Cybercrime: Vandalizing the Information Society

Steven Furnell

Network Research Group, Faculty of Technology, University of Plymouth,
Plymouth, United Kingdom
sfurnell@plymouth.ac.uk

Abstract. Cybercrime has received significant coverage in recent years, with the media, law enforcers, and governments all working to bring the issue to our attention. This paper begins by presenting an overview of the problem, considering the scope and scale of reported incidents. From this, a series of common attack types are considered (focusing upon website defacement, denial of service and malware), with specific emphasis upon the potential for these to be automated and mounted by novices. Leading on from this, the problem of policing cybercrime is considered, with attention to the need for suitable legislation, and appropriate resourcing of law enforcers. It is concluded that that cybercrime is an inevitable downside of the information society, and that organizations and individuals consequently have a stake in ensuring their own protection.

1 Introduction

Cybercrime is now recognized as a major international problem, with continual increases in incidents of hacking, viruses, and other forms of abuse having been reported in recent years. Although the problem of computer crime has been apparent since the early days of computing, the difference today is the increased scope available to would-be attackers – largely due to the popularity of the Internet. The numerous benefits offered by the Internet and, in its turn, the World Wide Web have now led to their widespread public adoption. At the same time, however, their increased usage has also amplified the accompanying problems, and not a day seems to go by without a cybercrime incident of some kind being reported.

The majority of Internet users, whether corporate or consumers, have little appreciation of the online world in which they participate. They do not understand how the system works, and quite legitimately they have no wish to. However, although a detailed understanding of the technology is not necessary, Rheingold observes that the opportunities it offers can only be realized by an informed population [1]. Similarly, an uninformed population is more likely to find itself vulnerable to the risks. As such, an awareness of cybercrime problems is not only prudent, but also increasingly essential.

J.M. Cueva Lovelle et al. (Eds.): ICWE 2003, LNCS 2722, pp. 8–16, 2003.

2 The Cybercrime Problem

At the most basic level, cybercrime is clearly a crime involving the use of computers. However, this is obviously a very broad classification, and in order to define the topic more precisely, it is useful to sub-categorize the issue. A useful classification is provided by the UK Audit Commission, which has been conducting computer crime and abuse surveys since the early 1980s. In the most recent version of their survey, released in September 2001, the Commission suggested the categories and associated definitions below [2]. This is by no means the only classification, and various other views are possible [3], but this provides a manageable list that does not group too many distinct issues together.

- **Fraud:** Private gain or benefit by: altering computer input in an unauthorized way; destroying, suppressing or stealing output; making unapproved changes to stored information; or amending or misusing programs (excluding virus infections).
- **Theft:** Theft of information.
- **Use of unlicensed software:** Using unlicensed copies of software.
- **Private work:** Unauthorized use of the organization's computer facilities for private gain.
- **Invasion of privacy:** Breaches of data protection legislation.
- **Hacking:** Deliberately gaining unauthorized access to an information system.
- **Sabotage:** Interfering with the computer process by causing deliberate damage to the processing cycle or to equipment.
- **Introduction of unsuitable material:** Introducing subversive or pornographic material, for example, by downloading from the Internet.
- **Virus:** Distributing a program with the intention of corrupting a computer process.

Having introduced the scope of the problem, another relevant factor is the scale. Some specific statistics are presented in the later discussion of common attacks, but it is useful to get a general overview that includes some evidence of the pattern over time. A good example in this respect comes from the Computer Security Institute (CSI), which has been conducting annual surveys in the United States since 1996. As Fig. 1 illustrates, there has been a notable increase in the proportion of organizations experiencing unauthorized use of their computer systems.

In total, the CSI's 2002 survey reported losses approaching $171 million, from 41 respondents who were willing and able to quantify the financial impacts of their incidents [4]. With an average loss per incident of over $4.1 million, this is not a problem that one should dismiss lightly. It is also worth noting that financial loss is merely one type of impact that may result from cybercrime. Other impacts, such as disruption to services, loss of data or damage to reputation, are more difficult to quantify and may actually be more significant in many contexts.

