# Promoting Australia's Response to Internet-Based Attacks

## *A Discussion Paper for the NIICF*

CONFIDETIAL

Rob McMillan
Australian Computer Emergency Response Team
23 September 1998

## Contents

*Executive Summary* ..... 2
*1. Introduction* ..... 4
*2. National Assets* ..... 6
*3. Vulnerabilities* ..... 7
*4. Threats* ..... 8
*5. Summary of Issues* ..... 11
*6. Solutions and Recommendations* ..... 12
6.1 A National Infrastructure Protection Agency (NIPA) ..... 14
6.2 An Australian Internet Communication Network ..... 17
6.3 Improved Operational Awareness and Expertise ..... 20
6.4 An Improved National Program of Research and Development ..... 21
6.5 An Emerging Technology Oversight Group (ETOG) ..... 22
*7. Conclusion* ..... 23
*Notes* ..... 24
*Acronyms* ..... 28
*References* ..... 30
*Appendix A - Attacks Against Current Technology* ..... 34
A1. Background ..... 34
A2. Buffer Overflows ..... 35
A3. Domain Name Service (DNS) ..... 35
A4. World Wide Web Browsers ..... 35
A5. Closing Thoughts ..... 36
*Appendix B - Statistics Describing the Potential Threat* ..... 37

# Executive Summary

During 1996 and 1997 the United States underwent an exercise of evaluating its reliance on the Internet for its National Information Infrastructure (NII), and the ability of the NII to withstand attack. The closing words to that report ([PCCIP97]) are:

> *This is not an exercise in problem solving. It is an attempt to deal with a rapidly changing, technology driven environment in which information and communications technologies add a new dimension of concern...Our nation is in the midst of a tremendous cultural change, which will have a profound effect on our institutions...While we do not believe a debilitating attack is imminent, the threats to our nation and the vulnerabilities in our infrastructures are real. And the time to act is now...*

Conventional wisdom would have it that in terms of technology adoption Australia is anywhere from six months to two years behind the United States. The threat that faces Australia is always state of the art.

The threat may be manifested against such emerging services as the Public Key Infrastructure (PKI), Electronic Commerce, and industries like health care and online taxation (for example). There are several problems we face in combating the threat.

First, these assets and services are in the main supported by low level technologies (such as operating systems, routers and firewalls) that are developed by organisations with a primary loyalty to a foreign government.

Second, although we can draw on computer and network intrusion data generated in the United States, there is a dearth of locally generated data. At this time, Australia is faced with a situation in which we must defend our emerging technology-driven infrastructure by making decisions without sufficient locally generated supporting information.

Finally, in the event of an intensive, coordinated attack against Australia, it is unclear that we have done the necessary homework to make a coordinated response with the required speed, although Australia has started work in this area ([DSD97], [Cobb98]).

Cobb's paper ([Cobb98]) makes some specific recommendations regarding the NII specifically. The purpose of this paper is to expand and complement both this work and the work of the President's Commission for Infrastructure Protection (PCCIP) in the United States ([PCCIP97]) to provide a coherent and proactive proposal to further the defence of our NII.

There is no magic bullet. We believe that the solution requires a response across a number of sectors. Our specific recommendations are:

1. *Establish an National Infrastructure Protection Agency (NIPA), driven by a Council, with operation work carried out by a Warning Centre.* In addition to producing proactive and reactive notification, this centre will act as a central data collection agency.

2. *Establish an Australian Internet Communication Network.* If the Australian Internet community is under attack, other forms of communication must be used. Depending on the size and type of attack, different methods of communication may be required.

3. *Ensure that the system administration community is given the knowledge and tools needed to make sure the systems they administrate are secure.* In times of attack, they need to know how to respond without having to make decisions in the heat of the moment. Prevention is better than cure.

4. *Improve the national program of research and development.* While Australia's reliance on imported hardware and software for our networking and IT infrastructure is unlikely to change significantly in short to medium term, it is recommended that mechanisms be explored to encourage development of our capability to ensure self reliance on critical infrastructure.

5. *Create an Emerging Technology Oversight Group (ETOG).* Australia's position as a technically savvy "can-do" nation depends on our ability to understand and apply leading-edge technology. In understanding this technology, we are also better placed to defend against attacks on infrastructure based on it.

These solutions are aimed at the civil community, and are intended to support and complement initiatives that may already be underway in the intelligence and defence communities.

We do not have the benefit of the large reserves of wealth and manpower that countries as the United States can boast. The proposal seeks to offer a government-led community response that is cost effective for all parties. Some of the components are already in place. In other cases, some investment is required, but there also exists the potential for payoff in future years.

# 1. Introduction

1.1 Australia is currently in the throes of grappling with an emerging economy - the information economy. This is a new and potentially lucrative opportunity that has been brought about by the popularisation of the Internet. As we move towards the adoption of the information economy, we anticipate a number of events. Consumers will be able to shop anywhere. Vendors will consider their target market to be global. Services, both commercial and government, will become available on line.

1.2 As a nation, we are taking a measured approach to transforming the national psyche from considering this technology as something new and exciting, to an everyday tool that we use without thinking. The legal world is thrashing out how our laws and precedents must adapt ([ECEG98]). Commercial agencies are developing services. The Federal Government through agencies such as the National Office of the Information Economy (NOIE) and the Attorney-General are trying to determine how to provide a workable infrastructure, hopefully without introducing Big Brother[1.1] ([ECEG98], [NPKIWP98]).

1.3 And all this time our adversaries are taking notice. The Internet may be new in mainstream society where information technology is not the topic of daily discussion, but it's a different story to information technology professionals and the "hacker underground". We will soon reach a point, if we haven't already, where the Internet and other computer networks are an indispensable part of our National Infrastructure.

1.4 As we, the citizens of Australia, come to rely on the Internet for carrying out our profession to earn our pay, bank that pay, pay our bills, purchase our groceries, transport our goods, submit our tax returns, buy our car or our clothes, and use our medical records when in hospital, we place ourselves in a position where the Internet is *critical.* All of these services are either available now or in progress, either in Australia or overseas.

1.5 All of these services are also a potential point of attack for an adversary. You can estimate a person's physical whereabouts using the Internet[1.2]. You can find out where they receive their email and use this information to find points on the Internet where they are likely to carry out their business. You can then attack those sites, and if successful, use a variety of social engineering and technical methods to disrupt their lives.

1.6 Attacks are clearly possible at the national level too. For instance, it is trivial to launch a denial of service attacks against name servers[1.3]. More serious attacks are possible against these machines which could compromise the entire Internet. Some expert groups have in the past boasted that given motivation, they could bring down the entire Internet within minutes. ([Wallack98]).

1.7 As adoption of the National Information Infrastructure (NII) becomes of increasing importance, so does its protection. The United States is moving rapidly towards a coordinated defence network for all components of what's considered to be critical infrastructure ([CERT97-1], [PCCIP97]):

- information and communication
- physical distribution
- energy
- banking and finance
- vital human services

1.8 Australia has also started work in this area ([DSD97], [Cobb98]). Cobb's paper ([Cobb98]) makes some specific recommendations regarding the NII specifically. The purpose of this paper is to expand and complement both this work and the work of the President's Commission for Infrastructure Protection (PCCIP) in the United States ([PCCIP97]).

1.9 Our recommendations are aimed at the civil community, and are intended to support and complement initiatives that may already be underway in the intelligence and defence communities.

# 2. National Assets

2.1 The introduction pointed out some of the everyday services that exist now, or will soon come to exist. What we really want to consider in this paper is the type of Internet-based service that can be regarded as a national asset - that is, services which support or enhance the Australian way of life. Examples of services at this level include:

- The Federal Government has embarked on *Project Gatekeeper* ([NPKIWP98]) to established a national authentication structure ([NOIE98]):

  > "These frameworks include ... a public key authentication framework to provide security, privacy and trust in transaction and messaging systems the Commonwealth is implementing the Project Gatekeeper strategy for the introduction of public key technology for government use a government online services charter to provide service guarantees to citizens and to ensure consistency across the whole of government." *[sic]*

- While Electronic Commerce in Australia is still in its infancy ([ABS98])[2.1], it is set to boom within 5 years, according to IDC Australia Pty Ltd ([IDC98]): "*Total Internet commerce revenues in Australia will grow from $127.3 million in 1997 to over $16 billion in 2002 according to a new research study published IDC Australia*"*[sic]*. The

- The Australian Taxation Office is trialling the *ATOassist* and *e-tax* schemes to allow submission of taxation forms using the Internet[2.2].

