



Trust and Security on the Internet

Keeping the Internet safe for e-government in New Zealand

A report by the State Services Commission's E-government Unit

24 November 2004

1	Introduction	3
	1.1 Background	
	1.2 Scope	
	1.3 Approach	
	1.4 Digital Strategy	
2	Role of government in Internet security	5
	2.1 Public confidence in using the Internet	
	2.2 Law enforcement	
	2.3 'Public health' on the Internet	
3	Problems on the Internet.....	7
	3.1 Attackers	
	3.2 How Internet attacks work	
4	Analysis	11
	4.1 Framework for analysis	
	4.2 Assets	
	4.3 Threats	
	4.4 Possible actions	
5	Conclusions	23
	5.1 Recommendations	
	Appendix – Threat Assessment.....	26

1 Introduction

This paper assesses threats on the Internet as they relate to e-government, and considers whether the government should do more to protect the use of the Internet for e-government purposes. It is intended to guide policy.

1.1 Background

The e-government programme aims to improve the delivery of Government services and information by using information technology and the Internet. A specific goal of e-government is that, by June 2007, networks and Internet technologies will be integral to the delivery of government information, services and processes. To meet this goal, the New Zealand government is making substantial investments in putting its services online.

The e-government programme was created as a way of exploiting the many benefits that technology, including the Internet, can offer, the better to serve New Zealand people. In principle, people should be able to interact with government using the same technologies as they do with many private companies. Beyond this, the Internet has the potential to enhance the application of democracy through greater access to information and wider consultation. The E-government Strategy¹ develops these ideas more fully.

However, as well as benefits the Internet harbours threats. It has a dark side. Newly purchased computers fall victim to attacks in a matter of minutes when connected to the Internet.² Dealing with the latest software flaw has become the stuff of mainstream news reports. Spyware, worms and spam have gone from mere nuisances to being tools of organised crime.

It would not be surprising if people's concerns about the problems associated with the Internet made them more cautious about what they do online. This is largely a good thing, provided that it focuses correctly on high risk behaviour and does not lead to a blanket rejection of doing business online, of e-mail in general or even of the whole Internet. Yet the negative experiences many are having when connecting to the Internet may cause such a withdrawal.

Surveys in 2002 and 2003³ showed that there is a challenge ahead in making people feel safe about using the Internet and e-government. The challenge is to control the problems that people face on the Internet, to ensure they know how to use the Internet without adverse effects, and to help people recover from problems such as computer viruses and identity theft.

This project has sought to understand the issues affecting trust and security on the Internet as they affect e-government in New Zealand, and makes recommendations for government action to mitigate some of the issues.

1.2 Scope

In scope:

- Explore the link between security and use of Internet-based online services.
- Assess perceptions versus reality of security around online services.
- Assess the risks of security failures to damage uptake of online government services.

¹ Available at e.govt.nz

² For instance *Windows XP: Surviving the First Day* SANS Institute Internet Storm Center 23 November 2003, sans.org/rr/papers/index.php?id=1298

³ GO2002 and GO2003, Taylor Nelson Sofres plc, e.govt.nz/docs/go-survey-2002/ and e.govt.nz/docs/go-survey-2003/

- Assess technical, educational and legislative options to improve security (real and perceived) on the Internet.

Out of scope:

- Dealing directly with government security issues.
- Assessing government personnel risks (“insider risks”) which are already the focus of the SSC standards, values and ethics project.
- Detailed financial modelling (if the project identifies a potential measure whose costs and benefits require detailed analysis, this will be proposed as a recommendation).
- Other factors affecting trust in e-government such as fulfilment failure.
- Other risks online that would be characterised as ‘personal safety issues’ as opposed to security risks, such as cyberstalking, ‘grooming’ of children in chatrooms etc. These situations may also contribute to a lack of trust in the Internet.

1.3 Approach

Steps on the way to this report:

- A preliminary assessment of the threats.
- Consultation with Internet players (InternetNZ, ISPs, telcos) on the extent of threat and possible solutions.
- Preliminary analysis of potential government responses.
- Consultation with government agencies.
- This final report.

1.4 Digital Strategy

In June 2004 the Government released a draft digital strategy for consultation

This report is listed under the *Safety and Security* section of the Draft Digital Strategy⁴ as the Trust and Security e-government project. In that section, the draft strategy notes the concerns of businesses and consumers that restrict their use of the Internet due to concerns about virus attacks and people trying to break into their computers.

This report agrees with the draft Strategy that business and consumers require adequate legislation, self-regulation and education to protect them from attacks and fraud via the Internet. The recommendations of this report are consistent with the actions listed in the draft Strategy to address the challenges it identifies.

⁴ A Draft Digital Strategy for New Zealand, *Ministry of Economic Development*, June 2004, med.govt.nz/pbt/infotech/digital-strategy/draft/

2 Role of government in Internet security

There are several reasons for government involvement in Internet security matters.

2.1 Public confidence in using the Internet

To use a government service online, people need confidence in the Internet, in online services in general, and in government services online specifically. Surveys indicate that this confidence may not be very high:

- A 2003 New Zealand telephone survey⁵ showed that 35% of the population consider it safe to provide the government with personal information via the Internet. This sample was taken from the general population and included Internet users and non-users. In that same survey, only 45% of Internet users considered it safe. This suggests that the majority of the general population, and the majority of Internet users, may be reluctant to use e-government services that require them to provide personal information online.
- An online survey on spam held in the US and EU in late 2003⁶ found that 52% of respondents said that they had cut back on online shopping or stopped it altogether because they were worried about it leading to more unsolicited email. (All respondents were Internet users, as this was an online survey.)

