Parliamentary Office of Science and Technology

postnote

October 2006 Number 271

COMPUTER CRIME

An increasing number of domestic and international criminal activities are using the Internet. Computers and other electronic devices can be tools to commit crime or are targeted by criminals. A personal computer connected to the Internet without protection may be infected with malicious software in under a minute. This briefing discusses the scale and nature of computer crime, the technologies available to protect computers, and highlights the key policy challenges.

Background

The increasing range of programmable electronic devices, from set-top TV boxes to mobile phones, means that 'computer' crime can affect more than just personal computers (PCs). They and other electronic devices are particularly vulnerable to attack because they are flexible, can be reprogrammed, and are frequently networked with other devices. There are two main ways by which computers can be involved in crime (some examples are given in Box 1):

- old crimes conducted using computers as a tool: for example storage of illegal images on a hard disk instead of in print; harassment using mobile telephones or illegal downloads of music and other forms of piracy. Another example is 'phishing': confidence tricks involving spoof emails and fraudulent websites to acquire sensitive information (see Box 1).
- new types of crime made possible by specific technologies. One example is denial of service attacks or DoS (Box 1) which prevent computer resources being available to intended users, for example by flooding web servers with more data than they can process, thus forcing websites offline. Other crimes involving attacking a computer (often by 'hacking' or gaining unauthorised access to a computer system), or writing a virus (a type of malicious software or 'malware', see Box 2) to delete stored data.

Box 1. Examples of computer crime

Phishing scams and fraud
A 'phisher' may use spoof emails to direct a computer user to fraudulent websites to elicit a transfer of money, or sensitive information such as passwords or credit card details, from the user. Attacks are increasing, with financial services accounting for over 93% of impersonated or hijacked brands through bogus websites and emails.[1] Almost all of the UK's high street banks have been affected by phishing.

Distributed Denial of Service (DDoS) attacks
Criminals can gain control of multiple computers and use them to attack a specific target or targets. This was done in 2004 by a Russian crime gang in an extortion attempt on UK gambling websites during the 2004 Grand National. The National High Tech Crime Unit (NHTCU) acted with Russian authorities to arrest those responsible and helped set up the Internet DDoS forum to share data about attacks.

Types of attack

There are different types of attacks on computers which may:

- attempt to access information stored on a computer. Information may have a sale value (corporate espionage), may be valuable to the owner (ransom opportunity) or may be useful for further illegal activity such as fraud.
- try to impede or alter the functioning of the computer itself. Also, if a computer can be controlled it can be used to send spam, host illegal content, or conduct further attacks.

Targets of computer crime

Some attacks do not have a specific target. However, attacks against specific computers or groups of computers are becoming more common. Home computer users, organisations with large networks of computers, or entire infrastructures may be targeted. Attackers using computers may also attempt to damage the functioning of the Critical National Infrastructure (CNI) which includes emergency services, telecommunications, energy distribution and finance, all of which rely on IT. Many CNI systems which were once isolated are now connected to the Internet, increasing their vulnerability.

There has been speculation over the prospect of terrorists using electronic attacks to target computer systems and networks. According to the National Infrastructure Security Coordination Centre (NISCC) the probability of terrorists carrying out an electronic attack against the CNI is currently low compared with other risks such as using explosive devices, although the NISCC points out that threats can change quickly.

Box 2. Malicious software types ('malware')

The uses of malicious software range from placing excessive demand on a computer's resources, to destruction of data or even hardware. In some cases the user is made aware of the presence of the malware, for example when it sends a message to the user or deletes the contents of a hard drive. Recent forms of malware may operate without the user's knowledge, steal financial information such as credit card details, or convert infected computers into an asset for the attacker. Common types of malware work as follows:

- **Viruses** infect computers or other electronic devices and are passed on by user activity, for example by opening an email attachment.
- **Worms** self-propagate using an internet connection to access vulnerabilities on other computers and to install copies of themselves. They are often used as a conduit to grant attackers access to the computer.
- **Trojans** are malware masquerading as something the user may want to download or install, that may then perform hidden or unexpected actions, such as allowing external access to the computer.
- **Spyware** transmits information gathered from a computer, such as bank details, back to an attacker. For example 'keylogging' software records anything entered using the keyboard, such as passwords.

