attribute to task completion, rather than a task itself. This prompts the proposal of a guideline, which encourages software designers to alter their model – that security is a task – to better align with the users model – that security is an attribute of a task. In practice this may be achieved by developers of security only tools such as anti virus or encryption programs to closely collaborate with developers of task-oriented tools such as operating systems or e-mail clients in order to merge security with task completion in a way that is currently not fully present. A combination of use cases with threat models could be used to identify users' likely tasks, and the necessary security that should be provided for each. Unfortunately the only barrier to working in this way seems to be the profit making nature of software houses whereby collaboration between houses is seen as dangerous and frequent releases of new software versions are seen as necessary.

Chapter 4

After evaluating the Polaris software to identify the effectiveness of HCI-SEC principles, it was necessary to focus on one of the many applications areas of security. Although Polaris happened to be anti-virus in nature, it was thought that the area of e-mail security would yield greater benefits under analysis. E-mail enjoys a user base of around 1.1 billion users exchanging around 183 billion messages per day (marketWire, 2006), but e-mail has also become a favourite avenue for numerous novel attacks such as phishing and identity theft. Technology such as PKI encryption is technologically sound and mature enough to significantly cap the security threats of e-mail, yet it seemed according to anecdotal evidence that it was not being used to full effect. As the problem of low use of e-mail encryption had been identified, case study was an appropriate

qualitative methodology to use to investigate the cause of the problem. Interviews were used to collect data from individual members of the public and organisations to discover the actual use of e-mail encryption, the need and perceived need for it, and attitudes towards it.

The data collected in the interviews confirmed the anecdotal evidence that the use of e-mail encryption is very low. Generally, respondents showed a good awareness of the risks of the Internet, regardless of their age or technical experience; this is perhaps influenced by the heavy media reporting on the subject (see Appendix C). However, despite their knowledge of the risks of sending data via e-mail, it was admitted that large amounts of sensitive data were sent via e-mail, including sensitive work documents contracts and research findings, passwords, and personal details. Further contradictions were found when most respondents attributed a strong sense of protection over their privacy, yet later claimed their data did not deserve protection. This behaviour was rationalised amongst the public by the notion that security attacks only target businesses for financial gain, and that attackers were unlikely to find their data appealing or valuable. There seemed to be little understanding that financial gain could be made from personal details in the forms of phishing and identity theft. Business rationalised their abstention from e-mail encryption for various reasons, including the cost of implementation, the perceived complexity and difficulty of use, and the perceived necessity created by their peer organisations or regulatory bodies.

Overall, the main barriers to the adoption of e-mail encryption were found to be lack of awareness of the technology, lack of willing to invest time and effort security because it does not seem to directly accomplish any of the user's goals, is felt to be unnecessary, or is not mandated by any peer or regulator. Despite this, e-mail encryption was seen by most as being beneficial and desirable.

There were strong patterns towards accepting security in principle, but rejecting it in practice. Rather than actively avoiding security, this rejection was passive in that it the reasons behind it were largely lack of awareness, lack of perceived relevance, and lack of perceived accessibility of the technology.

As low awareness was one of the reasons respondents were not able to enter the trial phase of adoption, they were asked their opinions on how awareness could be improved. The predominant suggestion was more publicity in the form of TV and radio, and Internet advertising. Other suggestions included integrating encryption more closely in e-mail client software, and training courses offered in the workplace.

The literature had identified problems with obtaining the necessary digital certificates to use encryption, and with the user interface, but the data from this study showed that users had not

been able to progress to this stage of using the technology due to their prior knowledge and perceptions of the technology. This indicates that more detailed research needs to be done focusing on the adoption problem of e-mail encryption. Adoption is a mature research area which has been applied to other technologies such as television and broadband internet, but has so far been lacking in this area.

Respondents from the public already have a desire to protect their privacy, and a desire to use encryption, so it suggested that once the adoption issue has been addressed, that guidelines be issued by bodies of authority which explain the valuable nature of personal data, encourage the use of encryption, and explain clearly the process required to do so. Similarly, it seems that organisations would respond well to the issuing of recommendations by their regulatory bodies explaining the need for and use of e-mail encryption.

Chapter 5

Since passwords are the most widely used authentication mechanism, and since the problem of remembering passwords was one which emerged throughout the interviews with both business and public respondents, they were chosen for a study which examined their memorability. There is already a great deal of research on their improvement; however most of this has focused on developing alternatives such as biometrics, graphical passwords, or an online authentication framework such as OpenID, rather than improving the password in its current state. It is argued that passwords in their traditional format are deserving of more research attention because they are widely deployed, familiar to most users, and it is hard to beat their convenience and low monetary cost. In the hope of reaching a specific guideline to improve this aspect of security, an experiment was performed to assess the impact on memorability of different types of specially constructed password. It was proposed that since the password is heavily infiltrated in today's culture that more research be done to improve it in its existing forms rather than in alternative forms such as the graphical password, which remain immature. It was hypothesised that numeric only passwords in combination with a three strikes and you're out approach would offer a balance between usable and security by facilitating learning of passwords whilst simultaneously increasing the security of the system they protect by the burden on system administrators to reset forgotten passwords and reducing the need for users to choose insecure passwords or write them down. It was necessary to use a quantitative approach to measure the actual recall performance of various passwords amongst users, where a qualitative approach would have only addressed the perceived effect. The study was longitudinal to collect data over time in order to make the results applicable to long term memory. Statistical analysis of the data collected during the experiment showed the effect of these specially constructed on memorability not to be highly significant, however other effects were found, namely that self-chosen passwords yielded more successful recall than issued

passwords. Also, a phenomenon was discovered whereby most users recall success dramatically dropped when the password had not been used for between 15 and 21 days, but users who ‘survived’ this period tended to have good recall until the end of the study. Based on this, it was suggested that a reminder is issued if a user has not logged in within 15 days of account registration.

Chapter six presented a discussion synthesising the findings of the thesis as a whole.

7.3 Research Contributions

This thesis contributes to the security engineering profession by demonstrating that usability can have a significant and direct impact on overall security, and therefore requires much more attention throughout the software life cycle than it currently receives. Throughout the thesis it has been demonstrated that despite popular myths to the contrary people do care about privacy and security a great deal. In studies where they are shown to ignore security indicators (e.g. (Schechter, *et al.*, 2007)), or perform unsafe operations (e.g. the Polaris usability study) users are often focused only on performing a primary task, with security forming an attribute of task completion rather than a discrete task; this is contrary to the way much security software is designed. Furthermore, participants’ behaviour in laboratory settings can be influenced by their surroundings, the authority of the researcher, and the knowledge that they are not truly at risk. This has led to the acceptance of the approach taken in this thesis that security should be designed and analysed with recognition that it is perceived as an attribute to task completion, rather than a task of itself.