- There is a trend towards improving service and cutting costs in the health industry by making more information available electronically. The type of service envisaged would include remote access of electronic patient records, and perhaps online diagnosis systems[2.3].

- The Victorian Government has had a policy for several years of making public services available via on-line means[2.4]. Other states and some local governments have made similar commitments.

- Transport companies in Australia are using Internet technology to allow tracking of packages and coordinate delivery[2.5]. Its not a stretch to envisage that these service will be expanded. Disruption to such a service has the potential to cause serious problems, as demonstrated in the *Eligible Receiver* exercise in the United States earlier this year[2.6].

2.2 This is of course not meant to be an exhaustive list of what exists now or of future possibilities. What this list illustrates is some examples that may be a point of attack for a person wishing to interrupt the daily business of the nation.

# 3. Vulnerabilities

3.1 An adversary can attack an infrastructure at several levels. Details about physical attacks are beyond the scope of this paper and are covered in the references ([DSD97], [Cobb98]). This paper augments the references with some pragmatic suggestions from an Australian perspective. A brief, high-level discussion which highlights *some* examples of attacks that could be mounted against Australian Internet-based infrastructure at the present time is presented in Appendix A.

3.2 In summary, the old adage holds that those who ignore history are doomed to repeat it. In AusCERT's experience, this holds true just as much with software vulnerabilities as with any other facet of life. Many of the attacks described in the appendix have been seen in one form or another on multiple occasions. Literature shows that such problems have existed in various forms since the dawn of the software age.

3.3 The problems repeat for several reasons:

1. Some of the fundamental building blocks are just not designed with security in mind. Problems of this genre are difficult or impossible to solve.

2. Secure design techniques and programming are not ingrained in computer science students as a core element of software design and implementation.

3. Time to market is such an important element to competitive advantage that it precludes comprehensive security testing.

4. Security is not a bottom line issue for many vendors. Features and convenience are the crucial sales criteria.

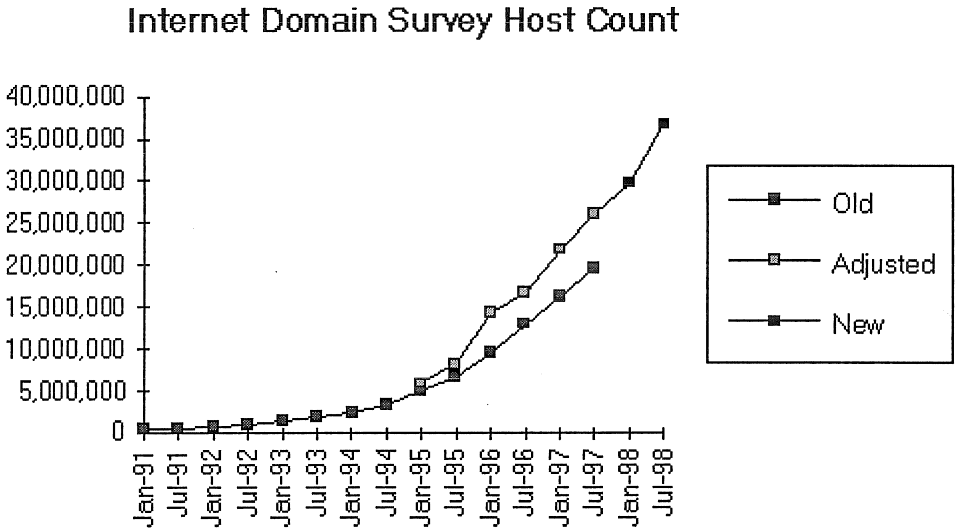
5. Software tools and applications are invariably used for purposes for which they were not originally intended, and therefore with unpredictable results.

# 4. Threats

4.1 Its very difficult to quantify the size of the threat. Because the Internet is so open, an attack may be source from anywhere within Australia or the world, via a number of different techniques. Complicating this is that the indicated source (if there *is* a source indicated) may be a forgery. Furthermore, a successful attack may take place over a number of milliseconds. Determining an attack in real time would be impossible. Without high quality logging, finding the source after the fact would be just as difficult.

4.2 However, it is possible to obtain some idea of the size of the threat. Network Wizards[4.1], a respected Internet consulting organisation carries out a semi-annual survey of the Internet[4.2]. In the July 1998 survey, the Internet was comprised of approximately 37,000,000 hosts, of which approximately 750,000 were registered as Australian hosts[4.3]. This means that the Australian network population comprises around 2% of the entire Internet population.

4.3 The Internet has grown phenomenally ([RFC1296]), and shows no sign of slowing:

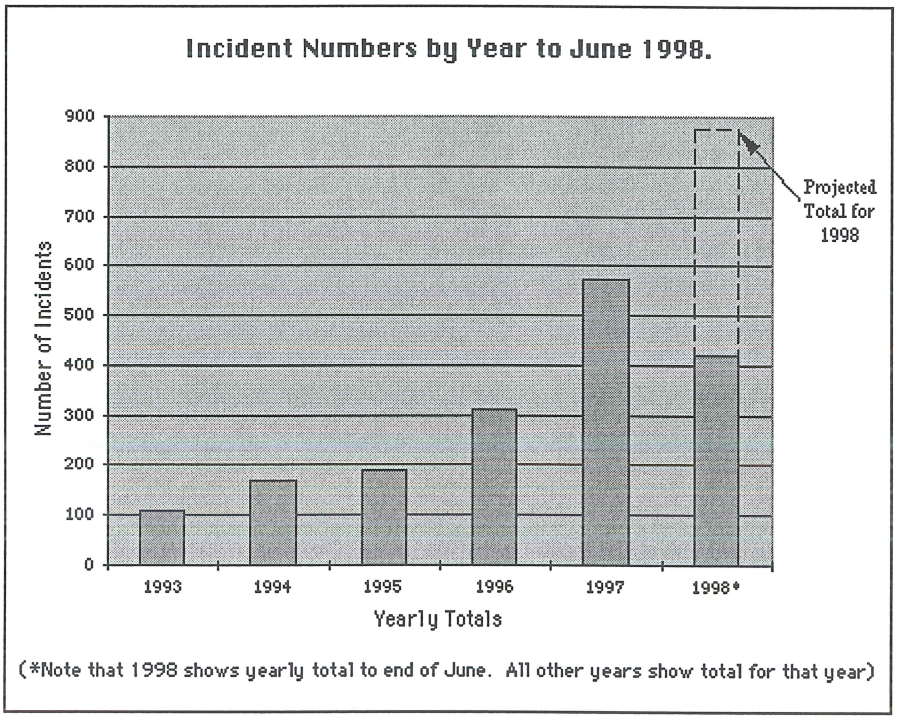


*Graph supplied courtesy of Network Wizards*[4.4].

*Prior to 1998 Network Wizards estimated the size of the Internet using a technique that has since been improved. The reader should rely on the upper line of the two shown on the graph.*

4.4 Generally speaking, incident trends have followed this growth.

4.5 The CERT Coordination Center (CERT/CC) in the United States recorded steady growth in incidents each year until about 1994/1995 at which point it leveled off at about 2,500 per year[4.5]. It was at this point that more response teams within the United States and externally (including AusCERT) began to relieve some of this workload. As response teams other than CERT/CC began to coordinate incidents within their constituency, the load of CERT/CC leveled off. In the Australian arena, the steady growth recorded by AusCERT supports this ([AusCERT98]):


Incident Numbers by Year to June 1998.

(*Note that 1998 shows yearly total to end of June. All other years show total for that year)

4.6 It is noteworthy that in June 1998 AusCERT recorded the highest number of incidents within Australia in any month since its inception in March 1993.