If problems on the Internet affect people's willingness to use e-government, this may undermine the investments the government is making to put services online, as well the usefulness of the Internet itself.

In the first half of 2004 the E-government Unit commissioned a study on the use of e-government in New Zealand.⁷ This study consisted mainly of focus group interviews. In some of these groups, questions were asked to elicit the extent of trust or distrust of the use of the Internet to deliver government services and information. The findings were that people were largely able to distinguish between the activities of criminals and vandals on the Internet and government actions. The .govt.nz domain was seen as authoritative. Interviewees' trust or otherwise in government online derived from their view of government in general; they trusted government to solve any security issues associated with doing government business online. (This was a qualitative study done with a very small sample.)

In mid 2004, the E-government Unit commissioned a telephone survey⁸ on public attitudes to various aspects of e-government. Some of the questions were designed to explore the link between security and trust. Particular findings were:

- 62% of home computer owners had their machines hit by a virus, and of these 26% (i.e. 16% of computer owners) were less likely to use the Internet as a consequence
- 53% said that they had received spam, and of these 22% (i.e. 12% of those questioned) said that they were less likely to use email as a result of this.

⁵ GO2003, Taylor Nelson Sofres plc, December 2003, e.govt.nz/docs/go-survey-2003/

⁶ Trans Atlantic Consumer Dialogue, www.tacd.org. This survey is the basis of the ongoing OECD Workshop on Spam.

⁷ *Wired for Wellbeing: Citizens' Response to E-government*, Rowena Cullen and Peter Hemon, Victoria University of Wellington, June 2004

⁸ *E-government: Telephone Survey of 5,000 New Zealanders*, Cate Curtis, Jack Vowles and Bruce Curtis, University of Auckland, August 2004

2.2 Law enforcement

Many of the problems affecting people on the Internet result from criminal behaviour, which government addresses through its law enforcement function.

The New Zealand Police has a unit called the E-Crime Lab which investigates and prosecutes criminal activity involving the Internet. The unit prosecutes those committing offences such as cracking (attacking computers directly over the Internet) and phishing (a form of fraud involving deceptive emails in an attempt to obtain valuable personal information such as bank account passwords). International cooperation is highly necessary for these prosecutions.

The E-Crime Lab also works with other New Zealand parties to improve computer security. It works with the Centre for Critical Infrastructure Protection⁹ (the CCIP) which aims to improve the security of New Zealand's critical infrastructure and key government departments from information-borne threats such as cracking, viruses and spam. The E-Crime Lab deals directly with banks over the security of online banking, where criminal activity is indicated.

The New Zealand Police and the Ministry of Education jointly sponsor NetSafe¹⁰, a programme of the Internet Safety Group. NetSafe educates Internet users about risks and strategies for safety on the Internet. It provides material through several channels including schools.

2.3 'Public health' on the Internet

An attacker may take advantage of a user's insecure machine to attack others, often without that user's knowledge. Therefore, individual users' computer security precautions can enhance the wider community of Internet users. This is a classic public policy issue similar to those in public health, where everyone is safer when all are vaccinated.¹¹

On the Internet, this is a global problem. Networks of compromised home computers overseas send spam to us, and New Zealand machines are used to send spam to users in other countries.¹²

⁹ The CCIP is a unit of the Government Communications Security Bureau or GCSB. It has a web presence at www.ccip.govt.nz.

¹⁰ www.netsafe.org.nz

¹¹ This argument is advanced by security expert Bruce Schneier at www.schneier.com/crypto-gram-0406.html#4

¹² *Trojan Horse behind German hate-mail spam flood* Computerworld New Zealand, 14 June 2004, idg.net.nz/news.nsf/UNID/D9346AA045E52DCFCC256EB2001EF883

3 Problems on the Internet

This section discusses problems on the Internet – that is, problems which affect people who use the Internet. Examples are a deluge of unwanted spam emails, viruses taking over people's computers and well-disguised attempts to defraud people of the contents of their bank accounts, insurance policies and life savings.

The Internet itself works extremely well. The problems discussed here are problems of human behaviour. These problems – a better term is 'attacks' - are generated by people who, for a variety of reasons, want to pursue their own agendas on the Internet at a cost to others.

3.1 Attackers

In the Internet's early days, those who abused it were seen by many as harmless explorers, or even as romantic heroes who were pushing back the boundaries of technical knowledge. If it was ever true, that scenario is now out of date. Today, viruses are designed to compromise machines so they can be used to send spam or attack web sites; networks of compromised machines are sold or rented.

People attack others over the Internet for a variety of reasons, including social status among their peers, for entertainment, for petty theft, for ideology, or to prove to themselves that they are capable¹³. They apparently believe that this is acceptable behaviour, or at least that they will not get caught because of the difficulties of tracing people across the Internet and the problems of transnational jurisdiction. New Zealand-based research¹⁴ shows that communications across the Internet are subject to a form of disinhibition in which participants behave quite differently online compared with how they would behave in the real world.¹⁵

With the increasing use of the Internet for business, Internet attacks have also become a tool of organised crime gangs for extortion and fraud. This is now a very serious problem world wide.¹⁶ According to the National High Tech Crime Unit in the UK¹⁷, these gangs have built on their traditional activities of prostitution, drug sales and extortion, to use the Internet to do similar things online. They operate from countries where organised crime is common, and see Internet crime as low risk, high reward. In July 2004, three men were arrested in Russia in connection with these attacks.¹⁸

The Internet has brought great benefits to people over most of the globe. Unfortunately, it has also enabled criminal behaviour at a distance, across international boundaries. It lets the unscrupulous exploit others whom they never meet and with whom they have little in common. It amplifies the scope of traditional criminal behaviour by giving criminals wider access to victims and little chance of prosecution. Because the Internet crosses jurisdictions it is harder for each government to protect its citizens.

