Australian Government
Australian Institute of Criminology

AUSTRALIAN HIGH TECH CRIME CENTRE

HIGH TECH CRIME BRIEF

2005

07

Hacking techniques

Criminal hacking

Hacking has a number of meanings and in common use refers to gaining access to another person's computer. Australia's cybercrime model legislation prohibits causing unauthorised access to data on a computer, where this is done with the intent to either commit a serious crime, or to cause harm or inconvenience. Special meaning is given to the word 'access' which is defined as 'execution of a function of a computer'. This captures direct or remote use without any physical contact with an individual computer or its components. It includes viewing files, as the computer is required to execute a function to make data viewable. Associated offences are: impairing electronic communications; possessing data with intent; impairing data; and accessing restricted data.

This paper examines the nature of hacking techniques, not to inform potential offenders, but to assist in law enforcement and preventive activities by alerting computer users to the security measures they need to employ to resist the intrusions of hackers. Not even a fraction of hacking incidents can be investigated, let alone prosecuted. Computer security therefore depends on all users being aware of the risks and taking responsible action to avoid these risks. Some of the distinct ways in which a computer may come to be under attack are:

- from within, by a person with physical access to a computer;
- from outside, by a person targeting a specific computer or any vulnerable computers on an intranet or across the internet; and
- from outside, in an automated process spread from computer to computer.

The hacker's target: networked or not

The level of connectivity of a computer determines the ways in which a hacker can gain access to that computer. A hacker may use an input device for a specific computer (such as a keyboard). If a computer is connected to other computers by a local area network (LAN) or to the internet, then the hacker may be able to gain access to that computer over the LAN or via the internet. New technology creates new opportunities for hacking and hackers can also gain access to wireless computers or networks by intercepting the signals used to communicate between one device and another. At present this involves interception of telecommunications, which may be illegal if carried out without authorisation.

The hacker's base

A hacker may operate from more than one computer, using a personal home computer, publicly accessible internet cafes, large computer networks accessed through work or study, or remotely infected computers. For the hacker, a degree of anonymity can be secured through the use of encryption, by the use of email accounts that do not require user identification, and by routeing messages through proxy servers.

In a recent US case an AOL employee was charged with using the identification codes of a colleague to steal the AOL subscriber list of 92 million screen names in 2003. The list is alleged to have initially been sold to a spammer who resold a version for US$52,000 (The smoking gun 2004)

In the 2004 AusCERT computer crime and security survey, 67 per cent of respondents said they had experienced at least one electronic attack that 'harmed the confidentiality, integrity or availability of network data or systems'. When asked about the source of attacks, 88 per cent of respondents identified at least one attack as coming from an external source and 36 per cent of respondents identified at least one attack as coming from an internal source.

Sometimes vital information about a system can be obtained from people with privileged access using 'social engineering'. For example, a hacker pretends to be another person with privileged access and rings up the IT help desk or another privileged user to obtain information in a 'crisis' or 'as a favour'. In some circumstances, a computer may not be physically secured from use by members of the public and portable items such as laptops are easily targeted. In some cases the privileged user becomes a hacker.

Vulnerabilities and exploits

Most computer programs balance functionality with security and contain vulnerable points. A vulnerability can be used by a hacker to enter, damage or control an affected computer. The software created to make use of a vulnerability is called an exploit.

When a vulnerability is discovered it may be reported publicly. A software developer or an anti-virus company may not report it until a patch has been prepared so that the fix is available at the same time the vulnerability is announced. There is an opportunity for the vulnerability to be exploited using malicious code between the announcement of a vulnerability and when individual computer users update their own computer operating system or anti-viral software. Hackers may also reverse engineer a patch to make new exploits that work around the patch (Ward 2004). The time in which malicious code can be written and distributed to exploit a vulnerability appears to be decreasing dramatically.

Schneier (2004) reports that the 'Witty worm' infected and destroyed the worldwide population of some 12,000 vulnerable machines within 45 minutes of its launch, which took place within about 36 hours of the announcement of the vulnerability. An attack of this nature leaves too little time for the development of a patch, let alone its installation on vulnerable machines. The situation is complicated further if the software developer restricts the availability of patches to those who can show that they are running authorised versions of the software product. In such instances a population of vulnerable machines will remain unprotected.