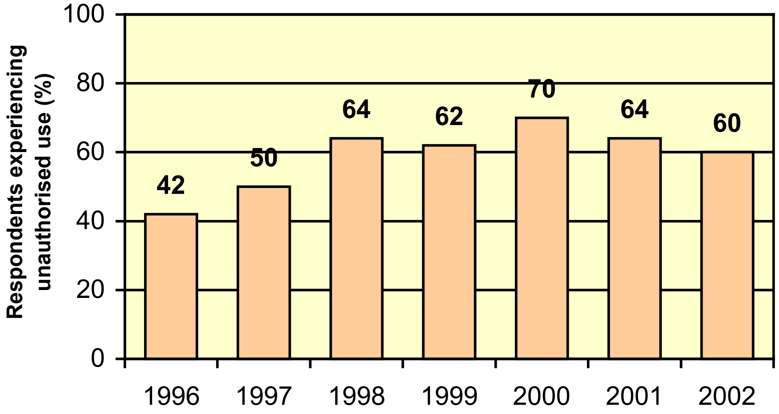


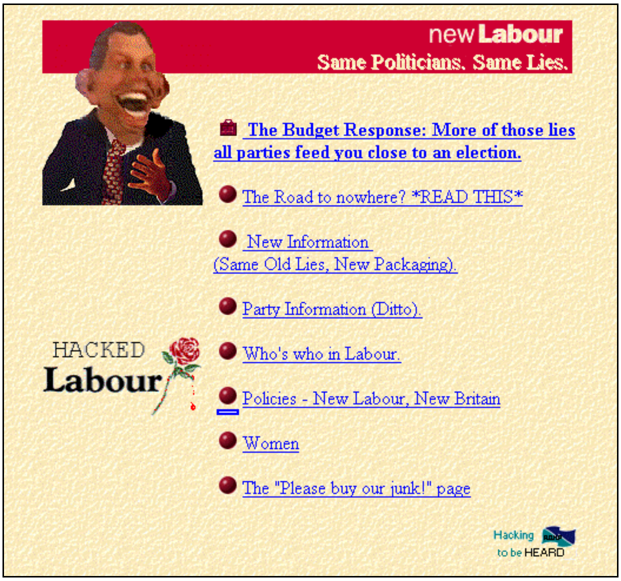
Fig. 1. CSI/FBI Computer Crime and Security Survey results 1996-2002

3 Common Forms of Attack

As the classifications in the previous section have identified, cybercrime can manifest itself in a number of guises. This section considers some of the most commonly encountered incidents – namely website defacements, denial of service, and malware – that frequently occur in the Internet environment.

3.1 Defacing Web Sites

The defacement of web sites has become very popular in the last five years, and is an attack that falls quite literally under the heading of vandalism suggested by the title of this paper. Defacing a site enables hackers to leave their mark in a very visible manner. While such an attack does not necessarily result in any breach of privacy, financial loss or even significant disruption, it does have the potential to cause significant embarrassment to the affected organization. In addition, to the casual observer who logs into the site during the period in which it has been affected (or hears reports about it in the media), the nature of the breach may seem more significant. Results from the CSI/FBI survey [4] suggest that vandalism is the most common form of web-related security incident. In the 2002 survey, 166 organizations indicated that their web sites had suffered some form of unauthorized access or misuse within the previous year. Of these, 70% cited the problem of vandalism [4]. Numerous high-profile organizations have suffered such attacks, including the CIA, the US Department of Justice, the New York Times, and online auction site eBay. An illustration is provided in Fig. 2, which depicts a fairly early website defacement, targeting the UK Labour Party back in 1996.



new Labour

Same Politicians. Same Lies.

The Budget Response: More of those lies all parties feed you close to an election.

The Road to nowhere? *READ THIS*

New Information (Same Old Lies, New Packaging).