¹³ *Know Your Enemy* (Honeynet Project 2004), by Max Kilger et al. Esp. chap. 16. Online at honeynet.org/book/Chp16.pdf

¹⁴ *Disinhibition on the Internet: Implications and Intervention*, by Quentin Atkinson, University of Auckland, online at www.netsafe.org.nz/resources/resources_disinhibition.asp

¹⁵ For a tragic example see the story of Brandon Veda at en.wikipedia.org/wiki/Brandon_Veda

¹⁶ For example: *Bookies suffer online onslaught*, BBC News 19 March 2004, news.bbc.co.uk/1/hi/technology/3549883.stm

¹⁷ Presentation at AusCERT2004 by Detective Superintendent Mick Deats, Deputy Head of NHTCU

¹⁸ *Bookies extortion gang caught*, BBC News 21 July 2004, news.bbc.co.uk/1/hi/business/3914363.stm

3.2 How Internet attacks work

This section outlines the reasons for threats on the Internet and explores the extent to which they are inherent to its design.

3.2.1 History of the Internet

The Internet began with a technical research project funded in the 1970s by the US government. Through the 1980s, the engineering work which underpins it was done. The quality of this work drove the initial expansion, and the network effect (as people began to realise how useful the Internet could be) drove it through the late 1990s.

Through the mid-1990s the Internet began to get press and government attention. Much of the press coverage warned of the use of the Internet to spread pornography while ignoring other more beneficial uses. Governments realized that the web gave them an opportunity to get closer to their citizens by publishing information directly and at very low cost. By the late 1990s the Internet had become part of the mainstream, with companies increasingly using the web not just for publishing but to host all or part of their business.

The Internet is a co-operative. Anyone can join by paying only their own expenses. This fact has led to people being able to experiment and develop services which run across it. Email and the web are both examples of things developed to run over the Internet by people who thought they would be a good idea.

The Internet's open architecture is both its main strength and its undoing. Its lack of built in security and service quality control has prevented it from being captured by providers and governments; however this lack also makes policing the Internet difficult.

The success of the Internet is primarily a social phenomenon. It contains some superb and unique engineering which, as a matter of policy, was made available for all to copy and mass produce without charge. The Internet's expansion has been due at least as much to the policies that surround it as to its technical brilliance.

The engineering of the Internet has handled its dramatic expansion remarkably well. An area it has perhaps not dealt with as well is the introduction of a wider spectrum of users with different agendas. The mainly technical people who used the Internet during its original building phase evolved a consensus on what behaviour was appropriate. Known as 'netiquette', this was a set of guidelines designed to help people not to waste others' time or the resources of the Internet. As the Internet expanded out of computer science laboratories the mix of people using it changed. Some new users started to exploit the commercial possibilities of the Internet, others used what they saw as their right to say or do whatever they saw to be in their own interests.¹⁹

Attacks on the Internet, and on people via the Internet, usually exploit either technical weaknesses in software or human fallibility. Some attacks exploit both. These are discussed in more detail below.

3.2.2 Security weaknesses in software

Security weaknesses are continually being found in widely used software. These are sometimes published, often but not always, after the software author concerned has had time to

¹⁹ See, for instance: en.wikipedia.org/wiki/Canter_&_Siegel

fix the problem and issue a patch. Once a patch is available, all affected machines need to be patched. This may be challenging for technically naïve users even they if understand the need. In some cases, patches are issued so frequently that proving them and installing them on production systems can occupy a great deal of expensive technician time, as well as causing unacceptable levels of downtime.

Weaknesses do not spring into existence when their discovery is published. They are inherent in software from its release. Unscrupulous individuals finding weaknesses can exploit them without the software author even understanding what is going on.

Why are there so many weaknesses in software? There are many reasons. One is that modern software, particularly operating systems (where most exploitable weaknesses are found) are very large and complex,²⁰ and contain many parts which can interact in myriad ways. Another concern is that new software features are more attractive to customers than is security, which causes software authors to provide software where security is traded off against perceived usefulness. Finally, commercial imperatives drive software companies to release revised versions of products to a schedule, knowing that they can issue patches later.

The result of these problems is that a lot of the machines connected to the Internet, perhaps most of them, have software with known and unknown security weaknesses. These weak systems expose not only their owners but others on the Internet because, once compromised, they can be used to break into other machines. This effect is exploited by viruses and worms, which typically use a particular weakness to penetrate a machine which they then cause to scan for similar machines so they can pass on the infection.

A 2002 paper²¹ raised concerns about so-called ‘flash worms’ that could potentially spread across the entire Internet in minutes using clever scanning techniques. This was followed by the Slammer Worm which spread across the Internet in ten minutes and caused considerable disruption, including shutting down ATMs, airlines reservation and credit card processing systems. It did this without a destructive payload, simply by the enormous amounts of traffic it generated while scanning for new systems to infect²².

Internet users and customers of businesses using the Internet were harmed by Slammer whether or not they had machines which the worm compromised. This is an example of the network effect (which is more usually seen as a way of magnifying the benefits of the Internet).