4.7 In order to gauge the level of threat at the present time, two useful references are available, *Issues and Trends: 1998 CSI/FBI Computer Crime and Security Survey* the Computer Security Institute (CSI) in the United States, and the *1997 Computer Crime and Security Survey* ([OSCA97][4.6]), by the Office of Strategic Crime Assessments (OSCA) in Australia. Statistics from these studies are discussed in Appendix B.

4.8 There are many interesting statistics from these studies. One of the most important outcomes is that there is a severe lack of data available about the Australian experience. For instance, in the case of Australian sites who were broken into, only 19% reported the incident to law enforcement. There is a far larger volume of data about the US experience, and much of it is useful. However projections based on the US experience are not nearly as valuable as having accurate, locally compiled data. *This lack of data impairs our ability to understand the prevailing conditions and make the best possible decisions for the future.*

4.9 Various authors have already set out the potential for attack on Australian infrastructure ([Cobb98], [DSD97]), with stark and specific examples[4.7] in the US given by Pethia and Vatis[4.8] ([Pethia96], [Vatis98]). There have been documented attacks against some infrastructure organisations within Australia[4.9]. However apart from a notable first effort by OSCA, information such as this is difficult to obtain for the Australian experience. If this was because Australian sites are not being attacked then it would be a *good thing*. However we know that these attacks are occurring. Its possible but unlikely that the data required exists. If it does, it is not in a central obvious place. This lack of data is one of the primary problems we face in our national decision making. Even in the face of this problem, there are still constructive steps we can take *now*, and some decisions that we can make *now*. As we implement the solution, the fundamental problem of data scarcity should disappear with time.

# 5. Summary of Issues

5.1 In our opinion, the most urgent issue is without doubt that of the lack of availability of raw and processed data for informed decision making. This paper and other Australian studies have relied heavily on data drawn from the United States experience. One can only speculate on how much the Australian experience may differ. Until Australia has a national program for gathering information on the frequency and type of attacks on the NII, foreign experiences and *best informed guess* will continue to be our decision making technique. This is a theme echoed by the Defence Signals Directorate (DSD) ([DSD97]).

5.2 Obtaining and using the data in the long term is not the only problem. It is important to be able to identify an attack and respond in the short term to mitigate damage. The best way to respond is to quickly identify key sites and assist them in in identifying the source, gathering new intelligence and preventing damage. AusCERT seeks to do this with its membership, but it is not clear that there is such a national direction across the spectrum of government, educational and commercial organisations.

5.3 While Australia undoubtedly has the collective ability to produce good quality, high-tech products we are heavily dependent on foreign-made products for our NII. Brand names such as Cisco, Bay Networks, Sun Microsystems, Hewlett-Packard, Silicon Graphics, Checkpoint, RSA, Oracle are all well known and respected in the Australian IT industry. They all produce good quality products. As a nation, we continue to rely on them. Yet they are all owned and produced by foreign nations. In the event of a nation state wanting to disrupt the Australian NII, it is far easier to do so when the target relies on technology produced by the attacker - particularly when the attacker may be aware of weaknesses in the product that the victim isn't[5.1].

5.4 Related to this point is the problem of intellectual dilution. In the past few years, Australia has produced a number of individuals in the high-technology field who have gained international renown. While some of these individuals continue to practice in Australia, many others are attracted to the opportunity and financial rewards available in countries such as the United States. In fact, the US actively seeks talented foreigners to assist in strengthening the US position (militarily, financially and so on). So long as gifted individuals see better opportunity and reward overseas, it will be difficult for this country to retain them. When these people leave Australia for greener pastures they don't just take their store of knowledge and talent, but the expertise that they can pass on is now given to another country and not Australia. If we are to build a strong infrastructure and build the sort of products that will attract foreign sales, we must invest in our future by educating our young and retaining our talent.

5.5 Finally, in the case of national brain drain and important and emerging technology, those Australians best able to evaluate and apply the technology are either not in Australia, or alternatively plan to use the technology for specific commercial strategy. It is not clear that we as a nation are making a significant enough commitment to ensuring that our most capable technologists see a long-term, financially rewarding and intellectually challenging career in developing national policy and strategy[5.2].

# 6. Solutions and Recommendations [6.1]

6.1 In outlining the proposed solutions below, be aware that this paper is concerned only with a response at a national level - we are not seeking to delve into lower level technical issues here. However, it should be noted that a social response is necessary because *a purely technical response will not overcome all of the potential threats outlined earlier.*

6.2 Consequently, we believe that the solution requires a response across a number of sectors. Our specific recommendations are:

1. Establish an National Infrastructure Protection Agency, driven by a Council, with operation work carried out by a Warning Centre.
2. Establish an Australian Internet Communication Network.
3. Ensure that the system administration community is given the knowledge and tools needed to make sure the systems they administrate are secure.
4. Improve the national program of research and development.
5. Create an Emerging Technology Oversight Group.

6.3 These recommendations augment Cobb's work ([Cobb98]). Moreover, we also fully agree with NOIE ([NOIE98]) when they state that:

> Because electronic commerce crosses national boundaries, the government favours national approaches to strategic issues that are consistent with those evolving in a wide range of international fora. Australia is committed and already working to help develop a set of norms and conventions for international governance of electronic commerce across national boundaries, that accords with Australia's national interests and ensures the openness, safety, security, and fairness of all transactions.

6.4 Many very good recommendations have been made in the US context by the PCCIP ([PCCIP97]) - these are a mix of recommendations to improve state of affairs across the board (but with heavy cyber influence. A number of these look to be applicable to the Australian situation - in particular we believe that Chapter 8 in its entirety is worthy of consideration (translated to the Australian context of course). While finance and scalability may preclude us from adopting some of these recommendations, it is nevertheless worth considering how we can create a stronger infrastructure through educating the next generation of Australians. In any case, we won't further address the PCCIP work ([PCCIP97]) as the point of this paper is to look at some practical steps Australia could take to augment the feasible steps we could take from the PCCIP ([PCCIP97]).

6.5 Following are several proposed steps that we believe should be a part of a documented overall national strategy. The urgency required by the data gathering problem is reflected in this list, and we list the steps in what we believe to be descending order or urgency. All items should be considered important regardless of urgency, and we believe that it is in the national interest to address each item sooner rather than later.

## 6.1 A National Infrastructure Protection Agency (NIPA)

6.6 Cobb's ([Cobb98]) principle recommendation is that the Australian Government establish a National Infrastructure Protection Agency (NIPA), made up of a Council, a Warning Centre and a Secretariat. The proposed structure has some similarity to the one currently being implemented in the United States[6.2].

6.7 Some of the basic requirements proposed by Cobb already exist, or are in the process of being established. The Attorney-General's Department has convened the National Information Infrastructure Consultative Forum (NIICF), which will lead to a report to the Federal Government (expected in December 1998). Many of the participants of this forum will be players in the various industry components that comprise the Warning Centre. As Cobb notes, senior industry officials and Government ministers will possibly comprise the Council.

6.8 AusCERT's interest in this effort is to act as one of the participants in the Warning Centre, and possibly as one of the participants in the Council.

6.9 The primary problem identified earlier was a lack of raw data on which to make policy decisions at a number of levels and react to an attack in the short term. AusCERT has filled this role for Australia in a limited manner for over five years. While this paper is not intended to be a marketing document for AusCERT, it should be pointed out that AusCERT has coordinated incident response, vulnerability analysis and threat notification in this country and internationally, and gained universal respect in doing so ([SANS98]). However, while AusCERT is clearly respected among the expert community, the quality of information that we can provide to organisations such as national policy makers, individual clients, industry experts, and law enforcement agencies is limited by the size of our membership base.

6.10 Our proposal is that the Federal Government continue with the effort to implement the NIPA, and formally recognise AusCERT as a member of the Warning Centre, and desirably as a member of the Council. The outcome that we believe is necessary is that all government agencies with an Internet connection be required to become AusCERT members. Furthermore, we believe that strong encouragement should likewise be given to civil agencies to become AusCERT members, particularly those who conduct business with the federal government. This will realise the following benefits:

1. AusCERT's funding base becomes wider and its future viability is assured. This opens up the opportunity for AusCERT to expand its services to provide greater community benefit.
2. The combination of the encouragement from the government, and the position of AusCERT as an independent body will avoid any unease that organisations may feel in reporting to a regulatory body such as the Australian Federal Police (AFP) or DSD.

