AUSTRALIAN HACKERS AND ETHICS

M.J.Warren[Φ] and W.Hutchinson[Ω]
[Φ]School of Information Technology, Deakin University,
Geelong, Victoria, Australia.
[Ω]School of Computing & Information Science, Edith Cowan University,
Mount Lawley, Western Australia, Australia.
E-mail Contact: mjwarren@deakin.edu.au

ABSTRACT

The aim of the paper is to look at the way hackers act and ways in which society can protect itself. The paper will show the current views and attitudes of hackers in an Australian context. The paper will also include a case study to show how a hacking incident can develop and how technology can be used to protect against hacking.

Keywords: Computers and Society, Australia and Hacking.

INTRODUCTION

We have seen a rise in computer misuse at a global level, it is generally thought that 'Hackers" are responsible for these attacks. Hackers are perceived as being adolescent males, in dark bedrooms being able to cause massive damage across the world just by the use of their computers. A more romantic perception portrays them as being determined: cyber knights with a code of conduct to live by just like the great Arthurian knights. This paper looks at hackers, their ethical viewpoint and the role and impact of hackers within Australia.

COMPUTER HACKER - THE DEFINITION OF HACKING

According to Bruce Sterling (1993) in his book titled 'The Hacker Crackdown', the term "hacking" is the act of intruding into computer systems by stealth and without permission (Lopez-Fernandez and Warren, 2002). However, this name is used routinely today by almost all enforcement officials with any professional interest in computer fraud and abuse to describe any crime committed with, by, through, or against a computer. Moreover, 'hacker' is what computer-intruders choose to call themselves, not as a criminal pejorative, but as a noble title given to those "soaked through with heroic anti-bureaucratic sentiment." (Sterling, 1993). Hacking then, can describe the determination to make access to computers and information as free as possible. Hacking can involve the heartfelt conviction that beauty can be found in computers, that the fine aesthetic in a perfect program can liberate the mind and the spirit (Levy, 1984).

STATE OF AUSTRALIAN IT SECURITY AND AUSTRALIAN HACKERS

A recent AusCERT Survey (Auscert, 2002) has focused upon the state of IT security within Australia, the following is a summary of the main results:

- 67% of all organizations surveyed have been attacked in 2002 - twice the 1999 level and 35 per cent of these organizations experienced six or more incidents;
- 98% of companies had experienced either computer Security incidents / crimes or other forms of computer abuse (such as network scanning, theft of laptops, employee abuse);
- Of Australian organisations who were victims of computer incidents, 65% of these attacks were from internally parties within the organisation and 89% came from external sources;
- 43% of Australian organizations were willing to hire ex-hackers to deal with security issues, three times more than in the US.

The survey showed that IT security and computer misuse are a major problem within Australia. The survey showed that external attacks were the source of the majority of attacks. Perhaps of interest is the willingness of Australian organization to use hackers to improve their security.

HACKER MOTIVATION

A recent hypotheses put forward has been regarding hacking motivation is that they are suffering from Asperger syndrome (Dreyfus, 2002).
Aspies typically have an almost obsessional approach to solving problems and are often oblivious to their peers' view that a given problem is 'unsolvable'. Both are often prerequisites to becoming an elite-end hacker. There does not appear to be any in-depth research linking illegal hacking and Asperger syndrome. However, one of the world's leading Asperger syndrome experts, Australian clinical psychologist Tony Attwood, believes some hackers may share characteristics with "Aspies", as they refer to themselves (Dreyfus, 2002).
"It's the sheer challenge rather than any (criminal intent). It's the pursuit of knowledge and truth - with different priorities and perceptions. They see it as an intellectual challenge and a prize, (and) they look at the success of what they have done rather than the consequences of the lives of people they have affected" (Dreyfus, 2002). Perhaps technology and deception combined into 'honeypots' and 'honeynets' can offer protection against such individuals.

HONEYPOTS & HONEYNETS

A Honeypot is a 'pretend' server with the aim of tracking *black-hats* (an unauthorized person trying to get access to a system) (Spitzner, 2000a) in the act of probing and compromising a system. The aim is to deceive the black-hat into thinking they are attacking an actual real life server (software examples include systems by Cohen 2000, and Network Associates, 2000).
The aim of the honeypot is to monitor the black hats by a number of means (Spitzner, 2000a), they are:

- Tracking the honeypot firewall logs
- Analysis of honeypot system logs to determine what the kernel and user processes are doing.
- Using a *sniffer* on the firewall that 'sniffs' any traffic going to or from the honeypot. The advantage of a sniffer is that it picks up all keystrokes and screen captures.
- Using a *tripwire* on the honeypot. A tripwire tells the system administrator what binaries have been altered on a compromised system (such as a new account added to: /etc/passwd, or a trojaned binary).