Previous literature was reviewed and organised into a thorough synopsis of research affecting the topic of the thesis, highlighting agreements, contradictions, and areas which require further research and went on to direct the studies of the thesis. A cognitive walkthrough was performed to demonstrate the complexities with digital signature management in PKI.

A usability study was designed and executed which demonstrated that principles emerging from current research have not fully met their goal of aligning usability and security. Actionable improvements were suggested to improve principle of least authority style anti virus software specifically, and security software in general.

A case study approach comprising interviews and a survey was used to address the mystery of the seemingly low success of e-mail encryption despite the technological soundness and maturity of the technology. Insight was provided into the mental models of users towards e-mail encryption and identified a gap between the design model and the user model. It was found that organisations and businesses communicate many sensitive data electronically, yet do not adequately protect it

using e-mail security. E-mail encryption was welcomed in principle, but avoided in practice. It was shown that awareness of online security risks is generally high, indicating that education alone will not be enough to encourage people to use security tools effectively. Reasons for abstention from e-mail security were taxonomised and proposals for improving the situation given. E-mail security policy improvements were recommended as a result of the analyses of case studies, namely for regulatory bodies to strongly encourage the use of e-mail encryption with explicit instructions on how to do so. It was also suggested that user's mental models and perceptions, rather than poor software design are currently the responsible factor for the low adoption of e-mail encryption.

A re-usable methodology was designed to cost effectively gather data for longitudinal password recall studies. This methodology was used to collect password recall data from participants using specially constructed automated web sites, and unlike previous studies, using tiered data collection over increasing periods of time to better reflect real world use and to analyse how the period of non use can have an effect.

Statistical analysis of the password memorability data collected allowed rejection of the hypothesis that numeric passwords aid recall. However it was found that the length of time a password is not actively used for affects its recall success, therefore it can be recommended that users are give a reminder of their password after about two weeks to improve long term recall.

The acronym PLaGUE was introduced to emphasise how personal and social liabilities, responsibilities, perceptions and attitudes can affect the use of security software as equally as user interface problems, which are traditionally the cited cause for problems. A motivation is presented to continue further research into usable security with greater attention on identifying perceived liabilities and analysing how these might be considered to improve the design of security software so that it more fully matches users' expectations, is used more correctly, and is therefore more secure.

7.4 Future Research

In retrospect increasing the numbers of participants and using alternative methodologies, each of which are discussed below, could have improved the studies of this thesis.

The willingness of potential participants and the resources available to recruit them limited the number of participants who could be recruited. Therefore the statistical power of empirical results, and the depth of information gathered in the qualitative studies were also limited. It is always desirable to have a larger sample size to further validate results; more sets of data would have

strengthened findings, particularly those of the empirical password memorability study, and could have been performed with a relatively low amount of extra resources.

A recurring problem in the field of usable security studies is that of selecting a laboratory setting for experiments, or 'real world' observations. The former increases control over influential factors, but can alter the participant's behaviour. The usability study in chapter 3 used a lab setting and it was found that the motivation to protect the security of one's PC was difficult to emulate in lab conditions due to participants expectations of the study, feelings of trust or authority towards the researcher, and the awareness that the data being used is not 'real' and can have no impact on their lives. Using real data would give results that are considerably trustworthier when used to implement solutions to problems, but at the expense of putting users' at risk, expending considerably more time collecting data, and introducing more external variables that may influence the result.

An ethnographic approach would have augmented the critical case study approach used to collect data on the use of e-mail encryption, as it would allow observation of organisations performing their routine work and analysis of the security requirements would be more directed by actual processes than perceived benefits. However such an approach would also have its limitations and difficulties, such as the large amount of time required to collect data, the high co-operation required from organisations to allow access to the data, and the possibility that the researchers own subjective views influence the analysis.

A strong motivation is presented for researching the way users' attitudes, beliefs and perceptions, particularly of their responsibilities to security, affect the way they use security. These factors influence the way in which security is used, which in turn can have a huge detrimental impact on the overall system security, regardless of the soundness of the technology used. Current research has focused on the traditional software interface aspect of usability, failing to fully identify the user's behaviour in the security domain, or propose strategies to account for these in maintaining high security.

References

- "Electronic Signatures Directive," in *1999/93/EC*, vol. OJ L 13, 1999, pp. 12.
- "Electronic Communications Act 2000," in *ECA2000*, 2000.
- "Electronic Communications Bill," 2000.
- "Export Control Act," 2002.
- "Health and Social Care (Community Health and Standards) Act," *Cabinet Office*, 2003.
- Adams, A. and Sasse, M. A., "Users are not the enemy," *Communications of the ACM*, 42 (12) pp. 41-46, 1999.
- Ajzen, I., "The Theory of Planned Behaviour," *Organizational Behaviour and Human Decision Processes*, 50 pp. 179-211, 1991.
- Anderson, R., *Security Engineering. A Guide to Building Dependable Distributed Systems*: John Wiley & Sons, Inc., 2001.
- Anderson, R. J., "Clinical System Security - Interim Guidelines," *British Medical Journal*, 312 pp. 109-111, 1996.
- Articsoft, The problems with Secure Email, 2003,
<http://usablesecurity.com/2005/07/19/obedience-to-authority/>, accessed on 11 October 2005
- Austin, T., *PKI: A Wiley Tech Brief*: John Wiley & Sons Inc., 2001.
- Baddeley, A. D., Conrad, R., Hull, A. J., D.J.A., L., Rabbitt, P. M., B.A., S., and G.A., S., "Code design and the design of keyboards," The Post Office 1962.
- Balfanz, D., Smetters, D. K., and Grinter, R. E., "In search of usable security: five lessons from the field," *IEEE security and privacy*, 2 (5) pp. 19-24, 2004.
- Bauer, F. L., *Decrypted Secrets. Methods and Maxims of Cryptology*, p.196, Third ed. Berlin: Springer, 2002.
- Bell, D. E. and La Padula, L. J., "Secure Computer Systems: Mathematical Foundations and Model," MITRE, Bedford, MA, USA May 1973.
- Besnard, D. and Arief, B., "Computer security impaired by legitimate users," *Computers & Security*, 23 (3) pp. 253-264, 2004.
- Boehm, B. W., "A Spiral Model of Software Development and Enhancement," *Computer*, 21 (5) pp. 61-72, 1988.
- Bohm, N., Brown, I., and Gladman, B., "Electronic Commerce: Who Carries the Risk of Fraud?," *The Journal of Information, Law and Technology (JILT)*, 2000 (3), 2000.
- Borchers, J. O. and Thomas, J. C., "Patterns: What's In It For HCI?," presented at Computer Human Interaction, Seattle, USA, 2001 pp. 225-226
- Boyd, C., Profile: Gary McKinnon, 2006,
<http://news.bbc.co.uk/1/hi/technology/4715612.stm>, accessed on 24th February 2006
- Braga, A., Rubira, C., and Dahab, R., "Tropyc: A Pattern Language for Cryptographic Software," presented at Pattern Languages of Programming, Illinois, USA, 1999 pp.
- Brooke, J., "SUS: A quick and dirty usability scale," in *Usability evaluation in industry*, P. Jordan, B. Thomas, and B. Weerdmeester, Eds. London: Taylor and Francis, 1996.
- Brostoff, S. and Sasse, A., "Are Passfaces more usable than passwords? A field trial investigation," presented at HCI 2000, Sunderland, UK, 2000 pp. 405-424

