Personal Internet Security

The House of Lords Select Committee on Science and Technology

October 2006

A. **Defining the problem**

1. **What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?**

1.1 There are a number of threats to individuals' security on the Internet. Very generally these fall into two categories: attackers gaining access to information that they should not; and attackers having control over computer systems that they should not have access to.

1.2 The largest single threat to private individuals comes from those attempting to gain access to personal information in order to use this information for fraud. The most common type of attack in this class is known as 'phishing', in which a user is tricked into divulging confidential information such as bank account details to a third party (typically by getting an email supposedly from a bank, which asks them to go to a webpage and enter passwords and other details). The goal of a phishing attack is usually to enable either direct fraud or more general identity theft. By gaining access to private, personal information, bank accounts may be accessed, loans obtained in the name of the victim or documents obtained to further longer term fraud. The same techniques for gaining personal information may also be used for other types of privacy violation including stalking.

1.3 Another common route for gaining access to an individual's personal information is to gain access to that user's computer. If the attacker can install a program onto the user's computer, either by means of a computer virus or by having the user accept a 'Trojan horse' program[1], then the attacker may misuse the computer in a number of ways. The program may be used to send details of the user and information about their user names and passwords for web sites back to the attacker. The program may also enable the attacker to use the computer as a 'zombie', remotely using the computer for further malicious purposes. This may include commanding the computer to send out junk advertising email; using it to spread viruses; or using it, alongside many other computers, to access a particular server in order to overwhelm it in a 'denial of service' attack.[2]

1.4 The use by home users of always-on broadband and wireless Internet increases the risk of malicious companies or persons gaining access to computers owned by private individuals.

2. **What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?**

2.1 Reliable figures for the scale of the problem are hard to come by, for three major reasons. First, most reporting on the problems comes from companies in the business of selling tools to help combat the problems, so it is possible that the figures are exaggerated. Second, figures for the level of fraud resulting from illicit computer access are even harder to come by, since banks are unwilling to admit liability and frequently deny that customer accounts could be compromised without the complicity

[1] A malicious programme disguised as, or hidden within, legitimate software. A Trojan can be contrasted with a virus in that a 'virus' is malicious code that is attached to an otherwise bone fide program or file, whilst a 'Trojan Horse' is software that purports to provide useful functionality, but has deliberately been designed to include malicious code.

[2] Denial of service attacks usually target high-profile websites, seeking to bring them down by overwhelming the server that hosts them. Threats of such attacks have, in the past, been the basis of blackmail cases.

of the customer. Third, evidence of an attempted attack is usually only found by exploring a computer system, and in many cases it is likely that most users live in ignorance of security breaches until, say, a false transaction appears on a credit card statement.

2.2 Despite these difficulties, some judgements can and have been made about the levels of threat. It is obvious to most Internet users that phishing email scams have reached epidemic proportions. Many users receive multiple phishing emails each week. With regard to the level of infection with Trojan programs, the numbers vary by region but a recent survey put the rate above 30% of Windows PCs (though a caveat applies here, as this report was produced by a company with a business interest in this area).[3]

3. **How well do users understand the nature of the threat?**

3.1 Most users are aware that there is a problem but few are aware of the detailed nature of the threat. Phishing scams are confidence tricks and any success they have is due to a lack of detailed understanding of the threat. Phishing scams have become increasingly sophisticated, since making a convincing fake bank website is quite easy: the attacker can simply make a digital copy of a genuine site. Individual users need to be alert to the small details to know that a site is one created by a fraudster rather than a legitimate site. However, many banks and online vendors publicise warnings about phishing scams and give customers information on how to identify and avoid them.

B. **Tackling the problem**

4. **What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?**

4.1 One valuable way to help private individuals is to provide them with more information about what they receive, and what they are asked to download or run on their computers. This will enable them to make more intelligent decisions. The Oxford Internet Institute (OII) has a project entitled Stop Badware (see http://stopbadware.org) that seeks to do this. The website points out programs, such as screensavers and anti-spyware software, that in fact include spyware or other 'malware' that can be used to 'spy' on a computer (eg, check which Internet sites its user visits, or spy on keystrokes to find passwords), or interfere in its running. The aim is to inform and empower users so that they do not compromise the security of their computers by downloading such software. Projects such as this serve a useful purpose, but require support and funding to function.