The aim of the honeypot is to attract the black-hats, monitor them, let them gain root access to the system, and then eventually log them off the system, all without any suspicion being aroused. Once black-hats gain root access, they are monitored for several days in order for the system administrator to learn what they were doing. The biggest problem is how to limit the black-hats offensive actions (Spitzner, 2000b). This is done by using the honeypot firewall, and implementing a rule base schema that allows access from the Internet to a honeypot's firewall, but limits outbound network traffic. It is important that the black-hat is allowed enough outbound traffic so as not to arouse suspicion.

The results of these honeypot assessments are made public (http://project.honeynet.org/) so that network administrators can access the information and ensure that they are protected against common hacker attacks and techniques.
The work by Spiztner developed into expanding the Honeypots into Honeynets. Spitzner (2000c) identified that the honeypots needed to be expanded for the following reasons:

- to be able to determine attacks upon switches, routers and different operating systems of a network
- generate information from several sources (for example, honeypots) in order to provide information in greater detail.
- detect new attack patterns such as vulnerability scanning and how black-hats progress from one system to another.

The result was grouping a number of honeypots together to form a honeynet, so a hacker would feel that they were gaining access to a much large networked system. An ideal solution to stop someone suffering from the Asperger syndrome to cause harm is by the use of honeypots and honeynets.
A major issue is whether the use of honeypots and honeynets are ethically acceptable. Is it ethically acceptable to deceive an attacker who is trying to hack into a computer systems?

AUSTRALIAN HACKERS

Research in the early 90's within Australia showed that computer crime and hacking was a problem. Victoria was the first Australian state to implement state law to outlaw hacking in 1988 and the Commonwealth

followed in 1989 (Hughes, 1990). An analysis of computer crime in 1991, showed that within Australia between 1990 and 1991 there had been 497 computer abuse incidents and 31 incidents related to hacking (around 6% of incidents) (Kamay & Adams, 1992). Research at this time also indicated Australian perception towards computer crime was influenced by cultural precedents (Coldwell, 1995). Other studies at this time also looked at the Australian perception of Computer Crime, a study was undertaken looking at teachers' perception of hacking and found from a sample group that 60.2% thought hacking was unacceptable and 39.8% thought hacking was acceptable (Coldwell, 1994). In 1997 "Underground" was written which described the history of Australian hackers during the early nineties, the development of the 'Wank virus' and 'plans' to destroy NASA computer systems (Dreyfus, 1997). Since that time, most of the Australian hacking community seem to have disappeared, no well known Australian hacking groups or even Australian hacking conventions are in existence. The only large Australian hacking group is "2600 Australia", (http://www.2600.org.au/) this group is based upon the famous US hacking group 2600. The philosophy of 2600 Australia is "2600 Australia is a loose-knit group of people interested in computer security, electronic gadgetry, communications and just technology exploration in general" and in terms of their activities can be best described as a computer club. No research has been undertaken to determine the numbers of hackers within Australia. Since the mid nineties there has been no major hacking incidents involving Australia or Australian hacking groups, the Millennium Bug period and Olympic Game passed without any publicized incident.

The most recent famous Australian hacking case was to do with sewage. In October 2001, Vitek Boden was convicted of 30 charges involving computer hacking of the Maroochy Shire Council sewerage system. The attacks, which commence in late 1999, involved using remote radio transmissions to alter the actions of the sewerage pumping stations and caused hundreds of thousands of litres of raw sewage to be pumped into public waterways (Kingsley, 2002). In the year 2002, does hacking by Australian hackers and hacking groups pose a real problem?

AN EXAMPLE OF AN AUSTRALIAN HACKING CASE

The following is example of a typical Australian hacking case in chronological order. The case study shows how a hacking incident can develop and how the press become focal point (Lopez-Fernandez and Warren, 2002):

> *Carr defends MP in hacking case* (Australian Financial Review 07 Aug 2001)
> The NSW Labor MP at the centre of a hacking scandal said yesterday he had once trained as a computer programmer, after initially saying he ``wouldn't know the first thing about hacking into a computer''. It also emerged yesterday that the computer of a senior Liberal MP, Mr Peter Debnam, had been unlawfully accessed at Parliament on a public holiday. A computer belonging to the Labor MP, Mr Tony Kelly, was seized by NSW Police yesterday after allegations that confidential files belonging to the Opposition were found on a computer in the parliamentary office of the State Government's leading Upper House strategist Mr Tony Kelly.
>
> *Office ban on computer MP's son* (Sydney Morning Herald 07 Aug 2001)
> The son of the Labor MP at the centre of computer hacking allegations at State Parliament was barred from his father's parliamentary office last month, the Herald has been told. The Upper House MP, Mr Tony Kelly, who admitted training as a computer programmer in the 1970s and 1980s, refused to comment on reports his son had extensive computer skills. It is understood Mr John Kelly has been a regular visitor to his father's office.
>
> *Hacking skills denied* (Illawarra Mercury 07 Aug 2001)
> The NSW Labor MP at the centre of a parliamentary computer hacking scandal has revealed he had been a computer teacher at a TAFE college.
>
> *Political espionage* (Sydney Morning Herald 08 Aug 2001)
> Sometimes security is only noticed when there is none. The discovery that a State Government MP's office computer may have been used to hack into Opposition computer files has shaken the customary quiet sense of security that pervades parliamentary life.
>
> *MP in hacking affair steps aside* (Sydney Morning Herald 08 Aug 2001)
> The controversy surrounding the alleged hacking of an Opposition MP's computer deepened yesterday as the Carr Government politician at the centre of the allegations was forced to stand aside from his parliamentary positions.