The hacker's toolkit

The hacker has available a range of digital tools, not all of which are illegal and many

of which are automated. These tools can be loosely categorised in terms of the degree to which they intrude into the operation of another computer. Put simply, software may be used by a hacker to enter, damage or control another computer. The range of tools, from the least intrusive to the most, are used to scan, spy, insert data, manipulate data and cause a computer to launch an attack on another computer. The following are examples of possible techniques:

- probing computers and systems by 'pinging' or sending out messages that identify computers that are online, and then scanning these computers for open portals;
- infringing security by using password sniffer programs, password cracking programs, or keyboard logging programs to reveal passwords and other information;
- creating backdoors once an open portal is found and then using software to keep it open and to make it accessible to other computers over a network or the internet;
- inserting code into computers such as spyware programs, which report activity on the target computer; malware is used to execute malicious code such as worms (self-replicating pieces of code that transmit themselves once released without requiring any further human intervention) or viruses (self-replicating pieces of code that are disguised as, or attached to, another application and that become activated when a person tries to open what typically appears to be an email attachment);
- remotely controlling other computers to affect internal data or operations: 'Trojan horses' are a form of code that once activated on a target computer, enable that computer to be commandeered to perform a pre-determined operation or to be actively controlled to perform operations in real time;
- remotely controlling a computer to affect other computers, such as in a distributed denial of service attack where literally thousands of remotely controlled computers (bot armies) are made to bombard another computer or service causing it to be overloaded and degrade or fail; and
- intercepting wireless data transmissions.

Establishing liability

Given the definition of hacking offences, a number of the activities of hackers will not be captured. A key question is whether or not the entry into another computer was authorised (Kerr 2003). In addition, the attack needs to be properly characterised as being on data rather than, say, a server, while the capacity of a computer to handle high volume traffic may be at issue. There may also be the problem of proving a successful exploit attack, which by its very definition causes failure (Barrett 2004). Accessing a computer remotely involves a gap in time from when the hacker launched an application to the point that it executes a function on the computer of another and in the virtual world of computing it is often difficult to pinpoint where and when a particular action occurs.

Despite these problems, evidence of intent may be shown by the hacker's actions overall. Snooping around inside someone's computer (either by directly accessing it, or remotely accessing it, or by using automated spyware) may or may not be accompanied by malicious intent. Such intent is more readily identified in cases involving vandalising or corrupting data, stealing data, remotely controlling a computer to effect commands on that computer, remotely controlling a computer to launch attacks on other computers, or launching malware such as viruses, worms or Trojan horses over a network.

The intent element may also prove difficult in relation to a virus or other code that is created by one person but launched by another, or in relation to unintended recipients of code that is self-replicating. Launching a so-called 'good' virus which patched a vulnerability could be classed as illegal in WA, Tasmania and Queensland. In the other Australian jurisdictions this would not be an offence unless it could be shown that there was, in fact, an intent to cause harm or inconvenience, or the hacker was reckless as to that occurring. Where a person is engaged in testing a system to discover any vulnerability, this would not be a defence unless the testing was specifically authorised by a person responsible for the computer network being tested. If the testing is unauthorised, then while the prosecution might not be able to prove the intent to commit a serious offence, or to cause harm or inconvenience, the hacker is likely to be liable on the basis of recklessness to the possibility of causing harm or inconvenience.

Many of the sophisticated tools used in hacking are now widely available as easy to use tools. In addition, the authors of worms and viruses may post their work on the internet without necessarily intending to release harmful code themselves. The code may, however, be taken up by others (sometimes referred to as 'script kiddies') who, although unable to write the worm or virus, are able to create a vehicle to launch it to attack other computers.

Target hardening

Hacking is an intractable problem of the internet. While governments need to address this problem through law enforcement agencies, perhaps the best form of protection is prevention. Computer users should be aware that they have a common responsibility to maintain the security of their own computer and make sure that it is not hacked or becomes a vehicle for hacking attacks on other computers. All legitimate users of the internet must share in the effort in target hardening. The security of all computers depends on a combination of measures: considering the physical security of a computer, isolating strategic components from internet connections, using internal firewalls, maintaining and updating anti-virus software, updating operating system components, treating all suspicious or unsolicited email with caution and remembering the human element in the overall maintenance of security.

Contact
Australian Institute of Criminology
GPO Box 2944 Canberra ACT 2601
Phone: 02 6260 9200 Fax: 02 6260 9201
Web: www.aic.gov.au

Project no. 0074 ISSN 1832-3413

The Australian High Tech Crime Centre funded this research.

Further reading

AusCERT 2004. *Computer crime & security survey.* Brisbane: AusCERT

Barrett N 2004. *Traces of guilt.* London: Bantam Press

Grabosky P & Smith R 1998. *Crime in the digital age.* Sydney: Federation Press

Kerr O 2003. Cybercrime's scope: interpreting 'access' and 'authorisation' in computer misuse statutes. *New York University law review* 78(5): 1596

Parliamentary Joint Committee on the Australian Crime Commission (PJC) 2004. *Cybercrime.* Canberra: Parliament of the Commonwealth of Australia

Schneier B 2004. The witty worm: a new chapter in malware. *Computerworld* 7 June

The smoking gun 2004. *Pair nailed in AOL spam scheme.* http://www.thesmokinggun.com/archive/0623042aol1.html 25 June 2004

Ward M 2004. Hackers exploit windows patches. *BBC News* 26 February