3.2.3 Human factors

Another way to defeat computer security is to get a person to do it for you. Most email worms travel this way. The trick usually employed is to get users to run an attached file, which in most email programs just means clicking on the attachment. The ILoveYou virus tried various techniques to get people to run it, including inviting them to click an email attachment to see “who loves them”.

Typically the virus or worm will email copies of itself to everyone in the users’ address book. These people now receive the email which appears to be from someone they know, the owner of the compromised system. As with software weaknesses, once the user has been persuaded to subvert system security the potential harm to the system is virtually unlimited.

²⁰ Microsoft Windows XP is estimated to contain 40 million lines of source code. Linux distributions contain a comparable number. For a discussion of this and its relationship to security see en.wikipedia.org/wiki/Source_lines_of_code.

²¹ Staniford, Paxson and Weaver: *How to Own the Internet in Your Spare Time*, www.icir.org/vern/papers/cdc-usenix-sec02/

²² Moore et al, *The Spread of the Sapphire/Slammer Worm*, www.caida.org/outreach/papers/2003/sapphire/

Attacks such as this rely on making the email sufficiently interesting or persuasive to get the user to run the attachment. Other attacks over the Internet (or via other media, but this is outside the scope of this discussion) can also exploit human factors. Most Internet fraud, for instance, works by persuading people to do something which is ultimately against their interest. Simpler techniques such as telephoning and pretending to be 'from IT' and requesting passwords also have a high success rate. The generic term for these techniques is *social engineering*, reflecting the notion that people are being manipulated like machines.

4 Analysis

4.1 Framework for analysis

This paper uses the following framework²³ for considering security threats:

1. Identify the assets that we wish to protect.
2. Identify and assess threats to these assets. This will cover direct and indirect impact (i.e. through public confidence) with likelihoods.
3. Assess the extent to which each proposed security measure protects against the threats.
4. Identify any other risks caused by each measure.
5. Identify costs and trade-offs.

4.2 Assets

An “asset” in this context is something we wish to protect against a security threat. While we are not concerned here solely with ‘assets’ in the physical sense, the framework is valid when we consider the aspects of the Internet and its role in society which are necessary for its use in e-government. For e-government, four “assets” are considered in the analysis below:

1. **Internet infrastructure:** the Internet’s existence, its wide use, its robustness and openness, and its low costs are all necessary prerequisites for people to use it to communicate with government. Increasingly the Internet is becoming a critical part of the national infrastructure.

While the Internet itself is undoubtedly the most important “asset”, because e-government is inconceivable without it, protecting the Internet structure gets a lot of attention from people whose businesses rely on selling access to it. This includes ISPs providing a level of support for customers whose machines are so damaged or affected by hostile programs that they are unusable.

However, there are large numbers of home machines with broadband connections²⁴ which have been compromised but which are not the subject of complaints by their owners and are presumably still usable. While ISPs are often aware of these compromised customer machines because of the traffic they generate, some take no action because of the cost and implications for their customer relationship. This is a serious issue, because of the risk of coordinated attacks using a network of such computers, and because of the potential breach of confidentiality in transactions made with government using a computer that has been compromised.

2. **Public confidence:** for the Internet to remain useful people need to remain confident in its availability, and not be reluctant to use it for business purposes. This confidence could be damaged by the various public attacks on the infrastructure, by scams running over it, and by spam.

What is a reasonable level of public trust in the Internet? The problems on the Internet are real and should not be made light of. The challenge for e-government is to engender a level of trust that will make e-government possible without exposing people or the government to undue risk. This is particularly difficult in a rapidly developing technical environment.

²³ This framework is described by Bruce Schneier in *Secrets and Lies*, Wiley, 2000. It is consistent with AS/NZS 4360.

²⁴ i.e. DSL or cable modem. These machines are connected to the Internet by high-capacity links (relative to dial-up) and, more importantly, are often left continuously running and connected.

3. **Agency confidence:** Government agencies are increasingly investing ways to deliver services online. Threats to Internet security perceived by agencies could undermine such future investment by agencies, and as a result disrupt the e-government programme.
4. **Information:** the Internet is a mechanism for transporting information. The government has many obligations about information. It needs to protect information which should be kept private, preserve information which must be archived, and make available information which should be published.

Seeing information as an “asset” here reflects the need to protect the confidentiality of information and people’s privacy, the need for people to be confident that they can continue to access their own information, and the need for confidence in the integrity of information and messages.

4.3 Threats

An earlier phase of this project identified a list of threats on the Internet. A detailed list and discussion of these threats is included as Appendix 1. The threats, and the assets which they threaten, are set out in the table below.²⁵

<i>Threat Type</i>	<i>Impact on:</i>	Infrastructure	Public Confidence	Agency Confidence	Information
1. Viruses/Worms		X	X	X	X
2. Spam		X	X	X	
3. Identity Theft			X	X	
4. Inadequate Government IT Security		X	X	X	X
5. Phishing			X	X	X
6. Copyright lawsuits			X		X
7. Digital Rights Management etc			X	X	X
8. Cracking		X	X	X	X
9. Spyware			X	X	X
10. De-centralised Internet Governance			X		
11. Pornography / Child Abuse			X	X	
12. Fraud and scams			X	X	
13. Fear of surveillance			X		X
14. Availability of ‘Dangerous’ Information		X	X	X	X
15. Insulting Behaviour and Defamation			X		X
16. Denial of Service Attacks		X	X	X	X
17. Trojans		X	X	X	X

4.4 Possible actions

A variety of potential government actions is set out below. These have been taken from the following sources:

- During consultation, some of these items were recommended to us.
- Some of these measures are being taken by other governments.