3. Because the subscription base is wider, the number of organisations reporting activity to AusCERT will be increased. This means that the quality of information that AusCERT can provide to the range of organisations mentioned earlier will be far greater.

4. The information that will be available will be a more accurate reflection of the current situation, rather than a sampling of information from sites who are already sufficiently aware of security issues to have voluntarily taken out AusCERT membership. Because the information will give a more accurate reflection, it can be used with confidence as part of an evaluation criteria for the threat facing Australia.

6.11 This whole-of-government and civil community approach is consistent with the stated objective of the Federal Government ([NOIE98]):

> Because electronic commerce crosses national boundaries, the government favours national approaches to strategic issues that are consistent with those evolving in a wide range of international fora.

6.12 AusCERT is aware of a project under the auspices of the Department of Primary Industries and Energy named the *Secure Gateway Environment (SGE)*. In brief, DPIE seeks to become a service provider by supplying a single, secure gateway to all government departments and act as a single point of contact for security issues.

6.13 Leaving aside technical discussion, we believe that it is important that all government departments referred to above become members as individual entities rather than on a centralised basis. This is necessary because of the following reasons:

1. In an Internet security incident, a site may either be the source of an attack or the destination of an attack. In either case, it is likely that if an Australian government site was involved, it would be considered a victim in some form. In times of attack, it is necessary to contact victim sites with as much haste as possible.

   Foreign entities under attack from an Australian government site may either try to contact the site directly, or contact AusCERT as a known Australian reference organisation. They are unlikely to contact the gateway site. If the gateway site was the contact point for individual government sites, an unnecessary extra point of contact in the communications structure would be inserted, thus retarding the speed of the response.

2. If a single focus for the entire government network infrastructure was created, then all departments would be at risk from what is essentially a single point of failure.

3. Finally, and most importantly, in the event of a break-in to a government network, there exists the possibility that an intruder may have compromised related networks (eg the SGE). This means that the intruder can control the information flow for the entire government network infrastructure, making the infrastructure unusable for the recovery.

   Because AusCERT is a separate organisation not reliant on the SGE, the intruder will not have control over the information flow. This ensures reliability, integrity and confidentiality in the response to the incident.

## AusCERT - Promoting Australia's Response to Internet-Based Attacks

6.14 It is important that Australia continue to have an ongoing incident response presence that is accessible across the entire civil landscape. The PCCIP makes the point in the US context that the "overall success of our own infrastructure assurance efforts will therefore require substantial international collaboration. The federal government should continue efforts to work with appropriate international bodies to address infrastructure protection concerns and raise the level of international cooperation and coordination on computer intrusion matters." ([PCCIP97], P64)

6.15 AusCERT has been *the* Australian presence in this arena for over five years. We work with internationally respected groups such Computer Emergency Response Team for the Deutsches Forschungsnetz (DFN-CERT) in Germany, the Oulu University Secure Programming Group (OUSPG) in Finland, the Network Associates Security Labs in Canada, and a variety of other groups throughout the world ([AA-98.04], [ESB-98.141]). We are a leader within the Forum on International Response and Security Teams (FIRST)[6.3].

6.16 In the same way that the AFP liases with international law enforcement agencies, that the Australian Defence Force liases with the defence forces of other countries, and the DSD liases with the international intelligence community, so too should AusCERT be recognised as the appropriate organisation to continue liaising with the international Internet incident response community. If Australia chooses to discontinue following this peer group model, then there is the possibility that domestic and internation cooperation will be eroded, since foreign peers may be wary of different and competing objectives.

## 6.2 An Australian Internet Communication Network

6.17 One of the problems alluded to earlier was the speed with which Australia is able to respond to a cyber attack. One of the reasons for this is that it isn't clear that we as a nation have established a reliable and formal network of contacts across the range of important sites in the Australian domain, and we have not developed a procedure for contacting these organisations in the event of a massive, coordinated attack.

6.18 Furthermore, in the event of an attack, the most quickest method of reaching a large audience in the Internet infrastructure community is by using the Internet - but this is not a viable solution since this is the very medium that will have been rendered untrustworthy. Therefore, we need to establish a more formal out of band framework to allow a quick response.

6.19 We propose that a more formal structure be established to allow such a swift response. We see this structure as essentially a working group comprised of the following partners:

- Attorney-General's Department,
- AusCERT,
- Industry user groups, such as the groups already represented in the ongoing NIICF,
- Regional network operators, such as Telstra and Optus,
- Representatives of the systems administrator community, and,
- Representatives of the Australian research and development community.

6.20 Each of these groups is suggested for a reason. We see their roles as follows.

6.21 The *Attorney-General's Department* at the present time is taking the lead in developing Australia's strategy to a cyber attack in the civil arena. As the primary architect and decision maker in this field, it is clear that the Attorney-General's Department should continue this leadership.

6.22 As discussed earlier, *AusCERT* is the suggested organisation to continue to collect data and provide information on attack trends, act as the warning centre, coordinate responses domestically and internationally at several levels, and liase with other important groups such as the vendor community.

6.23 The shape of the response coordination will depend on the attack. The general rule of thumb to consider is that direct coordination among victims is the most efficient in a small to medium sized attack. However, hierarchical coordination is likely to be a better solution in a much larger attack, where the coordination will be to large for one organisation.

6.24 In the case of an intense widespread attack, coordination will take the form of AusCERT working as the central point of contact at the operational level for the group of partners in this list. (Note: at this level, a group member is a representative of the organisations comprising particular industrial sector.) Each partner will then operate also as a coordination centre to coordinate the response among individual organisational members.

6.25 In the case where the attack is not a massive attack, but is an attack at particular organisations, AusCERT can conduct the coordination between individual organisations directly. Only when this job becomes clearly too large for one organisation would we switch to the hierarchical model.

6.26 It should be clear that one of the crucial aspects to ensuring this system works is the maintenance of an up to date and reliable contact database for important Internet-connected organisations within Australia (including government, commercial, educational, vendors, and other human resources). This database should contain not only contact information but also encryption keys so that encrypted traffic can be sent when necessary. AusCERT has maintained such a database of its members, and also of other parties such as vendors and experts, and other response teams.

6.27 If this model were to be adopted, its conceivable that there would need to be some sharing of contact information between coordinating bodies in the contact hierarchy, both for the sake of efficiency and redundancy. The nuts and bolts of this particular consideration can be set aside pending the adoption of this model.

6.28 The *industry user groups* referred to above are distinct groupings of industry sectors who use the Internet and may be affected by an attack against the NII. Examples may include the defence, government services, finance, health care, insurance and communications industries. In each case, distinct representatives of each industry would be useful for coordinating a response to an intensive attack. Furthermore, such representatives are invaluable industry experts to explain particular industry-specific risks or outcomes as an attack unfolds.

6.29 The *regional network operators*, such as Telstra and Optus, have an important role to play as ultimately much of the traffic that constitutes an attack may be carried over their networks. Such a group would also include larger Internet Service Providers (ISPs, such as Ozemail and Connect.com.au) and other major networks such as the Australian Academic and Research Network (AARNet2)[6.4]. A similar group exists in the United States for these reasons, amongst others. The name of this group is the North American Network Operators Group (NANOG[6.5]).

6.30 Any technical solution will require the cooperation and expertise of *system administrators* - the hands at the keyboard. For this reason it is important that system administrator groups have some awareness of the existing communications structure (even if there is some need to supply information on a *need to know* basis). Candidates for such groups would be the System Administrators Guild of Australia (SAGE-AU), the Internet Society of Australia (ISOC-AU), and perhaps the Internet Industry Association (IIA)[6.6].

6.31 The final group suggested for representation is the *research and development* community. At the time of an attack, victim sites and coordination teams are often working with incomplete information. Furthermore, because of the occasional intensity of activity, insufficient analysis may take place due to time constraints or fatigue. In situations such as this it is valuable to have another expert resource available, so that that group can do the necessary analysis and lateral thinking to develop short and long term defences.