Hacking claims: MP steps aside (Illawarra Mercury 08 Aug 2001)
The NSW Labor MP at the centre of a parliamentary computer hacking scandal stood aside from his Upper House duties yesterday as the search for the hacker continued.

NSW Labor MP steps aside during inquiry into hacking (Australian Financial Review 08 Aug 2001)
The NSW Labor MP Mr Tony Kelly stood aside from parliamentary duties yesterday amid a police investigation into computer hacking at State Parliament.

Labor MP steps down from duties (Newcastle Herald 08 Aug 2001)
The NSW Labor MP whose office computer is at the centre of a parliamentary computer hacking scandal stood aside from his Upper House duties yesterday as the police investigation continued.

Hacking software found in Mp's computer (Sydney Morning Herald 09 Aug 2001)
A computer in the office of the Labor MLC Mr Tony Kelly was loaded with password 'sniffing' software that could have been used to break into the personal files of the Liberal MP Mr Charlie Lynn, a consultant hired to investigate hacking allegations inside the NSW Parliament has found. The Herald has confirmed that the 12-page preliminary report by a Melbourne firm, eSec, commissioned by parliamentary staff and handed to police on Tuesday, recommends a more detailed analysis of the computer files.

Staff kept suspicious software under wraps (Sydney Morning Herald 10 Aug 2001)
The NSW Parliament 'hackergate' controversy deepened last night when parliamentary staff revealed they had covered up for nine days the discovery of suspicious software on an MP's computer.

Carr denies Labor not cooperating (Illawarra Mercury 13 Aug 2001)
NSW Premier Bob Carr has denied Labor members were unwilling to cooperate with the police inquiry into State Parliament's computer hacking scandal.

MPs' House rules frustrate police hunt for hackers (Sydney Morning Herald 14 Aug 2001)
Police investigations into computer hacking allegations at the NSW Parliament are being frustrated by parliamentary privilege.

Hacker squad get the go-ahead on MPs' files (Sun Herald 19 Aug 2001) Detectives from the Commercial Crime Agency will return to Parliament House in Macquarie Street tomorrow following a major breakthrough in the computer hacking investigation.

MP clear in hack inquiry (Illawarra Mercury 31 Aug 2001)
NSW Labor MP Tony Kelly was cleared yesterday of any criminal activity by police investigating allegations of computer hacking at State Parliament.

Police clear MP of hacking allegations (Sydney Morning Herald 31 Aug 2001)
The mystery surrounding the NSW Parliament ``hackergate'' controversy remained yesterday when police cleared the Upper House Labor MP Mr Tony Kelly. They found that there were computer files belonging to Liberal Party MLC Mr Charlie Lynn on a computer from his office.

MP's son admits: `I loaded software' (Sun Herald 02 Sep 2001)
John Kelly, son of embattled Labor MP Tony Kelly, has told police investigators that he loaded hacker software on to his father's Parliament House computer.

Parliament insecurity (Sydney Morning Herald 03 Sep 2001)
The police inquiry into State Parliament's so-called ``hackergate'' controversy has done nothing to restore faith in a system that should guarantee MPs unconstrained freedom in representing the public effectively. After a month-long investigation police have confirmed that unauthorised copies of computer files belonging to the Liberal MP, Mr Charlie Lynn, were found on a computer in the parliamentary office of the State Government's leading Upper House strategist Mr Tony Kelly. This is a serious finding…

IT blamed for secret downloads (Sydney Morning Herald 04 Sep 2001)