²⁵ There is no obvious way to classify these threats. These are aimed to be comprehensive, while recognising that some of the different threats listed overlap or magnify each other.

- Some were based on our assessment of the situation in New Zealand and the opportunities for the government here.
- Some are recognised good practice.

Some of these measures are being undertaken already, others are not. They have been grouped into education; policy; enforcement. For each potential action the benefit, costs and tradeoffs are listed.

4.4.1 Policy actions

A. A centralised Internet gateway for Government Agencies

<i>Protects against:</i>	Viruses, Spam, Inadequate government security
<i>Rationale</i>	Government can afford to properly resource a common gateway far better than can individual agencies. By improving security for the agencies least able to do it for themselves, government will improve its overall security.
<i>How effective?</i>	Highly effective if adequately resourced and operated
<i>What are its risks?</i>	It presents a central point of compromise (although this can be mitigated by maintaining existing agency gateways as well)
<i>Costs and tradeoffs</i>	Significant costs to set up and resource gateway. This could be partly offset by consolidating costs of hosting websites and Internet bandwidth. It could also reduce agency flexibility in using new technologies – this could be reduced by agency-controlled governance.
<i>Comment</i>	This would particularly assist small and mid-sized agencies which cannot otherwise afford the level of security able to be offered by a well resourced gateway.
<i>Conclusion</i>	This should be scoped, including an outline cost, design and policies.
<i>Recommendation</i>	Government should consider a central Internet gateway to provide a single Internet point of access for government agencies, especially small and medium agencies.

B. Encourage ISPs to Intervene where Customer Computers are Compromised

<i>Protects against:</i>	Viruses, Spam, Denial of Service
<i>Rationale</i>	ISPs with broadband consumer networks are often aware that their customers' machines have been exploited for nefarious purposes such as sending spam but typically do not act on this information because of the effort required to convince, educate and support the customer. Outgoing attacks are less of a concern to an ISP than incoming ones, however they are easier to suppress, e.g. by simply cutting off the

affected customer until they have been contacted.

<i>How effective?</i>	Helping customers clear up compromised machines, or at least cutting them off until they do, will reduce the number of machines available to relay spam, forward viruses, host phishing websites or run denial of service attacks.
<i>What are its risks?</i>	Some ISPs may not regard this as core business and may see an approach by government to ask them to intervene as interference. They might also find it hard to determine whether or not a compromised machine had been successfully cleaned.
<i>Costs and tradeoffs</i>	Some costs will fall on ISPs as they deal with customers who may not be aware of the situation and don't want to have to clear it up.
<i>Comment</i>	If pursued globally this would greatly reduce harm on the Internet. This is a case of thinking globally and acting locally.
<i>Conclusion</i>	This action has the potential to be highly useful in mitigating problems if it is employed world wide. Government should approach InternetNZ and two main telcos who own almost all the broadband connections. There may need to be regulation or legislation.
<i>Recommendation</i>	Consider how best to encourage ISPs to take measures to watch for and manage compromised home broadband customers

C. Anti-Spam Legislation

<i>Protects against:</i>	Spam
<i>Rationale</i>	Legislation is a necessary part of a government attempt to tackle the problem of spam. Law defines the bounds of acceptable behaviour; it also would enable the necessary international cooperation.
<i>How effective?</i>	Not very effective of itself but needed before anything will work. To be effective it will need enforcement and international cooperation. Many other jurisdictions are passing similar laws.
<i>What are its risks?</i>	If exceptions are allowed e.g. for charities or political parties, this will risk legitimising messages which people find annoying and intrusive.
<i>Costs and tradeoffs</i>	There will need to be an enforcement budget or the law will be irrelevant. If the law is watered down during passage, as occurred for similar legislation in the US, it may do more harm than good. However, the stance of the New Zealand Direct Marketing Association (unlike their US counterparts) is that spam is unacceptable so the pressure on the bill will be less.
<i>Conclusion</i>	MED has begun the process of getting legislation in place. It is important to ensure that the legislation does not contain exceptions

and has a funded enforcer.

Recommendation Government should introduce anti-spam legislation

D. Show Leadership in Authentication by providing secure log ons

Protects against Identity theft, Inadequate government security

How effective? Highly effective

Rationale People are used to the relatively undemanding userid and password to sign on, even for such things as banking. This is inadequate in the face of the threats currently on the Internet.

What are its risks? May lead to lower uptake of government services online due to the more onerous security procedures necessary (e.g. using a one time password, using a smart card or receiving a text message containing an access code.)

Costs and tradeoffs In the 2004 budget Government made provision for an all-of-government authentication system.

A more robust authentication system will make accessing government online services less straightforward. When and if the banks tighten their authentication for online banking this will seem more natural.

Conclusion The authentication project in EGU should develop an authentication technique for high value government to citizen and government to business transactions which is not susceptible to attack by spyware or Trojan.

Recommendation Government should show leadership in securing online transactions by providing an authentication system which is more resistant to common threats.

E. Encourage Banks etc to Strengthen Authentication

Protects against: Identity theft

Rationale Userids and passwords are vulnerable to capture by the spyware which is now widespread. Banks overseas are moving to two-factor authentication or one time passwords, however New Zealand banks are mainly still using only userids and passwords.