- Brunel, Data Protection Policies, 2006,
<http://www.brunel.ac.uk/about/administration/infoaccess/dataprot/policies>,
 accessed on May 2007
- Callas, J., "Video Interview with Jon Callas, CTO and CSO of PGP Corporation," Help Net Security, 2004.
- Campbell, A., "'Phishing' gang jailed for £200,000 eBay scam", in *Metro*, London, 2nd November 2005, pp.
- CipherTrust, "Zombies: Steady Increase", in SC Magazine, July 2005 2005.
- Darke, P., Shanks, G., and Broadbent, M., "Successfully completing case study research: combining rigour, relevance and pragmatism," *Information Systems Journal*, 8 (4) pp. 273-289, 1998.
- de Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D., Ren, J., Rode, J., and Silva Filho, R., "Two experiences designing for effective security," presented at Symposium On Usable Privacy and Security, Pittsburgh, Pennsylvania, 2005 pp. 25-34
- Diffie, W. and Hellman, M. E., "New Directions in Cryptography," *IEEE Transactions on Information Theory*, 6 pp. 644-654, 1976.
- Dingledine, R. and Mathewson, N., "Anonymity Loves Company: Usability and the Network Effect," in *Security and Usability. Designing Secure Systems That People Can Use*: O'Reilly, 2005, pp. 547-559.
- Dourish, P., Delgado de la Flor, J., and Joseph, M., "Security as a Practical Problem: Some Preliminary Observations of Everyday Mental Models," presented at Workshop on HCI and Security Systems, CHI2003, Fort Lauderdale, Florida, USA, 2003 pp.
- Dourish, P., Grinter, R. E., de la Flor, J. D., and Joseph, M., "Security in the wild: user strategies for managing security as an everyday, practical problem," *Personal and Ubiquitous Computing*, 8 (6) pp. 1617-4909, 2004.
- Dourish, P. and Redmiles, D., "An approach to usable security based on event monitoring and visualization," presented at 2002 Workshop on new security paradigms, Virginia Beach, Virginia, 2002 pp. 75-81
- Dourish, P. and Redmiles, D., "An Approach to Usable Security Based on Event Monitoring and Visualization," presented at Proceedings of the 2002 workshop on New security paradigms, Virginia Beach, Virginia, 2002 pp. 75-81
- DTI, Goods Checker, 2006, <http://www.ecochecker.co.uk/goodschecker/>, accessed on 20th February 2007
- DTI, OGEL checker, 2006, <http://www.ecochecker.co.uk/ogelchecker/>, accessed on 20th February 2007
- Dubé, L. and Paré, G., "Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations," *MIS Quarterly*, 27 (4) pp. 597, 2003.
- eBay, Using eBay Toolbar's Account Guard, 2006,
<http://pages.ebay.com/help/confidence/account-guard.html>, accessed on 20th April 2006
- Ellison, C. and Schneier, B., "Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure," *Computer Security Journal*, 16 (1) pp. 1-7, 2000.
- Emigh, A., "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures," Radix Labs 3rd October 2005.
<http://www.antiphishing.org/Phishing-dhs-report.pdf>
- Eysenck, M. W. and Keane, M. T., *Cognitive Psychology: A Student's Handbook*. Hove and London (UK): Lawrence Erlbaum Associates, 1990.

- Faulkner, X., *Usability Engineering*: PALGRAVE, 2000.
- Festa, P., Firm unveils encrypted free email, 1999,
http://news.com.com/Firm+unveils+encrypted+free+email/2100-1023_3-226160.html, accessed on 30th November 2005 2005
- Festa, P. and Wilcox, J., Experts estimate damages in the billions for bug, 2000,
http://news.com.com/Experts+estimate+damages+in+the+billions+for+bug/2100-1001_3-240112.html, accessed on 9th February 2007
- Finn, J., "Photographing Fingerprints: Data Collection and State Surveillance," *Surveillance & Society*, 3 (1) pp. 21-44, 2005.
- FIPR, FIPR Response to NHS Confidentiality Consultation, 2004,
<http://www.cl.cam.ac.uk/~rja14/fiprmedconf.html>, accessed on 28th March 2006
- Flechais, I., Sasse, A. M., and Hailes, S. M. V., "Bringing security home: a process for developing secure and usable systems," presented at Workshop on new security paradigms, Ascona, Switzerland, 2003 pp. 49-57
- Foremski, T., Worm attack fails to interrupt internet, 2006,
<http://search.ft.com/iab?queryText=sobig&y=6&aje=true&x=12&id=030823000419&location=http%3A%2F%2Fsearch.ft.com%2FftArticle%3FqueryText%3Dsobig%26y%3D6%26aje%3Dtrue%26x%3D12%26id%3D030823000419&referer=http%3A%2F%2Fsearch.ft.com%2Fsearch%3FqueryText%3Dsobig>, accessed on 14th May 2007
- Freeh, L., "Speech to US Senate Sub-Committee on Terrorism, Technology & Government Information," 1997.
- FSA, The FSA's approach to the regulation of e-commerce, 2001,
<http://www.fsa.gov.uk/pubs/discussion/>, accessed on May 2007
- FSA, Miscellaneous amendments to the Handbook (No. 9), 2003, <http://www.fsa.gov.uk/pubs/cp/cp191.pdf>, accessed on May 2007
- FSA, Memorandum of understanding; Inland Revenue & Financial Services Authority, date unknown, http://www.fsa.gov.uk/pubs/mou/fsa_ir.pdf, accessed on May 2007
- Garfinkel, S., "Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable," in *Department of Electrical Engineering and Computer Science*. Massachusetts: Massachusetts Institute of Technology, 2005, pp. 472.
- Garfinkel, S. L. and Cranor, L. F., Eds. *Security and Usability: Designing Secure Systems That People Can Use*. CA, USA: O'Reilly, 2005.
- Gerd, D. and Markotten, T., "User-Centered Security Engineering," presented at Nordu2002, Helsinki, Finland, 2002 pp.
- Glaser, G. B. and Strauss, A. L., "The Discovery of Grounded Theory." London, UK: Weidenfeld and Nicholson, 1968.
- Godden, D. R. and Baddeley, A. D., "Context-dependent memory in two natural environments: On land and under water," *British Journal of Psychology* (66) pp. 325-331, 1975.
- Gong, M. and Yan, X., "Applying Technology Acceptance Model, Theory of Planned Behavior and Social Cognitive Theory to Mobile Data Communications Service Acceptance," presented at Eighth Pacific Asia Conference on Information Systems, Shanghai, 2004 pp. 444-457
- Grampp, F. T. and Morris, R. H., "Unix Operating System Security," *AT&T Bell Laboratories Technical Journal*, 63 (8) pp. 1649-1672, 1984.