Increases in computer crime

The 2002/03 British Crime Survey showed that 18% of households with internet access said their home computer had been affected by a virus. This had increased to 27% in 2003/04. One-third said the virus had damaged their computer.[2] The biennial Department of Trade and Industry (DTI) Security Breaches survey reports that 62% of UK businesses had a computer security incident in the 2006.[3] These statistics may underestimate the real situation as many organisations or individuals may be unaware that the security of their computer has been compromised. There are various reasons for the increase, outlined below.

Spread of computers

Computers are becoming more accessible as their cost decreases, leading to a marked growth in their use, particularly in personal and mobile computing. Studies suggest that many home users are typically unaware of the potential threats from computer crime or may not possess the technical skills to ensure their own security.

Broadband

Latest information from Ofcom shows that approximately half of all internet connections in the UK are high-speed, always-on, broadband connections, with 30% of households using this technology.[4] These connections allow greater volumes of network traffic, and when coupled with poorly implemented security measures increase the likelihood of computer attack.

Increasing financial motivation for computer crime

Information security experts suggest that the motives behind computer crime have changed. Traditionally it was motivated by desire for peer recognition and to demonstrate technical skills. However, it is now increasingly financially motivated. The growth of e-commerce, with 45% of internet users participating in some form, and the dependence of many aspects of financial life on computers, have motivated this shift. Evidence can be found in the occurrence of extortion attempts, thefts of credit card details and phishing. More people are producing malware to make money.

Legislation

Criminal law generally applies to illegal acts regardless of the medium used to commit the act. An exception is the Computer Misuse Act (CMA) 1990 (Box 3) which focuses specifically on computers.

Box 3. Computer crime legislation

The Computer Misuse Act (1990) is the only legislation that explicitly and solely focuses on computer crime. The act created three offences: unauthorised access to computer material; unauthorised access to a computer system with intent to commit or facilitate further offences; and unauthorised modification of computer material.

The Data Protection Act (1998) requires personal data held by organisations to be stored securely. Section 55 of the act includes the offence of unlawful gathering of personal data, including information stored on computers. In the 2006 '*What Price Privacy?*' report, the Information Commissioner called for sentences for this offence to include imprisonment.

The current Police and Justice Bill contains amendments to the Computer Misuse Act. These are intended to bring UK law in line with the Council of Europe Convention on Cybercrime and the European Council Framework Decision on Attacks against Information Systems 2005/222/JHA. The European Council decision was adopted in 2005 and must be transposed into UK law by March 2007. The amendments include:

- penalties for the offence of attempting to gain unauthorised access to a computer being increased from a maximum sentence of six months to two years;
- penalties for the offence of unauthorised attempts to impair the operation of a computer being increased from a sentence of five to one of ten years;
- denial of service attacks being explicitly criminalised;
- introduction of an offence of making, adapting or supplying tools for use in CMA offences.

Computer crime prevention and investigation

Box 4 lists key government or government-funded bodies involved in computer crime prevention and investigation. Ofcom, the UK communications regulator, is responsible for content standards on broadcast platforms, but it does not regulate media distributed over the Internet to devices such as mobile phones and PCs. Recent research by Ofcom suggests that online consumer protection issues require a broad range of solutions, with a much greater role played by industry and consumer self-regulation than is the case for broadcast media.

Box 4. Who's who in combating computer crime

Local police forces
All UK forces have some form of computer crime forensic and investigation capability. The Home Office says people who believe that they have encountered computer crime should contact their local police force for assistance. Other more specialist agencies may become involved if necessary.

Serious and Organised Crime Agency (SOCA)
SOCA's remit is to reduce harm caused by organised crime. Computer crime policing in the UK was formerly overseen by the National High Tech Crime Unit (NHTCU). As part of the Serious and Organised Crime Act 2005, NHTCU has been amalgamated into SOCA, which has an e-crimes directorate and twice the staff of NHTCU.

Child Exploitation and Online Protection Centre (CEOP)
The Internet is seen as a means of networking between child sex offenders, and of providing opportunities for contact with children. The CEOP runs a website and an offline education campaign to advise young people and their parents about online awareness and safety.