How effective? Highly effective – reduces the likelihood of account compromise.

What are its risks? Risks that banks ignore pressure and that compromises increase leading to confidence collapse about Internet business in general.

Costs and tradeoffs Costs would fall on banks and account holders. Costs need not be high; similar systems are in wide use by overseas banks. To a large

extent this can automated.

<i>Comment</i>	More robust security for Internet transactions in general will improve confidence in the Internet and in undertaking online transactions.
<i>Conclusion</i>	The police are already pressing banks to do this. The EGU Authentication project needs to work with the Police and banks to look at the extent to which a common system or policies should be implemented.
<i>Recommendation</i>	The authentication project should work with the police and banks to see how common authentication policies can be made.

F. Law to Clarify Software Licenses and to Expose Spyware and Trojans

<i>Protects against:</i>	Trojans, spyware, and the unexpected effects of digital rights management.
<i>Rationale</i>	<p>Users are required to assent to EULAs (end user licence agreements) when installing software. These are seldom comprehensible by the average user and generally rest on foreign legal systems.</p> <p>Software sometimes sends information about its user covertly across the Internet for marketing or other purposes. Users need to understand what the software will do with their information and be given a more reasoned opportunity to accept or reject it.</p> <p>Existing law may cover software which has covert effects, however this is not clear and is difficult for end-users to invoke. There is sector-specific consumer legislation in other sectors (eg motor vehicles) and some might prove beneficial in the software sector.</p> <p>Spyware bills are before the House of Representatives in the US and other jurisdictions are also reportedly considering legislation.</p>
<i>How effective?</i>	Will only become effective as other jurisdictions pass such laws.
<i>What are its risks?</i>	Could reduce the volume of software available here if New Zealand requirements are seen to be different to everyone else's.
<i>Costs and tradeoffs</i>	Will require some focus by government on how to frame such legislation or code.
<i>Comment</i>	<p>Existing law may cover software which has covert effects, however this is not clear and is difficult for end-users to invoke. There is sector-specific consumer legislation in other sectors (eg motor vehicles) and some might prove beneficial in the software sector.</p> <p>Spyware bills are before the House of Representatives in the US and other jurisdictions are also reportedly considering legislation.</p>
<i>Conclusion</i>	Government should consider whether there is a need for anti-spyware bill and any other software specific consumer legislation.

Recommendation Consider law change to outlaw covert sending of information by programs and clarify EULAs (End-User Licence Agreements).

G. Government to manage agency policies on digital rights management centrally

Protects against: Unexpected results of digital rights management – e.g. government being locked out of its own information.

Rationale DRM has attractive features but its use has significant downsides which can affect government as a whole – these need to be considered before agencies use it.

How effective? Medium

What are its risks? May miss some genuine utility of DRM system

Costs and tradeoffs Costs are low

Comment EGU is investigating the impact of commercial DRM systems and is advising agencies on their (non-) implementation. It is also canvassing other governments to build a coalition to deal with software vendors on the issue.

Conclusion It is important that government act as a whole in this regard.

Recommendation Government should manage agency policies on DRM use centrally

H. Government to clarify copyright legislation

Protects against: Copyright lawsuits, Unexpected results of digital rights management.

Rationale Current copyright law does not include ‘fair use’ provision permitting format changing. Use of iPods and similar may be therefore unlawful. Potentially people could be sued for using these devices. Removing this legal grey area will make it easier to assert what is and is not lawful use.

How effective? Medium

What are its risks? May provide opportunity for even more restrictive copyright

Costs and tradeoffs Will create a lot of comment in both directions

Comment MED is currently consulting on changes to copyright along these lines.

Conclusion MED appears to have this under control.

I. Government to participate in Internet governance

<i>Protects against:</i>	De-centralised Internet governance.
<i>Rationale</i>	Government currently has very little formal participation in Internet governance despite opportunities to do so. It risks decisions being taken which damage its ability to use the Internet for government business.
<i>How effective?</i>	Medium
<i>What are its risks?</i>	Main risk is government being blamed when there is an undesirable outcome. However, this is likely if government continues hands off strategy also.
<i>Costs and tradeoffs</i>	Some cost in resourcing and attending meetings with both bodies.
<i>Comment</i>	This is becoming more and important as government comes to rely on the Internet as the dominant means of ready access to government.
<i>Conclusion</i>	Government should commit to participating in ICANN/GAC process where international decisions affecting Internet policy and operations get made. Government should also consider a more formal relationship with the local body, InternetNZ.
<i>Recommendation</i>	Government should be engaged formally with the ICANN process and with InternetNZ

J. Government to review its arrangements for cyber-security

<i>Protects against:</i>	All listed threats.
<i>Rationale</i>	This paper identifies a list of threats to trust and security on the Internet, which are being addressed in varying degrees and by different parts of government.
<i>How effective?</i>	Medium-high
<i>What are its risks?</i>	Causing a false sense of security by failing to deal with threats.
<i>Costs and tradeoffs</i>	Little cost to review. Possible downstream costs if more effort is required by agencies.
<i>Comment</i>	This is the first attempt by government to consider threats to the use of the Internet holistically.
<i>Conclusion</i>	There is a need to ensure that all threats are considered and dealt with by the most appropriate agencies, and for ongoing review of this.
<i>Recommendation</i>	Government should be engaged formally with the ICANN process and with InternetNZ

4.4.2 Enforcement actions

K. Investigate and Prosecute Malware and other Security Incidents

<i>Protects against:</i>	Cracking, viruses and worms, spyware, trojans, phishing
<i>Rationale</i>	New Zealand needs to be able to show that it is prepared to investigate and prosecute malefactors before other countries will cooperate.
<i>How effective?</i>	Medium
<i>What are its risks?</i>	Could use a lot of resources with little direct gain.
<i>Costs and tradeoffs</i>	Medium
<i>Comment</i>	Done to a limited extent by Police E-Crime – one prosecution only since legislation came into effect.
<i>Conclusion</i>	Encourage New Zealand Police to work to investigate such incidents and to prosecute offenders where possible.
<i>Recommendation</i>	EGU to continue to work with Police E-Crime Unit to encourage investigation and prosecution.