- Gray, W. D. and Salzman, M. C., "Damaged Merchandise? A Review of Experiments That Compare Usability Evaluation Methods," *Human-Computer Interaction*, 13 pp. 203-261, 1998.
- Group, A.-P. W., Origins of the word "Phishing", 2005,
http://www.antiphishing.org/word_phish.html, accessed on 22-08-05 2005
- Gutmann, P., "PKI: It's Not Dead, Just Resting", in *IEEE Computer*, August 2002.
- Gutmann, P., "Inadvertent case study in SSL server cert effectiveness,"
hcisec@Yahoogroups.com, Ed., 2005.
- Gutmann, P., "Security Usability Fundamentals," m. hcisec@Yahoogroups.com, Ed., 2005.
- GVU, GVVU's tenth WWW user survey results, 1999,
http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/, accessed on
- Halkidis, S. T., Chatzigeorgiou, A., and Stephanides, G., *A Qualitative Evaluation of Security Patterns*, 3269 ed, 2004.
- Hébert, R., Code Overload:Doing a Number on Memory, 2001,
<http://www.psychologicalscience.org/observer/0901/code.html>, accessed on 29 September 2006
- Hinsley, F. H. and Stripp, A., *Codebreakers : the inside story of Bletchley Park*: Oxford University Press, 2001.
- Hogland, G. and McGraw, G., *Exploiting software : how to break code*: Addison-Wesley, 2004.
- Horley, L., "The National Programme for IT : Transforming the NHS," A. DeWitt, Ed. London, 2006, pp. BCS meeting.
- Ilet, D. and Hu, J., Zombie trick expected to send spam sky-high, 2005,
http://news.com.com/Zombie+trick+expected+to+send+spam+sky-high/2100-7349_3-5560664.html, accessed on 22-08-05 2005
- ISO, "Ergonomic requirements for office work with visual display terminals (VDTs) - part 11: Guidance on usability," BSI, 1998.
- ISO, "Information technology - Security techniques - Evaluation criteria for IT security," BSI, 2005.
- Jermyn, I. H., Mayer, A., Monroe, F., Reiter, M. K., and Rubin, A. D., "The Design and Analysis of Graphical Passwords," presented at Proceedings of the 8th USENIX Security Symposium, Washington DC, 1999 pp.
- Johansson, J. M., Security Management:The Fundamental Tradeoffs, 2004,
<http://www.microsoft.com/technet/community/columns/secmgmt/sm0104.msp>, accessed on 8th March 2005
- Johnson-Laird, P. N., "Mental Models on Cognitive Science," *Cognitive Science*, 4 pp. 71-115, 1980.
- Jones, R., Credit-card fraudsters target internet, 2005,
<http://business.guardian.co.uk/story/0,,1636516,00.html>, accessed on 24th February 2006
- Jøsang, A. and Sanderud, G., "Security in mobile communications: challenges and opportunities," presented at Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003, Adelaide, Australia, 2003 pp. 43 - 48
- Kaplan, B. and Duchon, D., "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study," *MIS Quarterly*, 12 (4) pp. 571, 1988.
- Karp, A. H., "RE: Polaris," A. DeWitt, Ed. London, 2006.

- Kis, M., "Information Security Antipatterns in Software Requirements Engineering," presented at 9th Conference of Pattern Languages of Programs (PloP), Monticello, IL, USA, 2002 pp.
- Kratz, M., Humenn, P., Tucker, M., Nolte, M., Wagner, S., Seppala, G., Shadrow, G., Wilson, W., and Auton, S., Health Level Seven Security Services Framework, 1999, accessed on 11th January 2006
- Leonard, F. and Safir, A., "Iris Recognition System And Method." USA, 1989.
- Mackay, W. E., "Is Paper Safer? The Role of Paper Flight Strips in Air Traffic Control," presented at Transactions on Computer-Human Interaction, 2000 pp. 311-340
- MacLeod, C., "Password Overload", in IT Now, March 2005 2005.
- marketWire, The Radicati Group, Inc. Releases Q3 2006 Market Numbers Update, 2006, http://www.marketwire.com/mw/release_html_b1?release_id=171272, accessed on 14th May 2007
- Mayhew, D. J., *The Usability Engineering Lifecycle*: Morgan Kaufmann Publishers, Inc., 1999.
- McCrickard, S. D. and Chewar, C. M., "Attuning Notification Design to User Goals and Attention Costs," *Communications of the ACM*, 46 (3) pp. 67-72, 2003.
- McNamara, P., You've got mail, 2005, <http://www.networkworld.com/techinsider/2005/081505techinsider-mail.html>, accessed on 11 October 2005
- Moores, S., Pokemon panic stirs fear of e-robbery, 2000, <http://observer.guardian.co.uk/business/story/0,6903,363630,00.html>, accessed on 16th January 2006
- Mouratidis, H., Giorgini, P., and Manson, G., "Integrating Security and Systems Engineering: Towards the Modelling of Secure Information Systems," presented at Conference on Advance Information Systems, Velden, Austria, 2003 pp. 63 - 78
- Nielsen, J., *Designing Web Usability: The Practice of Simplicity*. CA, USA: New Riders Publishing, 1999.
- Nielsen, J., Why you only need to test with 5 users, 2000, <http://www.useit.com/alertbox/20000319.html>, accessed on 29th November 2005
- Nielson, J., *Usability Engineering*: Morgan Kaufmann Publishers, Inc., 1993.
- Norman, D., A., *The Psychology of Everyday Things*: Basic Books, 1988.
- Norman, D., A. and Draper, S. W., *User Centered System Design; New Perspectives on Human-Computer Interaction*. Mahwah, NJ, USA: Lawrence Erlbaum Associates, Inc., 1986.
- Office, C., "Encryption and Law Enforcement; A Performance and Innovation Unit Report," Performance and Innovation Unit, London May 1999 1999.
- Orgill, G. L., Romney, G. W., Bailey, M. G., and Orgill, P. M., "The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems," presented at 5th Conference on Information technology education, Salt Lake City, UT, USA, 2004 pp. 177 - 181
- OUT-LAW, Encryption still underused in financial transactions, warns PwC, 2006, <http://www.out-law.com/page-6830>, accessed on 4th May 2007
- Palen, L. and Dourish, P., "Unpacking "privacy" for a networked world," presented at SIGCHI conference on Human factors in computing systems, Ft. Lauderdale, Florida, USA, 2003 pp. 129-136