Party Information (Ditto).

Who's who in Labour.

Policies - New Labour, New Britain

Women

The "Please buy our junk!" page

Fig. 2. The hacked UK Labour Party web site (6 December 1996)

Over the years, a number of websites have been created to monitor and record defacement activities, maintaining mirror versions of defaced pages. A notable example was Alldas.org, which began in 1998 – recording 74 defacements during the entire year. By 2001, however, this figure had risen to 22,379 defacements, and by February 2002 the volume of incidents became too much for Alldas to handle, and it ceased its mirroring activity (as a similar site, Attrition.org, had been forced to do the previous year for the same reason). One reason that so many defacements are possible is that web sites are being run on systems with vulnerable operating systems and servers. Hackers utilizing appropriate scanning tools can easily identify such systems, and then exploit the vulnerabilities in order to gain access (the exploitation is often handled by automated tools as well, removing the requirement for technical skill). Many systems continue to be vulnerable even when patches are made available, often because administrators are unaware of problems or have not prioritized the task of addressing them [5].

3.2 Denial of Service

The CSI/FBI findings suggest that denial of service (DoS) incidents represent the second most common form of website attack – with the aforementioned survey indicating that they were experienced by 55% of the 166 respondents. DoS attacks can range from fairly simple techniques, such as Ping of Death or SYN flooding, to more advanced distributed methods – all of which intend to undermine access for legitimate users. A significant example of the distributed DoS (DDoS) approach was witnessed back in February 2000, with sustained attacks that targeted Yahoo!, eBay, Amazon and other major sites [6]. A DDoS attack may involve potentially hundreds of computers, which then bombard other Internet sites with thousands of requests for information (the attacking systems typically participate unwittingly, with the DDoS attack code having been installed via stealth methods). The distributed attack is more difficult to combat, as the malicious traffic comes in from many sources and, in addition, the addresses may be spoofed, making them even harder to trace.

DoS attacks are popular with novice hackers, in the sense that they do not require any significant skill to implement (indeed, numerous tools are available to automate such attacks in software), but can nonetheless have dramatic and noticeable effects. Indeed, it has been conjectured that around 90% of hacking is conducted by people using such methods [7].

3.3 Malware

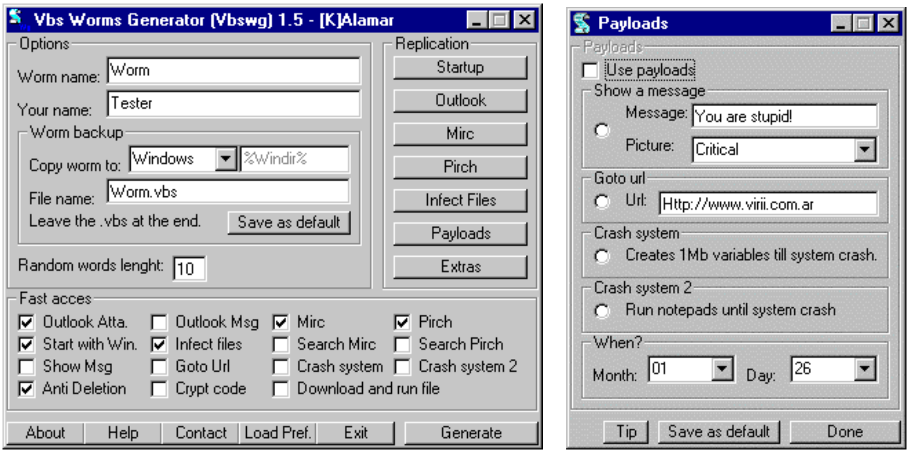
Although defacements and denial of service represent the most common targeted attacks against systems, by far the most common form of cybercrime relates to malicious software (or malware), such as viruses, worms and Trojan Horse programs. For example, 85% of the CSI/FBI respondents in 2002 had experienced a virus incident [4]. As of February 2003, anti-virus vendor Sophos was citing over 80,000 known virus strains [8], and the company claimed to have detected 7,825 new strains in 2002 – suggesting that the problem is far from disappearing. One of the significant reasons for this is the lower entry requirement placed before would-be malware writers. Related information and tools are now readily available on the Internet, including toolkits that enable someone with no technical skill whatsoever to create and release their own program. As with automated DoS and cracking tools, the problem with malware toolkits is that they make the task of releasing a virus or worm so easy that a complete novice could do it. An example of such a tool is the VBS Worms Generator, pictured in Fig. 3, which was used to create the so-called Anna Kournikova worm in February 2001 [9]. Creating a worm using this tool can be as simple as running the application, giving the worm a name, and selecting a payload for it to execute when it is triggered. The whole process (including locating, downloading and installing the application) can be accomplished in less than 5 minutes.