L. Enforcement action against New Zealand spammers

<i>Protects against:</i>	Spam
<i>Rationale</i>	Need for international cooperation to solve the problem of spam.
<i>How effective?</i>	Medium.
<i>What are its risks?</i>	Would be hugely popular. However, if prosecution failed (due to inadequate law or process) New Zealand would lose credibility.
<i>Costs and tradeoffs</i>	Medium. Will need investigative effort and international cooperation.
<i>Comment</i>	The responsibility for enforcement needs to be identified in the legislation, and budgeted for by the agency concerned.
<i>Conclusion</i>	Should be part of pending anti-spam legislation.
<i>Recommendation</i>	MED to ensure that anti-spam legislation contains an adequate budget and performance measures for enforcement.

M. Investigate and prosecute identity thieves and intermediaries in identity theft

<i>Protects against:</i>	Identity theft, phishing
<i>Rationale</i>	Establishes a deterrent to both the fraud and laundering the proceeds

<i>How effective?</i>	Medium
<i>What are its risks?</i>	May prosecute people who were not aware they were aiding fraud.
<i>Costs and tradeoffs</i>	Medium. Will need investigative effort and international cooperation.
<i>Comment</i>	The New Zealand Police is already doing this
<i>Conclusion</i>	There may be a role for more education and publicity so people are educated to protect themselves. See education recommendations.

N. Prosecute Crackers and Spyware Distributors

<i>Protects against:</i>	Cracking, spyware, trojans
<i>Rationale</i>	Deterrence, establishing the bounds of proper behaviour
<i>How effective?</i>	Medium
<i>What are its risks?</i>	Credibility loss if a prosecution fails.
<i>Costs and tradeoffs</i>	Medium. Needs investigative capability and international cooperation
<i>Comment</i>	New Zealand Police have prosecuted one cracker so far, case pending.
<i>Conclusion</i>	Trojans and spyware need to be seen in the same light and prosecuted.
<i>Recommendation</i>	EGU and MED to work together to establish where spyware fits into the New Zealand legal framework and recommend change if found necessary.

4.4.3 Education actions

O. Education for Internet users on security issues.

<i>Messages:</i>	<ul style="list-style-type: none"> • Importance of security software, firewalls, OS hardening • Never respond to or buy anything from spam • Protect passwords • Ignore phishing attempts • Copyright and risks of abusing it • Importance of parental supervision • The security issues in moving to broadband from dial-up • Risks around public Internet terminals • Risks around wireless connections • Awareness of social engineering • Where to get assistance in security maintenance such as spyware detection. • What the law in New Zealand is regarding electronic crime
<i>Rationale</i>	<ul style="list-style-type: none"> • Widespread protection will make it harder for viruses and spam to spread. It will also improve the experience for Internet users.

- Spam relies for its business model on getting some sort of response rate. If no-one bought anything, most of it would stop.
- People need to understand how important it is to maintain secrecy of their passwords.
- Education to ensure that people understand what it is legal to do with copyrighted works
- It is hard to be certain that cyber café machines are not compromised and sending user IDs and passwords out across the Internet.
- Some phishing scams are very convincing and telling them from the real thing is difficult even for experts.
- Educate children as well as adults, because they are often the administrator on their home computer.

<i>Protects against:</i>	Cracking, Spyware, Spam, Phishing, Identity theft, Fraud and scams, Dangerous information, Insulting behaviour, Fear of surveillance, Child abuse
<i>How effective?</i>	Variable. Will help some users save themselves problems. Might also reduce effectiveness and spread of viruses and spam.
<i>What are its risks?</i>	Could convince people the Internet as a whole is unsafe. Need some care and moderation in messages to explain risks, and must give clear advice.
<i>Costs and tradeoffs</i>	Medium
<i>Comment</i>	<p>The Internet Safety Group (ISG), partly funded by the Ministry of Education and the New Zealand Police, has made a start in this area. Its focus is on individuals and particularly on children and families.</p> <p>There is an equal need for education for businesses, particularly those which are too small to maintain in house IT expertise.</p>
<i>Conclusion</i>	Should look at the scope and reach of Internet Safety Group campaigns and consider extending them.
<i>Recommendation</i>	<p>Assess extent of support of ISG and other bodies and extent to which messages above are covered. Consider further funding if gaps are found.</p> <p>Consider a specific education campaign for small businesses to deliver the same messages.</p>

P. Education for agencies on Internet security issues.

<i>Messages:</i>	<ul style="list-style-type: none"> • Promote the Centre for Critical Infrastructure Protection – key government agencies are part of its target group • Promote incident reporting by government agencies to the CCIP • Promote Security in the Government Sector to agencies
------------------	--

- General IT security

<i>Protects against:</i>	Inadequate government IT security
<i>How effective?</i>	Low to medium. These messages have already been promoted and awareness is high.
<i>What are its risks?</i>	Burnout, boredom and complacency. Messages might be seen as spam.
<i>Costs and tradeoffs</i>	Costs are low.
<i>Comment</i>	Hard to see more effort being effective. Most agencies have received these messages repeatedly.
<i>Conclusion</i>	No further action

5 Conclusions

In his novel *The Hitchhiker's Guide to the Galaxy*, Douglas Adams suggested that an automatic translator which allowed you to instantly understand anything said to you in any form of language, would lead to more and bloodier wars than anything else in the history of creation.