## 6.3 Improved Operational Awareness and Expertise

6.32 Along with reliable data and communications, knowledge is an important facet in constructing a defence strategy. There are two areas where effort should be concentrated.

6.33 As discussed earlier, prevention and mitigation of an attack requires the cooperation and expertise of the system administration community. Since prevention is better than cure, it is important that as many sites as possible are aware of appropriate standards of practice, and implement these standards as far as possible. SAGE-AU have already begun internal discussions about the need document industry best practice. Other resources also exist[6.7] ([AS4444], [IIA98], [ACSI33]). There may be other opportunities for development in this area, such as:

- A register of available and appropriate training courses. Recognition or certification of such courses will increase the likelihood that knowledge levels among practitioners are of a consistent quality.
- Proposals to influence institutions and software vendors to train staff, and develop industry best-practice, quality, security-aware products.

6.34 Another initiative would be the training of industry groups in responding to cyber attacks. One problem that sites have faced in the past is not so much a lack of technical expertise, but a lack of procedures and a lack of knowledge about what's required by agencies such as law enforcement ([OSCA97]). For instance, the CERT/CC in the US offers courses on computer security incident handling[6.8]. In Australia, such courses could be put together and taught as a collaborative effort from organisations such as AusCERT and the AFP.

## 6.4 An Improved National Program of Research and Development

6.35 As stated earlier, one of the problems that we face is that we are almost totally reliant on imported technology for our computer network infrastructure. While Australia's reliance on imported hardware and software for our networking and IT infrastructure is unlikely to change significantly in short to medium term, it is recommended that mechanisms be explored to encourage development of our capability to ensure self reliance on critical infrastructure.

6.36 The security area is somewhat immature as a technology, although it is developing rapidly. There is opportunity for the development and commercialisation of specialist products and services.

6.37 An example is the development of products that emerge from research into the nature of software vulnerabilities and the steps that can be taken to prevent them and exploit them. This type of research is already underway in Australia and in other organisations overseas, such as the CERT/CC in the US[6.9] the OUSPG in Finland, among other places[6.10]. Additionally, research in intrusion detection systems, with an aim to produce a robust product is necessary[6.11]. The outcome of this type of research would be to feed in with the technology infrastructure work. It would also assist response teams, such as AusCERT, to more efficiently fill their Warning Centre role by allowing *proactive* warnings rather than *reactive* warnings.

6.38 The future of this type of research is uncertain at the present time. The Digital Millennium Act in the US ([Spaf98], [WIPO98]) is creating fear and uncertainty in the response team community throughout the world. Similar legislation is being considered in Australia in the form of the *Digital Agenda* copyright reforms[6.12]. While AusCERT commends reforming inadequacies in current copyright law, it should be noted that *prevention of software vulnerability analysis under such a law would seriously impair the ability of a warning centre to adequately perform its task.* It is essential that the capability is developed to enable development and dissemination of expert opinion on security issues to ensure maintenance of the NII.

## 6.5 An Emerging Technology Oversight Group (ETOG)

6.39 Another initiative that the federal government may consider is the establishment of an Emerging Technology Oversight Group (ETOG). The purpose of this group would be an early adoption agency with a view to understanding emerging technology and its implications. When new technology emerges, adopters must take time to understand the technology and how it will affect their operation, and only then develop an integration plan. A large part of this is, naturally enough, dependent on the information that the vendor chooses to pass on - information geared towards sales. Meanwhile, the intruder community can quickly gain an understanding. This amounts to technology adopters being at risk of attack from day one.

6.40 The ETOG would be an early adoption and evaluation agency. It would act as a reference point to give an alternative view of infrastructure technology without needing to place a market spin on the evaluation. Gaining an early understanding of a product and its weaknesses (gained as early as pre-release test cycles) will assist those sites adopting the technology to be forewarned of any potential problems, and hence fore-armed. Examples of emerging technology that should be examined are listed in [CERT97-2].

6.41 The ETOG would conceivably work with the industry user groups and Warning Centre to be as proactive as possible, thus allowing the Australian infrastructure to progress with confidence.

# 7. Conclusion

7.1 The integrity of Australia's national communications infrastructure is a complex issue requiring a coordinated response from across many sectors of the community. In this paper we have outlined components of a solution which we believe essential in the risk management of this critical and strategic resource.

7.2 There is insufficient data on which to base many decisions. However, we cannot afford not to do anything. This proposal provides a manageable and cost effective way forward to develop such a community response to the problem of security of our Internet-based National Information Infrastructure.

# Notes

*[1.1] An example of some of the other legal debate taking place in Australia can be seen in [Prospect98].*

*[1.2] Examples of Internet pages that can be used for locating individuals are:*

- *Telstra White Pages*
- *Four11 Directory Services*
- *Database America People Finder*
- *Yahoo!*
- *AltaVista*

*[1.3] Name servers are machines that act as the address book for all machines on the Internet. They operate on a hierarchical basis. Attacking the root name servers (i.e. the highest ones in the Internet namespace), of which there are a small number, would probably compromise the entire Internet. Examples have been documented by the CERT/CC in the United States ([CA-98.05]).*

*[2.1] The federal government has initiated the Australian Electronic Business Network (AUSe.NET) to foster awareness of electronic commerce among small to medium enterprises (SMEs). The web page notes a 1996 report by Monash University ("Advice on Electronic Commerce Programs for SMEs"), in which the following statement appears: "electronic commerce, per se, is not high on the agenda of successful and innovative small businesses in Australia, nor is it considered to be an important contributor to their success, at the present time". See http://www.aebn.org.au.*

*[2.2] See http://www.ato.gov.au and http://www.ato.gov.au/general/individs/etax98/Welcome.htm.*

*[2.3] The author was a panelist at a HotTopic session Information Security at the The 6th National Health Informatics Conference on Tuesday 28th July 1998. There was clearly some concern among the audience and panelists about how the dilemmas and problems faced in making electronic patient records available electronically (whether the mechanism is via the Internet or other means).*

*[2.4] See the Victorian Government's Internet Policy ( http://www.vic.gov.au/ocmpol/215a.htm).*

*The background states that "It is desirable that:*

- *any Government-held information which is deemed as freely available should be made as accessible as possible.*
- *quality of service be improved by bringing services and information as close to the client as possible.*
- *services be publicised widely.*
- *client self-help be encouraged, to decrease cost of service delivery."*

*[2.5] Fedex (http://www.fedex.com/au) and UPS ( http://www.ups.com/asia/tracking/tracking.html) are examples in the civil arena.*

[2.6] *See the United States Department of Defense briefing of 16 April 1998 at http://www.defenselink.mil/news/Apr1998/t04161998_t0416asd.html, and another discussion in [SMH98].*

[4.1] *See Network Wizards home page at http://www.nw.com.*

[4.2] *See http://www.nw.com/zone/WWW/new-survey.html for a description of the process.*

[4.3] *See http://www.nw.com/zone/WWW/dist-bynum.html.*

[4.4] *See http://www.nw.com/zone/hosts.gif.*

[4.5] *See http://www.cert.org/stats/cert_stats.html.*

*Note that the term incident can be very deceptive. At the most trivial level, an incident may consist only of one minor probe from one machine to another, with no real action required other than logging the event.*

*The vast majority of incidents logged by the CERT/CC are more serious than this. Most incidents involve a much larger number of machines, sometimes in the tens of thousands, with deep levels of network penetration. Such incidents may take months of intensive work to coordinate and resolve. Along the way there may be any number of political, legal and financial issues that require negotiation. (During the author's term of employment at CERT/CC, the view was expressed that a collective memoir would give a Tom Clancy novel a run for its money!)*

*While the AusCERT experience isn't identical to this, it is nevertheless quite similar. As Australia follows the same technological path that the United States follows, the two experiences will almost certainly converge.*

[4.6] *In our opinion, [OSCA97] is an invaluable resource and a tremendous first attempt at what should be an annual or bi-annual evaluation of NII health. One problem within the report, and this is symptomatic of Internet security affairs in Australia in general, is that the report doesn't contain enough details. However, as the survey and reporting procedure is refined, this problem should diminish.*

