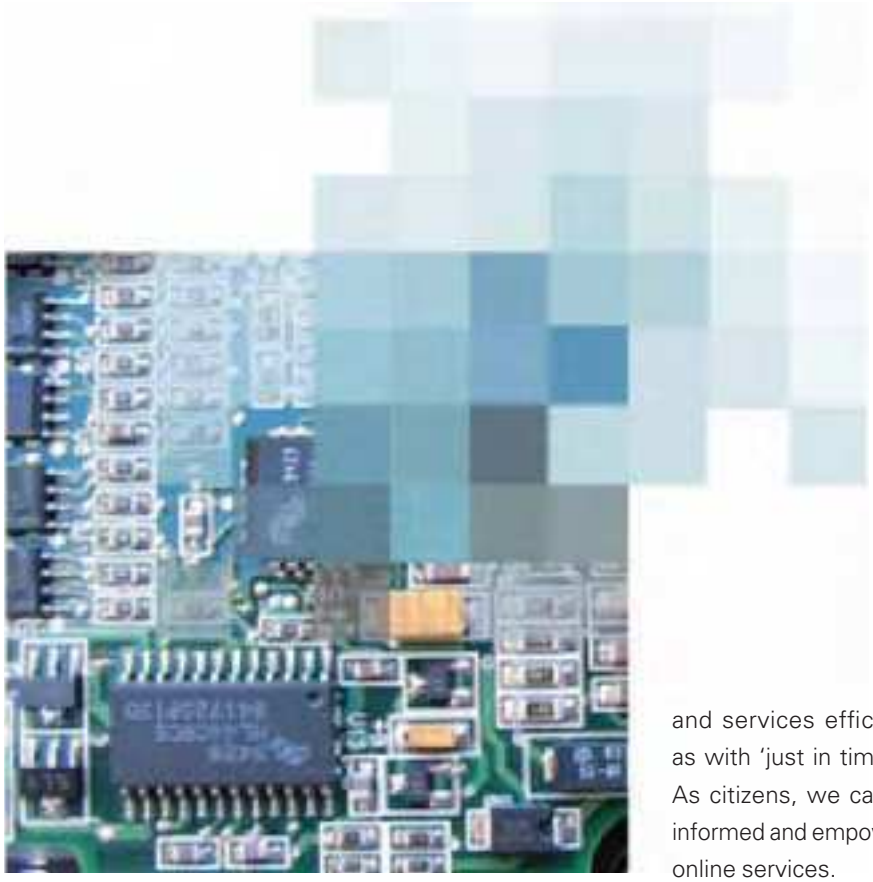
Gaps in cyberspace can leave us vulnerable

By Tony Krone , Australian Institute of Criminology



The word 'cyberspace' was coined in 1984 by novelist William Gibson to describe the world that exists within computers.

It was a radical and puzzling idea at the time. Now, 22 years later, we are all familiar with communicating in real time across the globe – we access government services online and we shop, view, read, search, explore and even simulate physical activities instantaneously.

In short, we are used to the idea of living in a world which includes cyberspace and for a significant majority of us the internet has replaced bricks and mortar institutions.

Physical and virtual security

Any online activity has a physical and a virtual aspect. In the context of crime in cyberspace it is important to consider physical and information technology security together, as it is now impossible to consider one without the other.

When used properly, information and communications technologies make it possible to be better informed, to participate in society more effectively, and even to trade in physical goods and services efficiently such as with 'just in time' ordering. As citizens, we can be better informed and empowered using online services.

This remarkable progress has been made by simplifying the user interface, speeding up data transmission and providing greater storage capacity at lower cost. The 'plug and play' cost is low allowing more people to jump onto the information superhighway. However, some users do not fully evaluate the risks of committing to new technologies.

There is a significant gap between the assessment of the value of adopting new technology and the risk involved. The problem is inescapable partly because

the criminal uses of new technology are difficult to anticipate and the risks difficult to quantify. Without an appreciation of the likely costs of using new technology or of making technological applications more secure, it is difficult to persuade those who invest in it that there is a downside.

High tech crime

Just as information and communications technologies have provided a platform for social, business and political activity, they also have been readily adopted as a platform for other less pro-social activity. Such technology is a powerful tool for those committing crimes, either by attacking computers or using them to further other criminal activity.

network digitally; many offenders have access to advanced computer skills; some offenders minimise their criminal activity as fantasy; computer crime is a low cost/high volume business which can lead to high levels of damage or profit; criminal activity can be divided into smaller and smaller functional segments that can be grouped and re-grouped at will; online criminal networks are flatter and less hierarchical than traditional crime groups; the behaviour and tools used by offenders online often have a legitimate use; ordinary users are often unaware of illegal activity affecting them; ordinary users may not know that their identity or computer has been hijacked by an offender; businesses and householders may be both victims and vectors of high tech crime.