- Rogers, E. M. and Scott, K. L., "The Diffusion Of Innovations Model and Outreach from the National Network of Libraries of Medicine to Native American Communities," University of New Mexico, New Mexico 10 December 1997.
- Roth, V., Richter, K., and Freidinger, R., "A PIN-entry method resilient against shoulder surfing," presented at Proceedings of the 11th ACM conference on computer and communications security, Washington DC, USA, 2004 pp. 236 - 245
- Saltzer, J., "Protection and the Control of Information Sharing in Multics," presented at ACM Symposium on Operating Systems Principles, New York, USA, 1974 pp. 388-402
- Saltzer, J. and Schroeder, M., "The protection of Information in Computer systems," *Proceedings of the IEEE*, 63 (9) pp. 1278-1308, 1975.
- Sandhu, R., "Good-enough security," *Internet Computing, IEEE*, 7 (1) pp. 66-68, 2003.
- Sasse, A., "Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery," presented at Workshop on HCI and Security Systems, CHI2003, Fort Lauderdale, Florida, USA, 2003 pp.
- Sasse, M. A., Majority of Sprint customers turn off passwords, 2005, <http://groups.yahoo.com/group/hcisec/message/430>, accessed on 8th March 2005
- Sasse, M. A., Brostoff, S., and Weirich, D., "Transforming the 'weakest link': a human-computer interaction approach to usable and effective security," *BT Technology Journal*, 19 (3) pp. 122-131, 2001.
- Schechter, S., Dhamija, R., and Ozment, A., "The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies," presented at IEEE Symposium on Security and Privacy, Oakland, California, USA, 2007 pp.
- Schneier, B., *Secrets and Lies*: John Wiley & Sons, 2000.
- Schneier, B., "We are all security consumers," *IEEE Security & Privacy Magazine*, 1 (1) pp. 104, 2003.
- Schneier, B., MySpace Passwords Aren't So Dumb, 2006, <http://www.wired.com/news/columns/0,72300-0.html>, accessed on 23rd January 2007
- Sheng, S., Broderick, L., Koranda, C. A., and Hyland, J. J., "Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software," presented at Symposium On Usable Privacy and Security, Pittsburgh, PA. USA, 2006 pp.
- Singh, S., *The code book : The science of secrecy from ancient Egypt to quantum cryptography*: Fourth Estate, 1999.
- Stallwood, O., "eBay sellers warned over PayPal swindle", in *Metro*, London, 9th January 2006, pp. 9.
- Straub, T. and Baier, H., "A Framework for Evaluating the Usability and the Utility of PKI-enabled Applications," presented at EuroPKI, Samos Island, Greece, 2004 pp. 112-125
- Suetonius, *De Vita Caesarum, Divus Iulius (The Lives of the Caesars, The Deified Julius)*, c.110, <http://www.fordham.edu/halsall/ancient/suetonius-julius.html>, accessed on 22nd February 2006
- Sutherland, I. E., "SketchPad: A Man-Machine Graphical Communication System," presented at AFIPS Spring Joint Computer Conference, 1963 pp. 329-346
- Tulving, E., "Cue-dependant forgetting," *American Scientist* (79) pp. 27-34, 1974.
- Venkatesh, V. and Davis, F. D., "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Management Science*, 46 (2) pp. 186-204, 2000.

- Virzi, R. A., "Refining the test phase of usability evaluation: how many subjects is enough?," *Human factors*, 34 (4) pp. 457-468, 1992.
- Weinshall, D. and Kirkpatrick, S., "Passwords You'll Never Forget, but Can't Recall," presented at CHI 2004, Vienna, Austria, 2004 pp. 1399-1402
- Weirich, D. and Sasse, M. A., "Pretty Good Persuasion: A first step towards effective password security for the Real World," presented at New Security Paradigms Workshop, Cloudcroft, NM, USA, 2001 pp. 137-143
- Weirich, D. and Sasse, M. A., "Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World," presented at Proceedings of the ACM New Security Paradigms Workshop, Cloudcroft, New Mexico, USA., 2001 pp. 137-143
- Whitten, A., "People to invite," *hcisec@Yahooogroups.com*, Ed., 2000.
- Whitten, A. and Tygar, J. D., "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," presented at Proceedings of the 8th USENIX security symposium, Washington, D.C., 1999 pp. 169-184
- Whitten, A. and Tygar, J. D., "Safe Staging for Computer Security," presented at Workshop on Human-Computer Interaction and Security Systems, CHI2003, Ft. Lauderdale, Florida, 2003 pp.
- Yan, J., Blackwell, A., Anderson, R., and Grant, A., "Password memorability and security: Empirical results," *IEEE security and privacy*, 2 (5) pp. 25-30, 2005.
- Yank, K., Interview - Jakob Nielsen, Ph.D., 2002,
<http://www.sitepoint.com/article/interview-jakob-nielsen-ph-d>, accessed on 16th March 2006
- Yee, K.-P., "User interaction design for secure systems," presented at 4th international conference on information and communications security, Singapore, 2002 pp. 278-290
- Yee, K.-P., "Aligning security and usability," *IEEE security and privacy*, 2 (5) pp. 48-55, 2004.
- Yee, K.-P., Challenges: Obedience to Authority, 2005,
<http://usablesecurity.com/2005/07/19/obedience-to-authority/>, accessed on 11 October 2005
- Yoder, J. and Barcalow, J., "Architectural Patterns for enabling application security," presented at Pattern Languages of Programming, Illinois, USA, 1997 pp.
- Zimmerman, P. R., *The Official PGP User's Guide*. Boston, USA: MIT Press, 1995.
- Zurko, M. E., Kaufman, C., Spanbauer, K., and Bassett, C., "Did You Ever Have To Make Up Your Mind? What Notes Users Do When Faced With A Security Decision.," presented at Computer Security Applications Conference, Las Vegas, Nevada, USA, 2002 pp. 371 - 381
- Zurko, M. E. and Simon, R. T., "User-centered security," presented at Proceedings of the 6th new security paradigms workshop, CA, 1996 pp. 27-33
- Zviran, M. and Haga, W. J., "A Comparison of Password Techniques for Multilevel Authentication Mechanisms," *Computer*, 36 (3) pp. 227-237, 1993.