Communications Electronics Security Group (CESG)
CESG is the National Technical Authority for Information Assurance (ensuring that communications and IT systems are secure and reliable) for UK Government agencies, armed forces and various bodies in the public and private sectors.

National Infrastructure Security Coordination Centre (NISCC) This cross-governmental centre works to reduce the risk to Critical National Infrastructure from electronic attack and acts to co-ordinate and promote information sharing.

Government Departments
The Home Office has a computer crime policy team while the Department of Trade and Industry produces a biennial information security breaches survey, web resources and other publications. It advocates international security standards and promotes these through an industry group. Finally, the Cabinet Office contains the Central Sponsor for Information Assurance and plays a lead role in 'Get Safe Online' and 'ITsafe', the government warning and alerting systems for computer viruses and technological flaws.

Issues

This section examines challenges faced in tackling computer crime, through lack of statistics on its scale and limited user awareness. It discusses technical solutions and measures taken by the government, commercial vendors, Internet Service Providers (ISPs) and individual users.

Assessing the scale of computer crime

Other than Computer Misuse Act 1990 offences (see Box 3), crimes that involve computers are not separately recorded. This makes identification of computer crime in government and police crime statistics difficult. Fewer than 1 in 4 police forces can generate any records of computer crime, nor is it one of the target measures by which police performance is assessed. Some organisations, including businesses, are reluctant to disclose security incidents for fear of damage to their reputation. However, sharing information about computer security breaches is seen by security professionals as necessary for defending against computer crime threats. The British Crime Survey also highlights that many home users do not report incidents to the police, but rather to their ISPs or website administrators.

User awareness

There is limited awareness of computer security among home as well as business users. Inadequately protected computers can be easy targets for unauthorised users. 'Get Safe Online' is a joint Government-industry initiative to provide computer security advice (Box 5). Their studies show that users tend to assume they know how to remain safe online, but they do not demonstrate adequate skills when tested.[5] Respondents rated computer security as a high priority but over half admitted to little or no knowledge of safe practices. Although 75% had a firewall (Box 6), 86% did not follow recommendations to update their security software.

Box 5. Get Safe Online

The Government–industry partnership education initiative 'Get Safe Online' is the first national internet-based computer security awareness campaign for the general public and small businesses. The 'Get Safe Online' website has 13,000 websites which are linked to it. It provides information to individuals on how to protect themselves, their families or their business from online threats. It recommends taking basic precautions such as using a firewall, anti-virus and anti-spyware software and keeping all security software updated.

Businesses and other organisations also face risks through lack of user awareness even when they have taken computer security measures. Trends towards mobile working mean that computers are often outside organisational security perimeters. Three-fifths of UK businesses do not have a formal information security policy. The DTI recommends that information security should be part of good business practice, through staff education and implementation of security policies.

Technological solutions

A range of technologies is available to home users and organisations to secure their computers (Box 6).

Box 6. Technological solutions

If correctly installed, the following can help to block attacks:

- **Firewalls** are hardware or software devices that block certain network traffic according to their security policy.
- **Software solutions** exist to identify and remove malware and to help manage spam email. Many must be paid for but free versions are also available.
- **Authentication** involves determining that a particular user is authorised to use a particular computer. This can include simple mechanisms such as passwords, to more complex methods using biometric technology.
- **Hardware cryptography** uses computer chips with cryptographic capabilities intended to protect against a range of security threats.
- **Patches** are programs designed by software manufacturers to fix software security flaws. Patching is often installed automatically. This reduces end-user participation and increases ease of use.

The onus is currently on home users to acquire and install these solutions themselves and to follow advice available from sources such as 'Get Safe Online'. However, even if users are aware that they should secure their computers, the technology may not be user friendly. Some software even presents users with options which may make their systems less secure. Ofcom, in conjunction with the Home Office and the British Standards Institute, has been working on standards and a kite-marking scheme for some computer security tools, to improve consumer confidence, and product quality and usability.