It is often said that there are no new crimes involving computers, rather, new ways of committing old crimes.

It is often said that there are no new crimes involving computers, rather, new ways of committing old crimes. To some extent that is true, but the digital age creates a whole new environment for criminal activity.

Some of the features of high tech crime include: no standard definition of online crimes either nationally or internationally; differences in laws and policing which are exploited to commit crimes; offenders

The move by criminals to specialise in various aspects of high tech crime is illustrated by the proliferation of malicious software, often developed by sophisticated hackers only to be taken up by less experienced users and launched onto the net infecting vulnerable machines.

Trojan Horse software is one such example as it can be used to compromise machines by taking control of them over the internet creating a 'bot army' which then can be hired out to spread spam, or commit a denial of service attack on another user.

Hackers can steal credit card records or other identifying data, using them directly or selling them to commit identity fraud. Spam or directed attacks can also be used in phishing attacks to obtain access to finances online.

The 'mules' or people needed to transfer the money back to the organisers of this sort of criminal activity can also be recruited online and then make their transactions online. All these products and services are now routinely networked among offenders enabling them to commit crimes.

Wireless revolution

We are in the midst of another ICT revolution as more users take up wireless technology. As with previous advances, there are many advantages to this new technology.

Without wires, systems can be installed and reconfigured at minimal cost and with a minimum of disruption. This is particularly important in heritage buildings, or where a business needs to be flexibly configured.

People can also connect to the internet from many more places and workers can be mobile without losing access to their office.

Just as with cyberspace, wireless technology blurs the distinction between

The use of wireless technology can compromise network security.

the real and virtual, between physical and IT security. It does away with the boundaries of a hard-wired network.

In a wireless network you can simultaneously expose your network to intrusion and intrude into the networks of others, without necessarily being aware that it is happening.

The use of wireless technology can compromise network security. According to the Advanced Computing Research Centre, "the addition of wireless extensions negates a lot of the security measures associated with the physical side of a LAN". Further to this, Mobile Ad Hoc Networks which involve connections between multiple mobile devices, are currently very insecure from attack.

Security threats

A lack of security can lead to criminal attacks on a network including: theft of data; corruption of system integrity; hacking; sabotage; espionage; theft of capacity; and loss or theft of mobile and portable devices.

The security threats that affect wireless LANs can be divided into active and passive attacks.

Active attacks

These include: spoofing the authorised access point; denial of service attacks; 'replay attacks' to cause a denial of service, or accelerate data flow to aid in the cracking of WEP encryption; and dictionary attacks to guess the base station SSID (Service Set Identifiers).

Passive attacks

Passive attacks rely on the collection of data in transit without interrupting the communication between authorised devices. A person can launch a man-in-the-middle attack using software that can cause significant disruption and loss.

Another example of a passive attack in the wireless environment is the phenomenon of 'war driving'. This is a variation on the older activity of 'war dialing' used to breach telephone systems. A war driver travels around using a laptop or PDA to locate and possibly exploit connections to wireless networks. While we know that war driving occurs in Australia we don't know much about the extent of the problem.

Network intrusion can also happen by chance. In a recent study researchers from the University of South Australia set up three 'honeypot' sites in Adelaide.

They found that each 'honeypot' experienced unauthorised connections and these were more likely when the 'honeypot' was surrounded by other wireless networks. Up to 18 per cent of connections to the access point were without authorisation. Of these, most were seeking access to the internet submitting DNS queries for popular web sites or instant messaging. Two of the 'honeypots' experienced malicious connections involving port scans or attempts to penetrate the 'honeypot's' virtual host.

War driving from public places is unlikely to constitute a criminal offence. However, where a person accesses a network, impedes network capacity, or interferes with or damages data, that may be a criminal act. A big issue will be the problem of innocent or unwitting connections made through the wrong access point even though such connections can cause bandwidth to leak to other users.

Some users simply set their machine to connect automatically to any available wireless network. If a host-based firewall is not used because the network is treated as trusted, a user can connect to another network and be hacked into or infected by a worm or other malware, and then spread the problem back into their own network.

Infrastructure exposed

Another way in which the distinction between physical security and IT security has dissolved is the increasing reliance in many sectors on wireless enabled computer control devices. In the essential services of electricity, sewerage and water, wireless devices are being used to control events and processes. These wireless devices can then be attacked. The case of Vitek Boden in Queensland illustrates how this can affect critical national infrastructure. During March and April 2000, Vitek Boden made 46 attempts using wireless connections to hack into Maroochy Shire Council's computerised waste management system. He had lost his job in developing the wireless network that controlled the sewage and drinking water system.