Appendix A - Materials used in the usability study of Polaris (chapter 3).

The task cards participants were presented with in envelopes:

Introduction

You have a new piece of software installed on your system called POLARIS. POLARIS is designed to protect you from viruses by restricting the authority of applications to access your files.

There is a documentation file for POLARIS on the desktop called:

‘Polaris User’s Guide Alpha.htm’

This file should contain all the information needed to complete the tasks in this experiment, and explain how to use POLARIS.

Please open each envelope in order, and only open the next envelope once you have completed the previous task. There are no time limits, and no right of wrong answers. If you cannot complete a task, please tick the box at the bottom of the task sheet and move on to the next envelope. **You may refer to the POLARIS documentation at any time.**

Now open envelope 1.

Task 1

Open the following applications from the desktop:

Adobe Acrobat Reader

Microsoft Word

Ahead Nero burning ROM

Identify which of these applications have been polarized?

Application	Has been Polarised	Has not been polarised
Adobe Acrobat Reader		
Microsoft Word		
Ahead Nero burning ROM		

I completed this task

I did NOT complete this task

Open envelope 2.

Task 2

Use the 'Polarizer' icon on the desktop to polarise Internet Explorer which will create a 'pet' with the name you have specified. **You may create more 'pets' at any time you feel appropriate throughout this experiment.**

I completed this task

I did NOT complete this task

Open envelope 3.

Task 3

Go to Outlook and check the e-mails. Open the message with subject 'Internet Banking'.

The hyperlink in this message points to your account manager site which allows you to review all of your financial data in one place. Please safely visit the website using a 'pet' of Internet Explorer, and log in with the following information:

User name: polaris

Password: 123abcyk

Pets name/memorable place/ first school : polaris

If you are asked to download a Java applet, click  . If you are prompted, choose 'Run'.

Write the number of nectar points you have:

Number of Nectar points: _____

Please indicate the following for this website:

	YES	NO
I think this website is secure		
I think this website is safe		

I trust this website		
----------------------	--	--

Logout and close Internet Explorer.

I completed this task

I did NOT complete this task

Open envelope 4.

Task 4

Go to Outlook. There will be two e-mails with subject 'try this!'.

Before you visit the links in these e-mails, what do you think of the websites the links point to:

E-mail From alex dewitt:

	YES	NO
I think this website is secure		
I think this website is safe		
I trust this website		

E-mail From Kirsten Gibbs:

	YES	NO
I think this website is secure		
I think this website is safe		
I trust this website		

Please visit the website in the e-mail from alex dewitt safely, using a pet of Internet Explorer. Do not click any links. – From your impression of this web page:

	YES	NO
I think this website is secure		
I think this website is safe		
I trust this website		

Close Internet Explorer. Please visit the website in the e-mail from Kirsten Gibbs safely, using Internet Explorer. Do not click any links. – From your impression of this web page:

	YES	NO
I think this website is secure		
I think this website is safe		
I trust this website		

I completed this task

I did NOT complete this task

Close Internet Explorer

Open envelope 5.

Task 5

Manually add some buttons to the toolbar of Microsoft Outlook which will let you safely open and save e-mail attachments using POLARIS.

I completed this task

I did NOT complete this task

Open envelope 6.

Task 6

Do not complete this task if you did not complete task 5. Skip to envelope 7.

Go to Outlook and open the e-mail with subject 'Test attachment 1'. Use the Outlook buttons you have just created to safely open this attachment.

Did it open?

yes

no

Now open the e-mail with subject 'Test attachment 2'. Use the Outlook buttons you have just created to safely open this attachment.

Did it open?

yes

no

If the attachment did not open, try to correct the problem so you can open the attachment safely.

I completed this task

I did NOT complete this task

Open envelope 7.

Task 7

Safely visit this website using Internet Explorer:

<http://www.brunel.ac.uk/~cspgajd/home.html>

Download the file 'moneymanager.exe' and save it to the desktop. Once downloaded, open the application safely. Did the application open?

Yes

No

Download 'ipinfo.exe' from the same website, and save to the desktop. Open ipinfo.exe from the desktop using the 'Icebox' feature of POLARIS. When open, ipinfo will show your IP address in a window like this:



Did you see this window?

Yes

No

I completed this task

I did NOT complete this task

Open envelope 8.

Task 8

De-polarize Microsoft Word, and open the document 'test.doc' in the normal 'unprotected' version of Word.

Did the document open?

Yes

No

If No, try to fix the problem so you can open 'test.doc'.

I completed this task

I did NOT complete this task

Finish!