It may be noted that automation of the attacks has been a common theme in all of these cases, lending the techniques to script kiddies (novice hackers, lacking technical skills, but typically prone to causing mischief and malicious damage). The problem is that the ease of launching the attack does not reduce the damage and inconvenience that it can cause; it just makes it more likely that attacks will happen.

4 Problems of Policing Cybercrime

Given the problems that cybercrime can cause for organizations and individuals, it is unsurprising that society has been obliged to respond through legislative and policing initiatives. Many developed countries have now introduced relevant legislation to address the problem of cybercrime and associated activities. An example is the UK's Computer Misuse Act 1990, which can be considered reasonably representative of the issues that other countries have also taken into account when enacting cybercrime laws. The CMA introduced new three offences [10], as below:

1. "Unauthorised access to computer programs and data"
2. "Unauthorised access with intent to commit or facilitate the commission of a further crime"
3. "Unauthorised modification of computer material, that is programs or data held in a computer"


Vbs Worms Generator (Vbswg) 1.5 - [K]Alamar

Options

Worm name: Worm

Your name: Tester

Worm backup

Copy worm to: Windows %Windir%

File name: Worm.vbs

Leave the .vbs at the end.

Random words lenght: 10

Fast acces

☑ Outlook Atta. □ Outlook Msg ☑ Mirc ☑ Pirch

☑ Start with Win. ☑ Infect files □ Search Mirc □ Search Pirch

□ Show Msg □ Goto Url □ Crash system □ Crash system 2

☑ Anti Deletion □ Crypt code □ Download and run file

Payloads

Payloads

□ Use payloads

Show a message

○ Message: You are stupid!

Picture: Critical

Goto url

○ Url: Http://www.virii.com.ar

Crash system

○ Creates 1Mb variables till system crash.

Crash system 2

○ Run notepads until system crash

When?

Month: 01 Day: 26

(a) (b)

Fig. 3. The VBS Worms Generator (a) main options and (b) payload selection

The law has been successfully used a number of times during the last decade or so, and other countries with similar legislation have had comparable experiences. However, some more recent categories of attack do not fit comfortably within existing laws. For example, Denial of Service does not clearly fit as an offence under any of the Computer Misuse Act sections above – if all the attacker is doing is requesting a web page, then this clearly is not an unauthorized access, because the web server invites public access. Similarly, by simply requesting information, there is no modification of data involved. Consequently, laws need to be able to keep pace with the fairly dynamic landscape of new attacks. Another fundamental problem is that while computer crime is international, the jurisdiction of the law is not. Indeed, many countries have no cybercrime law at all (a situation that, in 2000 at least, applied to 60% of Interpol member countries). Unsurprisingly, this can cause difficulties if a crime is committed from within a country lacking appropriate legislation. For example, the alleged author of the Love Bug worm (which caused estimated worldwide damage of $7 billion in 2000) was traced to the Philippines. However, the authorities were forced to release him because the country had no relevant law in force at the time of the incident. This is not to say that things cannot be done to improve the situation. An example here is the European Convention on Cybercrime [11], which was devised by the 41 member countries within the Council of Europe (along with and representatives from the United States, Canada, South Africa, and Japan), with the specific intention of reducing inconsistencies in the handling of cybercrime.