[4.7] *A notable report of a probe to an organisation producing an emerging encryption technology is documented in [Meganet98-1] and [Meganet98-2]. In the obviously heightened state of the developer, it would be interesting to determine whether the probe was benign, and if not, who gave the order to launch the probe.*

[4.8] *Vatis is the Chief of the National Infrastructure Protection Center. This facility is one part of the implementation of the PCCIP report ([PCCIP97]). See http://www.fbi.gov/nipc/welcome.htm.*

[4.9] *See R V Cooper (unreported), District Court Brisbane, 20 December 1996, in which a person was convicted of breaking into systems used by the Australian Electoral Commission. The Sunday-Mail on 29 December 1996 (P34) reported that "Cooper had used his skills to invade the AEC's system via the Internet. He had gained access to the system at the highest level, which would have enabled him to install programs and alter existing programs and data in the system. The AEC's system included the electoral roll of 11.5 million Australians, including some personal details not made public. The system enabled fast counting on election nights and was used for payroll details of some 60,000 casuals employed on election night." [SM96]*

[5.1] *The author is well aware that many of these brandnames are produced by US organisations. It is absolutely* **not** *the author's intent to infer in any way that the United States has any malevolent intent towards Australia nor seeks to undermine the Australian NII. The thrust of the argument is that Australia is building an infrastructure on materials produced by organisations that would ultimately be* **required** *to have loyalties to another nation.*

*In 1998, it so happens that for the most part, the* **other nation** *happens to be the United States - a national ally of long-standing that is well trusted and for whom Australia has great affection. However, our practice has been that we purchase operating systems, routers, and firewalls from foreign corporations rather than build our own. What happens in 2020 when Xylonia wants to bring down the Australian economy? Will our collective, implicit decision in 2010 to base our 80% of our information economy on firewalls from the country of Xylonia seem unwise?*

*What we seek to do is to be cognisant of this and to develop capabilities and strategies to defend the NII in this environment.*

[5.2] *This problem is not confined to the high technology field. The author was speaking recently with a professor in a non-technical field who lamented that he was having great difficulty recruiting Australians graduating from PhD programs in the United States. His problem was that salaries and conditions offered in the Australian academic arena just don't compare with those available in the US academic environment. The outcome was that our best minds were lost to another nation.*

[6.1] *A symposium on cross-industry activities for information infrastructure robustness is taking place in Crystal City, Virginia in the US in early November 1998. More information can be found at http://www.xiwt.org/ROBIN/ROBIN-Nov98-Symp.html.*

*Another workshop, "Information Survivability Workshop 1998 - Protecting Critical Infrastructures and Critical Applications" is taking place in Orlando, Florida in the US in late October 1998. More information can be found at http://www.cert.org/research/isw98.html.*

[6.2] *See http://www.fbi.gov/nipc/organization.htm.*

[6.3] *See the following for more information:*

- *DFN-CERT: http://www.cert.dfn.de/eng*
- *Network Associates Security Labs: http://www.nai.com/products/security/advisory*
- *OUSPG: http://www.ee.oulu.fi/groups/ouspg*
- *FIRST: http://www.first.org*

[6.4]*A AARNet has already started work in this area. On 27 October 1998, a closed workshop will take place in which there will be specific technical discussion on defences against a spate of Denial of Service attacks that have taken place on that network. Invitees include CAUDIT members, AusCERT and regional network operators such as Telstra and Optus.*

[6.5] *See http://www.nanog.org.*

[6.6] *See:*

- *http://www.sage-au.org.au*
- *http://www.isoc-au.org.au*
- *http://www.iia.net.au*

[6.7] *In addition to the listed references, see also the Security Improvement Modules Developed by the CERT/CC in the United States at http://www.cert.org/security-improvement/modules.html.*

[6.8] *See http://www.cert.org/training/index.html.*

[6.9] *This is in fact mandated by law in the United States. Section 10 of the Computer Security Enhancement Act of 1997 (H. R. 1903) states the following: "There are authorized to be appropriated to the Secretary of Commerce $250,000 for fiscal year 1998 and $500,000 for fiscal year 1999 for the Director of the National Institute of Standards and Technology for fellowships, subject to the provisions of section 18 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-1), to support students at institutions of higher learning in computer security. Amounts authorized by this section shall not be subject to the percentage limitation stated in such section 18."*

[6.10] *This research is well underway already. Refer to [CERT97-3], and to the following:*

- *http://www.isrc.qut.edu.au*
- *http://www.svrc.it.uq.edu.au*
- *http://www.cert.org/research*
- *http://seclab.cs.ucdavis.edu/projects/vulnerabilities*
- *http://www.cs.purdue.edu/coast/projects/vuln_test.html*
- *http://www.ee.oulu.fi/groups/ouspg*

[6.11] *This area of research is in an interesting stage. Many commercial products are able to detect intrusions using already known techniques. The problem that needs to be solved is detecting intrusions using a fingerprint that is* **not** *already known. There has been some research in this area using neural networks at the University of Melbourne.*

*Another interesting organisation is Network Flight Recorder, Inc. ( http://www.nfr.net). This organisation is involved in a project named Cooperative Intrusion Detection Evaluation and Response (CIDER), along with "NSWC Dahlgren, Network Flight Recorder, NSA, the SANS community and other interested parties". See http://www.nswc.navy.mil/ISSEC/CID/index.html for details.*

[6.12] *See [CLRC95].*

# Acronyms

| | |
|---|---|
| AARNet | Australian Academic and Research Network |
| AFP | Australian Federal Police |
| AusCERT | Australian Computer Emergency Response Team |
| CAUDIT | Committee of the Australian University Directors of Information Technology |
| CERT/CC | CERT Coordination Center |
| CSI | Computer Security Institute |
| DFN-CERT | Computer Emergency Response Team for the Deutsches Forschungsnetz |
| DNS | Domain Name Service |
| DSD | Defence Signals Directorate |
| ETOG | Emerging Technology Oversight Group |
| EuroCERT | European Security Incident Information Service |
| FIRST | Forum of Incident Response and Security Teams |
| IIA | Internet Industry Association |
| IPv6 | Internet Protocol version 6 |
| ISOC-AU | Internet Society of Australia |
| ISP | Internet Service Provider |
| NANOG | North American Network Operators Group |
| NII | National Information Infrastructure |
| NIICF | National Information Infrastructure Consultative Forum |
| NIPA | National Infrastructure Protection Agency |
| NOIE | National Office of the Information Economy |
| OGIT | Office of Government Information Technology |
| OSCA | Office of Strategic Crime Assessments |

| | |
|---|---|
| OUSPG | Oulu University Secure Programming Group |
| PCCIP | President's Commission for Critical Infrastructure Protection |
| PKI | Public Key Infrastructure |
| SAGE-AU | System Administrators Guild of Australia |
| SGE | Secure Gateway Environment |

# References

[AA-98.01] Australian Computer Emergency Response Team, *qpopper Buffer Overrun Vulnerability*, 3 July 1998. Available on line: ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-98.01.qpopper.buffer.overflow.vul.

[AA-98.04] Australian Computer Emergency Response Team, *Sendmail, Inc. Patch for MIME Buffer Overflows*, 11 August 1998. Available on line: ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-98.04.sendmail.MIME.patches.

[ABS98] Australian Bureau of Statistics, *Use of the Internet by Householders*, Australia, May 1998. Available on line: http://www.abs.gov.au/websitedbs/D3110122.NSF/66b4effdf36063e24a25648300177cd5/b61b772e5ff248764a25666a0083650e?OpenDocument.

[ACSI33] Defence Signals Directorate, *Australian Communications - Electronic Security Instructions 33. Security Guidelines for Australian Government IT Systems.*, January 1996. Available on line: http://www.dsd.gov.au/acsi33.

[AS4444] Standards Australia, *Australian Standard 4444 - Information security management*, 5 November 1996.

[AusCERT98] Australian Computer Emergency Response Team, *Incident Statistics for 1998 So Far*, AusCERT Newsletter Volume 2, Number 2. July 1998. Available on request.

[CA-97.20] CERT Coordination Center, *JavaScript Vulnerability*, 8 July 1997. Available on line: http://www.cert.org/advisories/CA-97.20.javascript.html.