During the attack his laptop identified itself as 'Pumping Station 4' and sent commands leading to the release of millions of litres of raw sewage into rivers and parks, with considerable environmental costs.

Police caught him in his car using his laptop to obtain wireless access to the sewerage control system. In October 2001 he was found guilty on various charges involving computer hacking, theft and causing environmental damage in what was described as the world's first environmental vandalism case. He was sentenced to two years jail.

Law enforcement challenges

Not all of the costs of high-tech crime control can be met by users, nor can they all be left for law enforcement. From a law enforcement perspective, industry and citizens must work with authorities to keep cyberspace as safe as possible.

> Someone else's wireless connection can provide an attractive base for a criminal seeking to hide their identity.

While methods of policing and immediate priorities have changed over time, the basic ideal of policing is to enforce the rule of law by working cooperatively within, and for, the community. The job of policing can be divided into three areas of prevention detection and investigation, and prosecution.

Each of these can be considered in relation to physical and IT security.

Prevention

ICT has been developed without building in from the beginning security mechanisms to protect it from misuse. Consequently, ICT platforms are readily misused and once a criminal application has been developed it can persist in ways that cannot easily be stopped. As a result, we are in a cycle of vulnerability, exploit and patch for each new vulnerability.

In the real world, crime-reduction strategies can target the architecture of public places and the ways in which their spaces are patrolled and monitored. In the physical world we accept that police cannot be posted on every street corner.

Police have limited influence over the architecture of the wireless environment. Prevention is therefore in the hands of users and the police interest is to ensure that users take into consideration the full impact of their decisions when committing to wireless technology. Most commercial enterprises and government agencies are aware of the need for IT security – the problem for them is deciding what is best.

The recommendations made here come from reports by the Advanced Computing Research Centre (2005a) (2005c) and are based on a survey of industry experts.

Overall, the most important message is that criminals can target physical security as well as hardware and software, and the people behind the machines, so our responses should cover all of these.

They are:

Physically based

- Match signal strength to site requirements so the signal is not spread further than necessary.
- Impose physical barriers to protect access points.
- Situate access points centrally in a building, rather than on the perimeter where they may radiate a signal out of the building further than required.
- Maintain site security.
- Require physical authentication of users.
- If connections are point to point, use directional antennae rather than omni-directional.

Hardware based

- Limit access to the wired network for wireless users.
- Block direct connections from the wireless network to the wired network.
- Put wireless connections on a timer for when the network should be available.
- Unplug or switch off the modem when the internet is not required.
- Use a firewall.

Software based

- Use encryption being mindful that Wired Equivalent Privacy can be readily broken and that WI FI Protected Access is the preferred standard. The ACRC (2005b) recommend 802.11i with Advanced Encryption Standard cryptography and Protected Extensible Authentication Protocol authentication protocol at layer-2 as the best solution currently for wireless LANs. It is noted that the 802.11i protocol may require wireless hardware to be upgraded.
- Layer security so that packets and networks are distanced from sniffing attempts.
- Encrypt all information transmitted through the access point.
- If using WEP use non-obvious keys and periodically change them.
- Only share what you need to and password protect items that are shared with a strong password.
- Disable SSID (network name) broadcast.
- Limit the MAC addresses that can access the network.
- Don't use unprotected file and printer sharing.
- Require a password to access the admin features of the router or access point.
- Disallow access point administration via wireless.
- Use VPN and keep access points apart from valuable resources.
- Conduct periodical site surveys.
- Disable or change Simple Network Management Protocol settings to prevent outsiders from obtaining personal information.

User based

- Educate employees to take care of data security.
- Minimise the opportunities for theft, use clear identification marks, maintain asset control and auditing.
- Provide education to counter social engineering.
- Don't use descriptive network names that would indicate location or use.
- Don't do sensitive things over unsecured wireless connections.

Detection and investigation

The three activities of sniffing, attacking and freeloading on another's wireless connection present different challenges for law enforcement. This is not an area where police could possibly monitor traffic nor would that be legal or desirable in terms of privacy.

There is therefore a limited role for police in the detection of illegal wireless activity. While law enforcement depends on complaints from users, many people may be simply unaware of intrusions on their wireless network.

Passive attacks and sniffing might be difficult to detect or might not be thought of as much consequence. Administrators

need to be mindful that their wireless network can be used illegally by others in ways that make them victims through an attack on their own system or in ways that make them vectors or the base for launching attacks on others.

Criminals use wireless to hide

Someone else's wireless connection can provide an attractive base for a criminal seeking to hide their identity.