Considering the perspective of those responsible for enforcing the law, the issue of investigating cybercrime has become much harder. Not only has the range of potential attacks increased, but the dramatic increase in desktop computing capabilities has also influenced the magnitude of the investigator's task. For example, whereas a typical computer in 1990 would hold an average of around 3,000 files, their modern equivalents hold around 25,000. So, whereas copying the contents for analysis would have taken one to two hours a decade ago, it is now more likely to take four to six [12]. Furthermore, the resulting volume of information is much more difficult to analyze.

Another historical difficulty has been a lack of police personnel with the necessarily skills to tackle cybercrime. An example of the limitations can be seen in the UK, where until 2001 there was no nationally recognised body to whom cybercrime could be reported (the nearest thing had been the Computer Crime Unit at New Scotland Yard). This situation finally changed with the establishment of a £25 million National Hi-Tech Crime Unit (NHTCU), which began operation in April 2001. At a national level, the role of the NHTCU is to investigate "attacks on the Critical National Infrastructure; major Internet based offences of paedophilia, fraud or extortion; information from seized electronic media; and gather intelligence on cybercrime and cybercriminals" [13]. Local police forces support this work by investigating crimes committed on computers and assist with requests for information from abroad.

Although policing and protection initiatives are moving in the right direction, there are still questions over whether appropriate levels of resources are being directed at the cybercrime problem. In the US, for instance, Gartner Group Inc. suggests that around 97% of all law enforcement funding for cybercrime is spent on about 300 federal agents (which represents less than 0.1% of the 600,000 agents that are funded in total). Furthermore, of the estimated $17 billion in federal discretionary spending that is directed towards law enforcement, only £10 million goes towards training, staffing, and support relating to cybercrime. This represents less than 0.1% of the total spending. As a result, Gartner concludes that the majority of Internet crime goes unpunished, and that cyber criminals know that they have little to fear from law enforcement [14].

Policing activities are also complicated by the fact that many incidents do not get reported (estimates have suggested that the level of reporting may be as low as 5% [15]). There are three general reasons why this may be the case. Firstly the organizations concerned may not consider the incidents to be significant enough to warrant concern or further action. A second potential reason is that the victim may lack confidence in the ability of the authorities to deal with the matter, and may feel that there is little to gain by getting them involved as few cases result in convictions (e.g. the chances of prosecution for hacking in the US are claimed to be one in 10,000 [16]). However, research suggests that the third explanation is the most likely -

namely, that organizations do not wish to report crimes as they are concerned about the adverse effects that widespread knowledge of such incidents could have upon their business [17]. Organizations are generally keen to avoid adverse publicity, as this may risk losing the confidence of the public or their shareholders. In addition, certain incidents could (if publicized) lead to a risk of legal liability. From a more personal perspective, those responsible for maintaining security may prefer to hush things up rather than report an incident in order to avoid potential ridicule by peers. The result of all this is that, in many cases, incidents are not willingly reported. It is, of course, easy to appreciate the company perspective in these situations – particularly in cases where the loss or disruption is ultimately perceived to be negligible or, at least, manageable. It may simply not be worth the effort, or indeed the risk, for them to report an incident. At the same time, those that keep quiet can be considered to be helping to hide the extent of the problem – which ultimately makes life more difficult for others. If the overall extent of the problem is underestimated, it will certainly receive less attention than it actually deserves. This may be manifested within individual organizations, as well as at higher levels, such as the level of funding allocated by governments to cybercrime prevention initiatives.

5 Conclusions

Widely reported incidents of computer abuse can do nothing but give the information society a bad reputation. It is often hard enough for new users to be faced with the task of becoming IT literate, without feeling that they are entering an unfriendly environment in which others may damage their systems or steal their data. Many organizations and individuals can see benefits that the Internet and the web will offer them. However, along with the good things, some of the most memorable net-related headlines have come from cybercrime incidents such as the Love Bug – which is somewhat off-putting.