Post test questionnaire:

Documentation Review

1. I understand what the purpose of POLARIS is

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

2. The documentation was easy to read

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

3. The documentation was confusing

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

4. Referring back to the documentation helped me to complete the tasks

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

5. The Documentation did not really help me to complete the tasks

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

Software Review

1. I think that I would like to use this software frequently

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

2. I found the software unnecessarily complex

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

3. I thought the software was easy to use

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

4. I think that I would need the support of a technical person to be able to use this software

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

5. I found the various functions in this software were well integrated

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

6. I thought there was too much inconsistency in this software

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

7. I would imagine that most people would learn to use this software very quickly

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

8. I found the software very cumbersome to use

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

9. I felt very confident using the software

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

10. I needed to learn a lot of things before I could get going with this software

Strongly Disagree Neutral Strongly Agree

1	2	3	4	5

Comments

Please write any comments you have here (optional)

Questionnaire:

		I have not completed this survey before – please tick to confirm					
Do you use e-mails?		YES	NO	Gender:		M	F
Age:	16-25	21-30	31-40	41-50	51-60	61-70	71-80
Do you Know what ‘Encryption’ means?		YES	NO	Do you use encryption?		YES	NO
Would you, if you could, want to have encryption for all your e-mails?		YES	NO	Do any of your friends family or colleagues use encryption?		YES	NO
Why would you want to encrypt your e-mails?							
Why aren’t you using encryption?							
Self given reasons				Clarify			
Suggested Reasons				Clarify			
Were you unaware of its existence? <i>What would make you more aware?</i>							
Do you think it will be too expensive to set up? <i>What is expensive?</i>							
Do you think it will take too long to set up - you don’t have the time <i>What part will take time?</i>							
Do you think you won’t have enough technical knowledge to install and operate it?							

<i>Why must you be technical?</i>	
Do you think your information cannot be accessed by others over the Internet? <i>Why not ?</i>	
Do you think your information is not worth protecting; you don't care if anyone can read your e-mails? <i>Why not?</i>	
Are you using some other way that you are aware of to secure the data on your PC? <i>What?</i>	
Do you want to use encryption but you don't know where to start?	
Have you ever had any problems with passwords in the past, e.g. forgetting? <i>Does this happen rarely or frequently? Do you confuse them or draw a blank?</i>	
Have you ever tried using encryption? Did you have software problems?	
Have you set up encryption but don't know anybody else who has so can't send any encrypted e-mails? <i>Have you asked anyone else to us it?</i>	
Have you started to set up encryption but got stuck with getting a digital certificate? <i>What happened?</i>	

Appendix C – Recent examples from the media on usability/security related issues

Below are presented some news clippings highlighting the media focus on security issues.

The first, appearing in the Guardian highlights the trust customers must place in retailers when giving them details, and how inadequate security can cause massive financial and reputational damage.

Charles Arthur

Thursday April 5, 2007

[The Guardian](#)

"Two momentous events in the past week: the clothes retailer TK Maxx admitted that millions of credit card details were stolen through its systems; and EMI decided that people might be prepared to pay more for less encryption (and better quality) on the music they buy online. Are those trends heading in opposite directions? Was it TK Maxx that had the right idea, in encrypting customers' card details? Or is it EMI, unlocking the shackles - although at a price - on the files that are its lifeblood, and offering better-quality sound than you would usually find on, say, a file-sharing network?"

The odd thing about credit card details is that although they're meant to be incredibly secret, the reality is that they're not. A few weeks ago I met a security expert who once stumbled across a criminals' site, which they used to check whether a stolen card had been reported or compromised. Yes, he was a security expert, but human too: "You cannot believe," he said, "how difficult it was - how incredibly difficult - not to type my own credit card number in there to check."

Because he knew that his number would be added to the database if he checked it. Stolen numbers cost about 25p online. They're a commodity.

TK Maxx helped, unfortunately: normally, all the details in a database were encrypted, such as the credit card number, the address, the customer name. But there was a period during a transaction when those details were decrypted - and that was when the Trojan program planted by the criminals captured them. Quite a haul: 45.7m credit and debit card details. There are 750m credit cards circulating in the US, and about 75m in the UK, so the TK Maxx heist nabbed perhaps 5% of the available details. But you don't have to shop at TK Maxx to have your card details ripped off. In the past year, both my wife and I have had card info used for faked purchases - in my case, buying credit from the PartyGaming website.

Encryption in databases can't, in the end, offer complete protection for card details. TK Maxx could have devised a system whereby once you gave it your credit card number and other details, nobody would ever see them unencrypted again.

You'd run the numbers through a hashing algorithm and store them; when someone gave their card number (perhaps by keying it into a phone or keyboard), it would be hashed and compared with the stored hash. If they match, it's a valid number. But the real problem is the same one that EMI has encountered and which Steve Jobs pointed out in the completely different context of music back in February with his [Thoughts on Music](#). Protection is pointless if what you're trying to protect is freely available elsewhere. Why wrap online music in digital rights software (which essentially encrypts it) if you sell CDs from which anyone can rip that same content? Similarly with credit cards: we talk to people on the phone, and they could be writing down those numbers instead of keying them into the transaction database. The site you make your purchase from could be phishing. What you have to hope is that it's not your turn today.

However, I think the solutions to these similar problems lie in different directions. EMI is trying to make us less likely to offer tracks to illicit file-sharing networks by offering a greater sense of ownership in the music you buy. If you spend 99p on a song, you're less likely to want to spread it to all and sundry. It's a gamble that I think will pay off.

For credit cards, I think the answer is more numbers - fake ones, to frustrate the hackers. Fill databases of valuable customer information with rubbish, to let the valuable names hide among the cruff. It's far harder to steal a usable number when only one in a hundred is real than when all of them are. The answer there isn't better, but worse quality. We can do that digitally too, you know."

The article below shows how the popular use of the term phishing has brought it to the public's attention, and also the seriousness of the crime (Metro, November 2nd 2005).

Wednes

'Phishing' gang jailed for £200,000 eBay scam

HE leader of an identity fraud gang which lured eBay buyers out of nearly £200,000 was jailed for four years yesterday.

David Levi is believed to be the first person convicted in Britain of 'phishing' - stealing goods after tricking computer users into revealing their bank details.

The conman, 29, his brother Guy and IT expert Daniel Lett, both 22, set up a network of computers which sent out e-mails to eBay users claiming to be from the site. People who replied using a quick link, which appeared to send users to the eBay site, were in fact connected to the criminals' computers. Sellers were then asked to tap in their log-in passwords, unwittingly handing them over to the fraudsters.

The gang then redirected e-mails meant for the true account holder to their mailboxes and offered 'valuable', but non-existent, goods for sale, such as Rolex watches and laptops. After sellers 'won' the items and paid for them the gang disappeared.

More than 160 people were duped in the scam between July 2003 and July 2004. Preston Crown Court heard. Levi, of Lytham, Lancashire, spent his share of the £197,000 in casinos and on luxury cars and a £7,000 family Caribbean cruise.