> Questions continue to be raised in the mystery over the NSW Parliament hacker scandal after a report blamed parliamentary IT staff for accidentally loading confidential files belonging to the Opposition MLC, Mr Charlie Lynn, on to the computer of the NSW Labor MP, Mr Tony Kelly.
>
> *Kelly no computer hacker* (Illawarra Mercury 04 Sep 2001)
> NSW Labor MP Tony Kelly has demanded an apology from Opposition leader Kerry Chikarovski after being cleared yesterday of hacking into confidential Liberal Party computer files.
>
> *MP's son loaded `hacking software'* (Illawarra Mercury 05 Sep 2001)
> The NSW Labor MP embroiled in a computer hacking scandal has confirmed his son was responsible for loading suspect software on his PC.
>
> *Revealed: how MP's son used computer in hacking* scandal (Sydney Morning Herald 05 Sep 2001)
> The son of Mr Tony Kelly, the Labor MP at the centre of hacking allegations, was using a computer in his father's parliamentary office late one Friday night to run software that can scan computer networks for security weaknesses while his father was overseas on parliamentary business.
>
> *No evidence of hacking, says clerk of Parliament* (Sydney Morning Herald 07 Dec 2001)
> The clerk of the NSW Parliament did not contact police after security software was found on an MP's computer because he had no evidence that any offence had been committed, he revealed last night. In a final report on the hacker controversy sparked after suspicious software and files were found on the computer of Legislative Council member Tony Kelly in July the clerk of the NSW Parliament, John Evans, said it would have been inappropriate of him to assume an offence had occurred without independent evidence.

The mini case study shows the main aspects of a hacking crime:

- the actual attack and determination that an attack had taken place;
- the response to the attack by the organisation;
- involvement of legal authorities;
- outcome of investigation.

From an ethical viewpoint it is interesting how the press reported the incident and raised unconnected issues e.g. an MP had been a computer teacher at a TAFE college. The mini case study showed two main ethical issues:

- The MPs son has access to his father's Parliament House work computer and was able to install computer software. The aim of the software was to scan network for security vulnerabilities e.g. the network at parliament house. An ethical solution would be to ensure that users do no allow other people to use their computers;

- The accusation that IT staff had accidentally downloaded sensitive computer files upon another users computer. The ethical dilemma is if it happened, why? If the IT staff did download the material accidentally then it is an issue of professionalism, if they did with intention to cause harm it is an issue of unethical behaviour.

At the end of the day no criminal charges were placed and the matter was resolved. If some simple ethical guidelines had been applied the whole series of events would never have occurred in the first place.

CONCLUSIONS

As stated before in regards to the Auscert survey, computer crime is a problem within Australia and to resolve this some organisations are looking to hackers to solve their security problem. Is this Ethical?
Ethics is an extremely important component of Information Security, but the problem is that Information Security tends to just concentrate on internal processes of access and amendment rights. The introduction of deception techniques (Honeypots & Honeynets) to trap hackers can technically be effective and has been proven to work. However, from an ethical viewpoint should deception techniques be used to capture hackers?

REFERENCES

AusCert (2002) *2002* **Australian Computer Crime and Security Survey**, University of Queensland, Australia.

Coldwell R (1994) **Perceptions of Computer Crime, Conference Proceedings Crime against Business**, Australian Institute of Criminology, March, 1994.

Coldwell R (1995a) Australian Attitudes Toward Legal Intervention into Hacking. **Communications of the ACM,** 38, 11.

Cohen, F (2000). Deception Tool – kit, URL: http://all.net/dtk/dtk.html

Dreyfus S (1997***) Underground Hacking, madness and obsession on the electronic frontier,*** Random House, Australia.

Dreyfus S (2002) Cracking the Hackers code, **The Age**, Melbourne, 20th August.

Hughes, G (1990) Computer Crime: the liability of Hackers, **The Australian Computer Journal**, 22, 2, May.

Kamay V and Adams T (1992) **The 1992 Profile of Computer Abuse in Australia**, ACARB, Centre for Computer Abuse research at RMIT, Melbourne, Australia.

Kingsley P (2002) QUEEN v BODEN, **ACISP 2002 Forensic Computer Workshop,** Melbourne.

Levy, S (1994). **Hackers:Heroes of the Computer Revolution**. Unknown.

Lopez-Fernandez M. and Warren M.J (2002) An Overview of Australian Hacking (2001), School of IT Technical Report – TRC 12.08, Geelong, Australia.

Network Associates (2000) **Cybercop Sting** . URL: http://www.nai.com/asp_set/products/tns/ccsting_intro

Sterling B (1993) **The Hacker Crackdown: Law and Disorder on the Electronic Frontier**, Mass Market Paperback, USA.

Spitzner, L. (2000a) **To Build a Honeypot**.
URL: http://project.honeynet.org/papers/honeypot/

Spitzner, L. (2000b). **Know Your Enemy: A Forensic Analysis**, URL: http://www.securityfocus.com/focus/ih/articles/foranalysis.html

Spitzner, L (2000c) To Build a Honeynet, **FIRST (Forum of Incident Response & Security Teams) Conference** *2000*, Chicago, USA.