Examples of successful investigation include a man in Tallahassee, Florida, who used his neighbour's internet connection to access a college bank account to buy pornography and sex-related products. He was caught when police tracked down the delivery address.

A 21 year old Michigan man was sentenced to nine years in prison for taking part in a scheme to steal credit card records by hacking into a wireless connection for a home improvement chain store.

Reporting crime

The annual AusCERT Computer Crime and Security Survey indicates that there is a low rate of reporting attacks on computers to police.

In the 2005 report, 69 per cent of those who experienced an "electronic attack harming the confidentiality, integrity or availability of computer network data or systems", chose not to report the attack to law enforcement.

A study by the Advanced Computing Research Centre (2005a) indicates that 'leaching' or the misappropriation of bandwidth is generally not reported to police. Sometimes people do not mind if others use their wireless connection, or those who do mind can counter the threat by a minor upgrade to their network security, because people seeking free access will move to easier targets.

Prosecution

The law enforcement priority regarding wireless networks is to encourage government, industry and householders to put security first and to limit the opportunities for the misuse of wireless capacity.

Achieving higher levels of security may in the short term mean that previously unrecognised intrusions and attacks become known to users.

In the longer term, the measure of success for law enforcement will be reduced opportunities to commit offences rather than more charges being laid.

A unique approach to law enforcement has been adopted at the Australian High Tech Crime Centre where the major banks in Australia have all contributed staff to work side by side with police from across Australia to combat electronic threats to the Australian banking system.

The Joint Banking and Finance Sector Investigation Team at the AHTCC is a good model of what can be achieved through close police and business cooperation. Banks can coordinate their responses to online threats and work with police to solve crimes as they happen.

It is important to review and evaluate this approach but early indications are that it is a positive way forward. Hopefully, Australian law enforcement agencies will continue to develop their electronic crime response capacity through such strategic partnerships.

Partnering with society

High tech crime is a volume business where any weak link in network security will be exploited with large flow-on effects. With wireless networks, security is only as strong as the weakest point. Overall it is imperative that we combat networked criminal behaviour with networks dedicated to crime control. More than ever, the job of policing is one of partnering with the rest of society.

Glossary of mobile and wireless acronyms

ICT	Information and Communications Technology
LAN	Local Area Network
MANET	Mobile ad hoc networks
ACRC	Advanced Computing Research Centre, Adelaide
PDA	Personal Digital Assistant
DNS	Domain Name System
WEP	Wired Equivalent Privacy 802.11b standard with 64 & 128 bit encryption
WPA	WI FI Protected Access
AES	Improved Encryption Standard. Wi-Fi Security enhancement using 802.11i, 802.1x and EAP standards, to enhance WEP - dynamic key assignment, strengthening encryption, ensuring keys are not repeated and adding the equivalent of a message hash to assure data integrity. WLAN security necessarily operates at physical or link layers (for example, at the MAC sublayer as in 802.11i) but if only IP service is provided then security at network or transport layer (for example TLS, SSL, IPsec) may be an alternative or a sensible addition, especially when using a public, Wi-Fi LAN. With128,192 & 256 bit key sizes.
PEAP	Protected Extensive Authentication Protocol – a method to securely transmit authentication information.
Layer 2	Within a hierarchy of access of computer administrator controls more restricted level.
SSID	Service Set Identifier. The SSID is a sequence of up to 32 letters or numbers that is the ID, or name, of a wireless local area network. The SSID is set by a network administrator and for open wireless networks, the SSID is broadcast to all wireless devices within range of the network access point. A closed wireless network does not broadcast the SSID, requiring users to know the SSID to access the network. Most wireless base stations come with a default SSID that is easily found on the Internet and security experts recommend changing the default SSID to protect your network.
MAC	Media Access Control Address. A unique code assigned to most forms of networking hardware. The address is permanently assigned to the hardware, so limiting a wireless network's access to hardware – such as wireless cards – is a security feature employed by closed wireless networks. But an experienced hacker, armed with the proper tools, can still figure out an authorised MAC address, masquerade as a legitimate address and access a closed network.
VPN	Virtual Private Network. A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorised users can access the network and that the data cannot be intercepted.
SNMP	Simple Network Management Protocol. A set of standards for communication with devices connected to a TCP/IP network. Examples of these devices include routers, hubs, and switches. A device is said to be 'SNMP compatible' if it can be monitored and/or controlled using SNMP messages. SNMP messages are known as 'PDU's' – Protocol Data Units. Devices that are SNMP compatible contain SNMP 'agent' software to receive, send, and act upon SNMP messages. Software for managing devices via SNMP are available for every kind of commonly used computer and are often bundled along with the device they are designed to manage.

www.afp.gov.au