4.2 However, while it is possible to seek to mitigate against the effects of 'Trojan Horses' by publishing lists that identify the software concerned, this is not possible in the case of viruses. Aside from not downloading any executable files, the key mitigation available to an individual to combat viruses is the use of up to date anti-virus software. The installation and use of firewalls on PCs is also of great value in protecting individuals from various threats.

4.3 Computer system vendors would do well to spend more time thinking about how to allow the user to make informed decisions, with effort in the areas of user interface design and mechanisms that let the user ensure that they are talking to the correct

[3] http://www.webroot.com/resources/stateofspyware/excerpt.html

web site. However, those in the computer security product business have a vested interest in selling things. There is already evidence of various false alarms from one or more of the vendors. Therefore, independent sites like Stop Badware may be more helpful. There is also a need to keep educating users to ensure that they always download the latest security patches for their operating system and the latest updates for any anti-virus software that they are using.

4.4 In addition to informing users, much more could be done to make computer operating systems less vulnerable to viruses and malicious code that can be installed without the users' knowledge. Windows is particularly vulnerable to malware, whereas other operating systems such as Linux and MacOS tend to be less vulnerable – though they are not free from vulnerabilities.

5. **What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?**

5.1 The Oxford Internet Surveys (OxIS) are tracking public uses and opinions about the Internet and have information relevant to the level of public awareness and concern. They reveal that most users are aware of threats, and most users have done something to address their concerns. For example, when asked: 'How concerned are you about protecting your computer from viruses?', only 12 percent of users said they were 'not concerned'. 65 percent said they were 'concerned and have done something' to address it. These statistics are presented in the report *The Internet in Britain: The Oxford Internet Survey (OxIS)*.

5.2 However, despite fairly high levels of awareness and concern about threats in general, the level of awareness of the actual threats is fairly low. Scare stories from parties with vested interests are widely reported by the press with over-simplification and sensationalism in reporting sacrificing the accuracy of the reports. Balanced and informative coverage of the issue is often judged too technical to be widely reported. As a result many people are worried about spurious threats while being ignorant of the real problems.

5.3 For those who have some awareness, there are various resources on the Internet but care is required because of the vendor self interest. Initiatives like Stop Badware could be useful for raising public awareness, as could the Government-run 'Get Safe Online' initiative. However, these need significant publicity in order for the wider public to benefit from them.

6. **What factors may prevent private individuals from following appropriate security practices?**

6.1 There are two main factors that hinder individuals' adherence to security procedures: ignorance and haste. When presented with a security critical decision, for example, when a pop-up box appears before downloading a program, many users view it as an obstacle to the download and simply click 'OK'. However, if the user was aware of the significance of the decision they may be less hasty. If the computer systems presented the security questions to the user in a more understandable manner, explaining the risks that the user takes in downloading a program, and if users were better educated as to the impact of making the wrong choice, then users would be more likely to follow appropriate security practices.

7. **What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?**

7.1 Engineers of all disciplines have a duty to ensure that their systems are 'fit for purpose'. The concern is that, currently, some computer software is not 'fit for purpose' with respect to issues of personal security. Therefore, better software, both at the operating system level and at the application level, would be hugely helpful in addressing this. For example, Trojan horse code derives its power from the poor level of separation of functional roles on most personal computers. Operating systems which better separate functional roles would give a degree of damage limitation in the face of Trojan code. Computer viruses propagate through weaknesses/bugs in the operating system. Fixing the bugs, or building systems with fewer bugs in the first place, would slow the propagation of viruses.

7.2 Hardware security devices can also be helpful for personal computers, though only with the co-operation of the software. Trusted Platform Modules (TPMs – modules that enhance security by cryptographically scrambling and controlling access to messages and stored data) are starting to appear on personal computers and these can, in theory, help with protecting user data but ultimately it is the software that is the critical factor.

7.3 Another possibility is the development of system designs and products that manage machines remotely for retail users. This remote management is normal practice for most corporations. Such remote management can ensure that all the patches that have been developed to combat known vulnerabilities of the computer operating system and software applications have been installed, that up to date anti-virus software is in place, and that the traffic flowing to and from the computer is under the control of an appropriately configured firewall.