[CA-98.05] CERT Coordination Center, *Multiple Vulnerabilities in BIND*, 8 April 1998. Available on line: http://www.cert.org/advisories/CA-98.05.bind_problems.html.

[CA-98.10] CERT Coordination Center, *Buffer Overflow in MIME-aware Mail and News Clients*, 11 August 1998. Available on line: http://www.cert.org/advisories/CA-98.10.mime_buffer_overflows.html.

[CERT97-1] Ellis, J., Fisher, D., Longstaff, T., Pesante, L., Pethia, R., *Report to the President's Commission on Critical Infrastructure Protection*, January 1997. Available on line: http://www.cert.org/pres_comm/cert.rpcci.body.html.

[CERT97-2] Longstaff, T. A., Ellis, J. T., Hernan, S. V., Lipson, H. F., McMillan, R. D., Pesante, L. H., Simmel, D., *Security of the Internet*, September 1997. Published in *The Froehlich/Kent Encyclopedia of Telecommunications vol. 15.* Marcel Dekker, New York, 1997, pp. 231-255. Available on line: http://www.cert.org/encyc_article/tocencyc.html.

[CERT97-3] Ellison, R. J., Fisher, D. A., Linger, R. C., Lipson, H. F., Longstaff, T. A., Mead, N. R., *Survivable Network Systems: An Emerging Discipline*, November 1997. Available on line: http://www.cert.org/research/tr13/97tr013title.html.

[CLRC95] Copyright Law Review Committee, *Computer Software Protection*, 1995, Australian Government Printing Office. ISBN 0 642 20830 1.

[Cobb98] Cobb, A. C., *Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks*, June 1998. Available on line: http://www.aph.gov.au/library/pubs/rp/1997-98/98rp18.htm.

[CSI98] Computer Security Institute, *Annual cost of computer crime rise alarmingly - Organizations report $136 million in losses*, 4 March 1998. Available on line: http://www.gocsi.com/prelea11.htm.

[DSD97] Defence Signals Directorate, *The National Information Infrastructure: Threats and Vulnerabilities*, February, 1997.

[ECEG98] Electronic Commerce Expert Group, *Electronic Commerce: Building the Legal Framework*, April 1998. Available on line: http://law.gov.au/aghome/advisory/eceg/ecegreport.html or http://law.gov.au/aghome/advisory/eceg/single.htm.

[ESB-98.141] Australian Computer Emergency Response Team (courtesy of Network Associates, Inc.), *Stack Overflow in ToolTalk RPC Service*, 4 September 1998. Available on line: ftp://ftp.auscert.org.au/pub/auscert/ESB/ESB-98.141.

[IDC98] IDC Australia Pty Ltd, *Internet Commerce Revenues in Australia to Reach $16 Billion by 2002*, 1997. Available on line: http://www.idc.com.au/Hot-internet.htm.

[IIA98] Internet Industry Association, *Industry Code of Practice*, Third Draft , 2 February 1998. Available on line: http://www.iia.net.au/news/code3.html.

[McMillan98] McMillan, R.D., *Removing the Mouse's Roar*, September 1998. Available on request.

[Meganet98-1] Meganet Corporation, *Virtual Matrix Encryption Explained.*, Available on line: http://www.meganet.com/explain.htm.

[Meganet98-2] Meganet Corporation, *Russian Federation Lab-1313 Forces 2 Massive Attacks On Meganet Corporation Servers In Search For Virtual Matrix Encryption Secrets.*, Press Release 21 July 1998. Available on line: http://www.meganet.com/07-21.htm.

[NOIE98] National Office for the Information Economy, *Towards an Australian Strategy for the Information Economy*, July 1998. Available on line: http://www.noie.gov.au/nationalstrategy/strategy.html.

[NPKIWP98] National Public Key Infrastructure Working Party, *Strategies for a Peak Body for an Australian National Electronic Authentication Framework*, March 1998. Available on line: http://www.noie.gov.au/reports/npki/npkiworkingpartyreport.html.

[NYT97] Krieger, T., *Hackers Go on TV to Show Perils in ActiveX*, New York Times, 13 February 1997. Available on line: http://www.nytimes.com/library/cyber/week/021397activex.html.

[OSCA97] Office of Strategic Crime Assessments, *1997 Computer Crime and Security Survey*, 1997.

[PCCIP97] President's Commission on Critical Infrastructure Protection*, Critical Foundations: Protecting America's Infrastructures*, October 1997. Available on line: http://www.pccip.org.

[Pethia96] Pethia, R. D., *Testimony of Richard Pethia Before the Permanent Subcommittee on Investigations U.S. Senate Committee on Governmental Affairs*, June 1996. Available on line: http://www.cert.org/congressional_testimony/testimony_Pethia96.html.

[Prospect98] Fitzgerald, A., Fitzgerald, B., Cook, P., Cifuentes, C., Ed., *Going Digital - Legal Issues for Electronic Commerce, Multimedia and the Internet*, Prospect Media Pty Ltd, 1998. ISBN 1 86316 134 1.

[RFC1296] Lottor, M., *RFC1296 - Internet Growth (1981-1991)*, January 1992. Available on line: http://www.nw.com/zone/rfc1296.txt.

[SANS98] The SANS Institute, *Australian Group Bestowed World-Wide Award For Improving Computer Security*, August 1998. Available on line: http://www.auscert.org.au/Information/sans.html.

[SM96] Hansen, P., *Hacker promises to log off*, The Sunday-Mail, 29 December 1996.

[SMH98] Gilligan, A., *When hackers converged in casino city*, Sydney Morning Herald, 15 September 1998. Available on line: http://www.it.fairfax.com.au/smh/980915/industry/industry1.html.

[Spaf98] Spafford, E. H., *WIPO Letter Campaign*, July, 1998. Available on line: http://www.cs.purdue.edu/homes/spaf/WIPO/index.html.

[Vatis98] Vatis, Michael, *Statement for the Record Michael A. Vatis, Deputy Assistant Director and Chief, National Infrastructure Protection Center Federal Bureau of Investigation Before the Congressional Joint Economic Committee*, 24 March 1998. Available on line: http://www.fbi.gov/congress/vatis.htm.

[Wallack98] Wallack, T., *Techno terrorism: U.S. feared ripe for cyberattacks*, The Boston Herald, 30 August 1998. Available on line: http://www.bostonherald.com/bostonherald/lonw/31terrw.htm.

[WIPO98] 105th Congress of the United States of America, *H. R. 2281 - Digital Millennium Copyright Act , August 1998*. Available on line: http://thomas.loc.gov/cgi-bin/query/C?c105:./temp/~c105dBof5h.

# Appendix A
# Attacks Against Current Technology

A.1 In this appendix, we present a brief, high-level discussion of some of the techniques that can be used in attacking a large number of systems, such as those that would compromise some aspect of an NII.

## A1. Background

A.2 To set the background for some of these examples, it is important to understand two concepts - potential points of attack in a physical sense, and potential points of attack in a logical sense. When we refer to the NII we refer to the overall collection of physical networks, and the software that relies on these networks.

A.3 Points of attack in the logical (or virtual) world can occur either at the application level (that is, the specific application that a user will see, such as a web browser or electronic mail program), or at the lower operating environment. Most lay folk will have some idea of the NII consisting of the services listed above (for example), built over some nebulous aggregation of computer systems that constitutes the operating environment. The bulk of AusCERT's experience lies in understanding the lower, more technical level and it is our opinion that this is where we should continue to focus. For it is this level that a serious intruder will try to attack, because if you undermine the foundation you can compromise any application that relies on it. The flip side is that if the foundation is more robust, then there is less potential for damage should an intruder compromise an application.

A.4 Attacks may be either on individual computer systems (or hosts) or at the network level. This is perhaps best illustrated using an example. Lets assume that a consumer buys a book from an online bookstore using the web. The consumer transmits their credit card number using a form. An intruder may be able to intercept that credit card number by monitoring data at any point on the network media between the consumer's machine (the client) and the bookshop's machine (the server). However, from media reports the consumer knows that some type of encryption should be used. Therefore the encrypted credit card number will foil the attacker who monitors (or sniffs) it over the network, but the number will almost certainly be stored in plain text on either the client or server machine, and therefore these become a likely point of attack.