He admitted fraud and perverting the cause of justice. He is already serving a four-year prison sentence for drug offences.

Guy Levi and Lett, both of St Anne's, Lancashire, received shorter terms after admitting fraud offences, while four gang members were jailed for money laundering.

Jailing Levi, Judge Phillip Sycamore said: 'You demonstrated an arrogant and callous approach enjoying an extravagant lifestyle at the expense of victims of this fraud.'



Conman: David L

The article below shows some efforts to raise the public consciousness about the risks of poor security strategies (Metro, January 9th 2006).

Are you a target for ID theft?

Millions of people are leaving themselves open to identity theft because they don't take basic precautions against fraudsters.

Every year, more than 100,000 people in Britain have their identities stolen when their personal information falls into someone else's hands and is used for fraud, theft or deception.

Following four steps can help to protect your ID: shred personal documents, check credit files regularly, have different passwords for financial accounts and cancel unwanted credit facilities.

Yet it appears few of us have got into the habit of doing the basics. Although 50 per cent of people



Alison Nicholson: Findings ring alarm bells

check credit files, one in four fail to shred documents or cancel credit facilities they haven't used for more than a year, according to research by MyCallcredit. A third of those surveyed use the same password or Personal Identification Number (PIN) more than once.

The findings are alarming, says MyCallcredit director Alison

Nicholson. 'They show people aren't taking steps to protect themselves,' she says.

Signs that you may have had your identity stolen include items appearing on your bank or credit card statements or on your credit file that you do not recognise.

Alarm bells should also ring if you apply for state benefits and are told you are already claiming; or if you receive bills, invoices or receipts addressed to you for goods or services you haven't asked for.

Other giveaways include being refused a service – such as a credit card or loan – despite having a good credit history or having a mobile phone set up in your name without your knowledge. JA

The below article reports on the financial loss organisations have taken as the result of ID theft (Metro, September 18th 2006).

Company ID theft costs firms £50m

BY SARAH HILLS

COMPANIES lost £50million to fraudsters stealing their identities last year – and will be losing 14 times that amount by 2020, a report warned yesterday.

In an echo of the boom in personal ID theft – which has seen one in ten people having their bank details used by thieves – corporate identity theft is one of the fastest-growing risks to firms.

Criminals hijack a legitimate business's name to trade on its credit and reputation, and potentially to steal its assets and empty its bank accounts, the study by insurer Royal & Sun Alliance said.

Firms with more than 250 staff are saddled with the biggest share of losses, researchers found.

Those in communications, banking, finance and insurance have become particularly common targets.

London firms are forecast to be hit by the greatest increase in costs, at £140million by 2020.

Rapid damage to a company's reputation is one big danger, the study says.

Simon Wallace, of the Centre for Economic and Business Research, said: 'We are on the cusp of a potential boom

in corporate identity theft. With almost universal computer usage and Internet coverage in the business environment, the potential for corporate identity theft is more significant than ever.

'Those willing to hack, scam and defraud will find new and technically advanced methods to open up the necessary loop holes and steal a firm's identity.

'Business will need to adapt to this risk and must be willing to increase their spending on new and improved IT security systems in order to fend off attacks and stay one step ahead.'

Jon Woodman, director of risk solutions at Royal & Sun Alliance, said: 'It is important to take measures to minimise exposure to fraudsters and have a good security policy in place.'

Firms are advised to check their details at Companies House, make sure they own every variant of their names online, and dispose of corporate stationery, including letterheads and bank details, in a secure way.

This next article aims to warn users of one of the most heavily used websites for buying and selling about the various threats they should be cautious of (Metro, January 9th 2006).

Monday, January 9, 2006 **METRO** 9

eBay sellers warned over PayPal swindle

BY OLIVER STALLWOOD

TRICKSTERS are duping eBay users into giving goods away for free in a new scam on the Internet auction site.

A seller is emailed asking if the item can be sent to Africa – even if the victim has agreed to post only to the UK or Europe.

The buyer offers £40 postage using PayPal, an eBay firm allowing online payments.

Then an email allegedly from PayPal says the money has been received and seeks a Royal Mail tracking number.

If that is not sent, an email purportedly from eBay threatens action against the seller's eBay account.

The aim is to pressure victims into mailing the goods, even though they have never been paid.

IT boss John McGregor was almost duped by the scam when he tried to sell his mobile phone on eBay. But the Internet security specialist was able to spot that the emails were not legitimate.

He said: "The real concern is that there

A LEFTOVER Christmas sprout has fetched £1,550 on eBay. Leigh Knight, 18, put the sprout up for auction as a joke after saving it from the rubbish while washing up. Bids started slowly at £1 and someone even offered a carrot in exchange. After receiving the money from a buyer called Rachel, Leigh has given it to charity.

are thousands of people who may get caught and taken for a ride.

The con is believed to originate from Nigeria. PayPal and eBay yesterday said its safeguards were 'a world class example of the tools that can be put in place to prevent these attacks'.

Members suspecting a hoax email should send it to spoof@ebay.co.uk or spoof@paypal.co.uk.

Within a few minutes, they will get a response confirming whether or not it is genuine.

The final article clipping demonstrates the value of information on office computers which seems to remain unrecognised by employees and employers (Metro, February 12 2007).

Monday, February 12, 2007 **METRO** 21

Who's got hold of your work secrets?

BY JOHN WARD

YOU might think your personal details are safe with your employer – but what happens when your work computers are replaced?

Most companies are not doing enough to stop their secrets – and yours – falling into the hands of fraudsters when they get rid of old machines, a report warns.

Less than half use expert firms to destroy used PCs, with most selling the units to employees or on the second-hand market, a survey of 329 British companies found.

Crooks are then able to obtain sen-

sitive information from the hard drives. The risk of identity fraud is soaring because many machines end up in West Africa, where ID theft and corruption scams are rife.

'We have all heard about PCs thrown away in council tips that have ended up in West Africa, with local extortionists and opportunists selling the contents, such as bank account details, for less than £20,' said Martin Allen, of data security firm Pointsec, which carried out the survey. 'Many

corporations also sell their old PCs to second-hand dealers who often do not have the skills or resources to clean them adequately.'

Only 17 per cent of firms destroy the equipment themselves. Mr Allen added: 'People store so much valuable information on computers – eight per cent store passwords and six per cent bank account details.'

If you want to recycle your PCs, Mr Allen suggests you donate them to charities such as Computer Aid International, which clears hard drives and sends them to developing countries.