7.4 Developments could be made to the design of access to websites such as banking websites, to prevent phishing attacks. An interesting example can be found on http://www.tricerion.com/. On this website Tricerion present a demonstration of a log-in procedure designed to prevent phishing attacks. They have incorporated a number of features into the login procedure, for example, presenting the characters of a user's password on a keypad displayed on the computer screen, which the users click on. This means that any programs designed to detect keystrokes cannot spy on the password. Moreover, they keypad is designed to look different for each user, and will only display a selected number of characters, so if the keypad looks unfamiliar, or does not have all of the digits in the user's password, they will know they are not at the genuine site. Tricerion also suggest using symbols for the password that are unique to a particular online service, such as a banking website. The user can only enter their password on a keypad displayed on the genuine site, meaning they cannot accidentally divulge it to a third party, eg via a phishing email.

7.5 These are examples of good practice that could be explored further. More research on novel ways to circumvent phishing scams or spyware would be of great benefit.

8. **Who should be responsible for ensuring effective protection from current and emerging threats?**

8.1 Operating system vendors are in the strongest position to build effective tools. There would be value in exploring ways that vendors could be made legally culpable when faults lead to security problems.

8.2 However, security threats to computer users are well-publicised, so there is also an onus on the users them to protect themselves. They could receive assistance in this matter by making self-protection easier, in the ways described above.

9. **What is the standing of UK research in this area?**

9.1 The UK has many well respected researchers in this area and is probably second only to the USA in the field.

C. **Governance and regulation**

10. **How effective are initiatives on IT governance in reducing security threats?**

10.1 Unless the issue of Internet Governance is resolved there is very little possibility of resolving the Personal Internet Security issue. The OII is involved with efforts to inform the new Internet Governance Forum, set up by the UN, and is supportive of security being one of the key issues that the forum should pursue.

10.2 However, initiatives in this area are frequently effective in the area of corporate security but with home users there is much less evidence of success. It is arguable that the best way to address security is to inform and empower users and to participate in balanced and credible efforts to achieve self-governance for Internet entities.

11. **How far do improvements in governance and regulation depend on international co-operation?**

11.1 The international nature of the Internet means that threats from the Internet are an international problem. Hence Internet governance is not an issue for an individual government, it is a global issue that concerns every individual globally and one country cannot legislate for all.

11.2 It is important to be aware that some governments have the objective to control and restrict the individual freedom of expression on the Internet, and wish to impose censorship rules. All governments should sign and adhere to an Internet user's 'bill of rights'. It is often the case that some countries with the strong views actually have low Internet penetration and usage. Hence a 'one country equals one vote' rule should not always apply.

11.3 It is important that in Internet governance there is cooperation between various branches of government and law enforcement in and between countries. Civil society should be fully involved and take part in the process, which should be fully transparent. User and business associations (NGOs) should be represented directly in any regulatory body, not just through their national governments.

12. **Is the regulatory framework for Internet services adequate?**

12.1 The Internet has benefited hugely from the very light hand of regulation to date and those benefits almost certainly outweigh the risks. Further regulation would be likely to reduce the social and economic benefits of the Internet.

12.2 There is, however, one area in which regulation of software and services might help security, although it is likely to be very unpopular with software vendors. At present most software vendors demand, in their End User License Agreement, that

the user gives up any right of recourse in the event that faulty software leads to loss or damage to the user's data. Furthermore, some vendors refuse to fix security problems in older versions of software and demand that users pay to upgrade to a more recent version in order to gain access to security fixes. There would be value in investigating the potential benefit to end users of imposing restrictions on these practices.

13. **What, if any, are the barriers to developing information security systems and standards and how can they be overcome?**

13.1 The barriers to developing information security systems are cost and inertia. New systems with better security characteristics are being developed all the time but it takes time before users upgrade and, as mentioned above, they frequently have to pay for the privilege of better security.

D. **Crime prevention**

No comments from The Royal Academy of Engineering.

Submitted by:
Mr Philip Greenish CBE
Chief Executive
The Royal Academy of Engineering

Prepared by:
Dr Natasha McCarthy
Policy Advisor
20th October 2006