It would be unrealistic to expect a complete removal of the criminal element from the information society – within any society there will always be elements that are unethical or disruptive. As such, we must change our attitudes and give the issue a similar level of consideration to that which we already afford to other types of crime, such as theft from our properties. In addition, an increase in the instances of computer crime must be seen as inevitable. As the technology itself becomes more pervasive, cyberspace will become a natural environment for criminal opportunities. The widespread acceptance of this fact will be the first step in ensuring that the information society is a safe place to be. Having said this, many of the common problems that enable cybercrime *can* already be solved with existing IT security measures. Security technologies, such as intrusion detection systems, are continually improving, with more advanced capabilities that will limit the future opportunities. So, with the technologies available or in place, the main ongoing problem is again linked to the attitudes and awareness of the people involved. Organisations must find a way to configure and maintain their systems securely. Everyone else must take their share of responsibility too, following good security practice where possible and ensuring that their own actions do not compromise protection.

Acknowledgement. The content of this paper is largely based upon material from the author's book, *Cybercrime: Vandalizing the Information Society*, published by Addison Wesley.

References

1. Rheingold, H. The Virtual Community – Finding Connection in a Computerized World. Secker & Warburg, London. (1994)
2. Audit Commission: yourbusiness@risk – An Update on IT Abuse 2001. Audit Commission Publications, UK. September (2001)
3. Furnell, S.M.: Categorising cybercrime and cybercriminals: The problem and potential approaches. Journal of Information Warfare, Vol. 1, No. 2. 35–44.
4. Power, R.: 2002 CSI/FBI Computer Crime and Security Survey. Computer Security Issues & Trends, vol. VIII, no. 1. Computer Security Institute. (2002)
5. Alayed, A., Furnell, S.M. and Barlow, I.M.: Addressing Internet security vulnerabilities: A benchmarking study. In Ghonaimy, M.A., El-Hadidi, M.T. and Aslan, H.K. (eds): Security in the Information Society: Visions and Perspectives. Kluwer Academic Publishers, Boston. (2002) 121–132
6. McCullagh, D. and Arent, L. 2000. "A Frenzy of Hacking Attacks", Wired News, 9 February 2000. http://www.wired.com/news/print/0,1294,34234,00.html
7. Akass, C.: On the straight and narrow – not. Personal Computer World, February (2000) 57
8. Sophos: Top ten viruses and hoaxes reported to Sophos in February 2003. Press Release, Sophos, UK, 3 March 2003
9. Greene, T.C.: Anna-bug author OnTheFly 'fesses up. The Register, 13 February 2001
10. HMSO: Computer Misuse Act 1990. Her Majesty's Stationary Office, UK (1990)
11. Council of Europe: Draft Convention on Cyber-Crime (Draft No 19), Council of Europe, PC-CY (2000) Draft No 19. Strasbourg 25 April (2000)
12. British Computer Society: Partner in crime, The Computer Bulletin, May (2000) 23–25
13. Home Office: New Hi-Tech Crime Investigators in £25Million Boost to Combat Cybercrime, News Release, 13 November 2000. http://wood.ccta.gov.uk/homeoffice
14. Garner Group Inc.: Gartner Says Most Internet Crime Goes Unpunished, Press Release, 7 December 2000
15. Blake, C.: Casting the Runes, Seminar presentation, British Computer Society Information Security Specialist Group seminar, London, UK, 7th February (2000)
16. Bequai, A.: Cyber-Crime the US Experience. Computers & Security, Vol. 18, No. 1 (1999) 16–18
17. Parker, D.B.: Consequential loss from computer crime. In Grissinnanche, A. (ed.): Security and Protection in Information Systems. Elsevier Science Publishers B.V., North-Holland (1989) 375–379