A.5 The following sections discuss particular types of vulnerabilities that have been commonly used in widespread attacks. The purpose of this examples is to remove some of the mystery for the interested, non-technical reader. This is not a comprehensive list, but it gives realistic examples of current technology.

## A2. Buffer Overflows

A.6 A very elementary class of problem that we have seen many examples of in the past are basic coding errors, such as buffer overflows. This term relates to instances in which a program has a finite amount of memory space set aside for a datum, but no method to ensure that the input doesn't exceed the amount of space set aside. The attacker then crafts appropriate input of sufficiently large size to overflow that space. By inserting particular values at particular points of the input, it is possible to then make the computer system execute arbitrary instructions at the attacker's whim. Cookbooks have been produced in the intruder and research communities to demonstrate how to produce such an attack in a well defined and reliable manner against a vulnerable program.

A.7 We have seen hundreds of examples of this type of vulnerability, and we still see examples even today ([AA-98.01], [CA-98.10]).

## A3. Domain Name Service (DNS)

A.8 The Internet operates around a service known as the Domain Name Service (DNS). The DNS provides all of the machine name and address mapping for the Internet. It is built around a hierarchical structure, with several top level (or root) DNS servers, which source a large hierarchy of domain specific servers. Much of this system, although distributed across a range of vendor products, is built around a common code base. Furthermore, the protocol used to exchange mappings between machines is known to be insecure.

A.9 The implication of this is that it is possible under some circumstances for one machine to pretend to be another. This means that although the user believes that they are connecting with one machine, they may in fact be connecting with another (a "spoofing attack"). When a vulnerability implying this type of problem occurs, the Internet community scrambles as this is considered to be an extremely serious technical class of problem.

A.10 Furthermore, there are occasionally implementation problems in the code used to implement this system ([CA-98.05]). This is another example of a vulnerability that causes the Internet community to scramble. He who controls the DNS effectively controls the Internet.

## A4. World Wide Web Browsers

A.11 Many applications that we see being developed today are based on web technology. Browser technology is still so young that new features appear with bamboozling regularity. However, one trend that is clear is the movement towards executable code downloaded from another machine, performing some function on the client machine. Examples include Java, Javascript and Active-X. While this technology is potentially extremely useful (and we do not want to dissuade its development at all) these examples have already had their problems ([CA-97.20]). A particularly interesting example was highlighted by the Chaos Computer Club in Germany, illustrating the danger of tools such as Active-X ([NYT97]).

A.12 We expect that executable code downloaded over the network may present more problems in the future, particularly given the complexity of the system. Vendors will argue that code certification mitigates the problem. Our response is that it doesn't really matter if who know who did the damage - it would have been far better if the damage had never been done.

A.13 Another problem besides implementation issues is the default configuration as shipped by the vendor. Vendors consistently ship software to highlight features and convenience. However, with facilities such as executable content, many users will not possess the knowledge of what the browser is capable of by default, much less how to disable it[a1.1].

## A5. Closing Thoughts

A.14 Yet another class of attacks are possible by exploiting vulnerabilities that exist in basic Internet protocols. Examples of such attacks and the problems they present are set out in [McMillan98]. Other examples are those relating to the DNS problems discussed above. Protocol based vulnerabilities are by far the hardest to solve. Protocols are absolutely ingrained into the structure of the Internet. More robust protocols are always under development (eg IPv6) but even then, implementation problems and perhaps new classes of protocol related problems are still likely to occur occasionally.

A.15 Furthermore, it won't matter how robust a protocol and its implementation are. Problems that arise due to lack of knowledge, lack of policies and procedures, and social engineering will still be possible.

[a1.1] *This problem doesn't just apply to web browsers. Operating systems are notorious for being shipped configured for optimum convenience, not security.*

# Appendix B

# Statistics Describing the Potential Threat

B.1 In order to gauge the level of threat at the present time, two useful references are available, *Issues and Trends: 1998 CSI/FBI Computer Crime and Security Survey* the Computer Security Institute (CSI) in the United States, and the *1997 Computer Crime and Security Survey* ([OSCA97][4.6], by the Office of Strategic Crime Assessments in Australia (OSCA).

B.2 CSI make the following observations ([CSI98]):

- *64% of respondents report computer security breaches within the last twelve months. This figure represents dramatic increases of 16% increase over the "1997 CSI/FBI Computer Crime and Security Survey" results, in which 48% of respondents reported unauthorized use and 22% increase over the initial 1996 survey, in which 42% acknowledged unauthorized use. (Note: If you include those reporting only incidents of computer virus or laptop theft, the number rises to 88% of all respondents.)*

- *Although 72% of respondents acknowledge suffering financial losses from such security breaches, only 46% were able to quantify their losses. The total financial losses for the 241 organizations that could put a dollar figure on them adds up to $136,822,000. This figure represents a 36% increase in reported losses over the 1997 figure of $100,115,555 in losses.*

- *Security breaches detected by respondents include a diverse array of serious attacks. For example, 44% reported unauthorized access by employees, 25% reported denial of service attacks, 24% reported system penetration from the outside, 18% reported theft of proprietary information, 15% reported incidents of financial fraud, and 14% reported sabotage of data or networks.*

- *The most serious financial losses occurred through unauthorized access by insiders (18 respondents reported a total of $50,565,000 in losses), theft of proprietary information (20 respondents reported a total of $33,545,000 in losses), telecommunications fraud (32 respondents reported a total of $17,256,000 in losses) and financial fraud (29 respondents reported a total of $11,239,000 in losses).*

- *The number of organizations that cited their Internet connection as a frequent point of attack rose from 47% in 1997 to 54% in 1998. This represents a 17% increase over the initial 1996 figure of 37%. And significantly, the number of respondents citing their Internet connection as a frequent point of attack is now equal to the number of respondents citing internal systems as a frequent point of attack. (In the past, internal systems has been considered to be the greater of problems. It is not that the threat from inside the perimeter has diminished, it is simply that the threat from outside, via Internet connections, has increased.) This trend was reinforced by another piece of data. Of those who acknowledged unauthorized use, 74% reported from one to five incidents originating outside the organization, and 70% reported from one to five incidents originating inside the organization.'*

B.3 The OSCA report had 159 usable responses from 310 organisations polled. Some of the findings were:

- 37% of respondents had suffered from some form of unauthorised use within the preceding 12 months. Another interesting finding is that an additional 17% did not know whether they had or not.

- It is not possible to obtain a precise figure on the cost of of these incidents, although it would appear to be of the order of around $5,000,000, an order of magnitude less than that noted by the CSI ([CSI98]). Of course, the impact of an intrusion cannot always be measured in purely financial terms, and it is attacks such as these which may have the greatest impact.

- Although 49% of respondents felt that intrusions were only motivated by curiosity, almost the same number (46%) felt that the intrusion was motivated by some combination of financial gain, espionage, extortion or terrorism. Between 40% and 45% of respondents classed the misuse as one of theft, damage, manipulation or copying of data (as opposed to simple unauthorised use of the machine). However, very few respondents felt that the intrusion was institutional (namely, a competitor or foreign government). In the vast majority of cases it was felt that the threat came from an individual (such as a "hacker" or disgruntled employee).

- 61% of sites who had experienced an intrusion had identified a source as being external to their organisation. 87% of sites who had experienced an intrusion had identified a source as being internal. Amazingly, in each case, a significant number of respondents (32% and 23% respectively) were unable to identify whether the source was external or internal.

- A slight inconsistency in reporting was uncovered. Of sites that suffered an intrusion, only 19% reported it to a law enforcement body, and 7% to a response team. Yet 30% of all sites stated that they would be willing to report an incident to a law enforcement agency immediately in the even of an incident (without qualification).

What this means is that 70% to 80% of sites fall in the range of unwilling to report to law enforcement under any circumstances to being willing to do so with conditions attached. Common wisdom evolved over time is that many intrusions are not reported because of privacy and related concerns. It would be interesting to determine whether sites would be willing to report to a non-regulatory organisation if there was some guarantee that the data was sanitised and was used for national policy for public benefit and corporate growth.