Software manufacturers

Software manufacturers are under pressure to release their products rapidly due to the competitive nature of the market. Because of this, software can often contain flaws. When these flaws are discovered, manufacturers respond with 'patches' (see Box 6). Months can elapse between flaw discovery and patch creation but there can be as little as a few days between discovery of a flaw and creation of code to exploit that flaw (a virus for example). This leaves a large window of vulnerability. Even with automation, many systems go 'unpatched'. Installing and testing security patches can lead to loss of operating time and may even introduce new security flaws.

Policing

Although all UK forces have some form of specialist computer crime forensic and investigation capability, police forces face challenges in tackling computer crime:

- The international nature of computer crime means that determining jurisdictional responsibility can be difficult, for example if crimes are committed in the UK by criminals overseas.
- Data can be stored on a range of devices and in large volumes that require time and expertise to access.
- Computer crime training has been made available to all officers, but uptake has been low. This may result in potential evidence of computer crime being lost.
- Specialist investigative staff are costly: they need up-to-date equipment and continuous training, due to the rapid pace of technological development.

The Association of Chief Police Officers (ACPO) recommends that computer crime should be treated as part of mainstream policing and that non-technical staff be sufficiently skilled to recognise and make use of digital evidence.[6] Some hold the view that the recent incorporation of the National High Tech Crime Unit into the Serious Organised Crime Agency creates a gap between local forces and national levels of policing, leaving victims of some computer crimes unsupported.

The Internet Watch Foundation (IWF) is an independent, UK industry-funded organisation. It works with the government, police and ISPs to minimise the amount of illegal material on the Internet. It operates a reporting system to help law enforcement agencies and ISPs to investigate and remove images of child abuse hosted worldwide. However it can act against criminally obscene or racist material only where it is hosted on UK-based web servers.

Whose responsibility?

Many consumers assume that their ISP is taking active steps to protect them from spyware, spam or other malicious activity. However, home users are largely responsible for their own computer security. Moreover, they may not realise that they themselves are acting illegally if malware on their PC produces spam or sends viruses to other PCs. Users surveyed for 'Get Safe Online' believe that online companies, along with banks and the government should do more to protect them from computer-mediated fraud and attack. The UK Internet Service Providers' Association (ISPA) has a Code of Practice for its members.[7] While ISPA considers that content providers, not ISPs, are responsible for the legality of content, they are expected to adhere to ISPA guidelines on the removal of illegal content on websites. European Directive 2002/58/EC requires ISPs to take appropriate measures to safeguard the security of their services. Most ISPs also have an acceptable use policy for consumers, contravention of which can lead to them being disconnected from the service.

Overview

- Computers are increasingly being targeted by criminals or used as tools to commit old and new types of crime.
- Legislative change to address the increase in and diversity of computer crime is in progress. However, policing computer crime is resource-intensive, complex and requires support from a number of organisations.
- There are several technologies available to improve computer security but their effectiveness may be limited without user awareness and education.
- Responsibility for securing computers against crime largely rests with the user (individual or organisation), although there is debate over whether the government and industry should do more to protect users.

Endnotes

[1] Anti-Phishing Working Group, *Phishing Activity Trends Report*, July 2006, www.antiphishing.org/

[2] The Home Office, *Fraud and Technology Crimes: Findings from the British Crime Survey 2003/4, the 2004 Offending Crime and Justice Survey and administrative sources,* September 2006

[3] Department of Trade & Industry, *Information Security Breaches Survey: Technical Report*, April 2006 06/803

[4] Ofcom *Media Literacy Audit*, March 2006

[5] Get Safe Online report, www.getsafeonline.org/

[6] Association of Chief Police Officers, *Strategy for the Investigation of Computer Enabled Criminality and Digital Evidence*, January 2005

[7] www.ispa.org.uk

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of public policy issues that have a basis in science and technology.

POST is grateful to David Wills for researching this briefing, to the ESRC for funding his parliamentary fellowship and to all contributors and reviewers. For further information on this subject, please contact the co-author Dr Sarah Bunn at POST.

The Parliamentary Office of Science and Technology, 7 Millbank, London
SW1P 3JA; Tel: 020 7219 2840; email: post@parliament.uk

www.parliament.uk/parliamentary_offices/post/pubs2006.cfm