The Internet enables communications between a wider range of individuals than any technology before it. This offers great benefits to people, businesses and governments. However, as the threats in this document show, it also exposes people to risks they do not understand.

The Internet's growth has been driven by people connecting because they see the benefits the Internet offers, and by firms and governments using the Internet to deliver services and information online. These benefits, and the growth of the Internet itself, have accrued because of:

- The network effect – the way in which the value of the network increases as more connect.
- The Internet's open architecture which allows anyone to offer innovative services.

The threats on the Internet are amplified by:

- The network effect which ensures access to large numbers of victims.
- Anonymity – it is relatively easy to conceal one's identity from most observers online.
- Open architecture which allows innovative threats as well as benefits.
- Software which is overly trusting, such as email programs which render HTML, or operating systems with inoperative firewalls.

Many strategies are suggested above to mitigate the various threats. They should be assessed against the extent to which they affect the factors driving threats, without damaging the factors causing the Internet's usefulness. This suggests that strategies aimed at dealing with two specific aspects of the Internet may work:

- The ability of the malefactors to hide.
- The installed base of trusting software.

5.1 Recommendations

Recommendation 1: Government should consider a central Internet gateway to provide a single Internet point of access for government agencies, especially small and medium agencies. All users of this gateway should be subject to an education programme and robust acceptable use policies.

Current status: EGU is bidding for GIF funding to create a Wellington network and a central Internet gateway.

Recommendation 2: Government should manage agency policies on Digital Rights Management (DRM) centrally.

Current status: EGU has advised agencies not to use DRM for the time being. EGU continues to investigate.

Recommendation 3: Government should introduce anti-spam legislation and allocate an adequate enforcement and education budget.

Current status: MED is working on legislation intended to be introduced during 2004.

Recommendation 4: Government should show leadership in securing online transactions by providing an authentication system which is resistant to current threats on the Internet.

Current status: EGU is working on a whole of government authentication programme which will take this into account.

Recommendation 5: Encourage banks to improve authentication.

Current status: The New Zealand Police has been encouraging banks to strengthen authentication procedures. To date one bank (ASB) has announced it will use text messaging to provide two-factor authentication.²⁶

Recommendation 6: Consider law change to clarify EULAs (End-User Licence Agreements) and make clear the effect of programs on user privacy.

Current status: None.

Recommendation 7: Encourage ISPs to take measures to watch for and manage compromised home broadband customers.

Current status: None. Seek comment from InternetNZ.

Recommendation 8: Participate in Internet governance at international and domestic level.

Current status: Patchy representation in the international field. While New Zealand has a representative on the Government Advisory Committee of ICANN, government does not normally fund this person to attend the meetings.

There are extensive informal contacts but little in the way of a direct formal relationship with the local body, InternetNZ.

Recommendation 9: Review government arrangements to protect the usefulness of and confidence in the Internet in New Zealand.

Current status: This report provides background.

Recommendation 10: Investigate New Zealand computer security incidents and provide a mechanism for anonymous reporting

Current status: Investigations are performed in some cases by the New Zealand Police when there is evidence of a crime.

Recommendation 11: Investigate and prosecute identity thieves and intermediaries.

²⁶ Two-factor identification relies on more than just an item to be memorised – it involves access to some other physical token or the use of a biometric. Practical examples for Internet use include the user keying a password sent by text message when they try to log on, and using a smart card and portable reader to generate a password valid only at the moment the user logs on.

Current status: New Zealand Police are doing this where there is evidence of criminal activity.

Recommendation 12: EGU, MED and the New Zealand Police to work together to establish where spyware fits into the New Zealand legal framework and recommend change if found necessary.

Current status: New Zealand Police have prosecuted at least one cracker since the enabling legislation was passed. There has been little publicity about it, however.

Recommendation 13: Assess extent of existing publicity and education for Internet users and consider whether more is needed. Key messages:

- The importance of security software, firewalls, OS hardening.
- Never respond to or buy anything from spam.
- Protect passwords.
- Ignore phishing attempts.
- Copyright and risks of abusing it.
- Importance of parental supervision.
- The security issues in moving to broadband from dial-up.
- Risks around public Internet terminals.
- Risks around wireless connections.
- Awareness of social engineering.
- Where to get assistance in security maintenance such as spyware detection.
- What the law in New Zealand is regarding electronic crime.

Current Status: The Ministry of Education supports the Internet Safety Group which does work in this area. CCIP has serving general New Zealand public as part of its mission. Publicity from vendors is sometimes self-serving.

Recommendation 14: Consider an ongoing programme of education for small and medium enterprises (SMEs) covering the same messages as recommendation 13.

Current Status: The Ministry of Economic Development is considering including such a programme as part of a revised Digital Strategy.

Appendix – Threat Assessment

This appendix contains material from the threat assessment issued and consulted on in March 2004. It comprises a list of threats to trust in government over the Internet, and for each threat an explanation and some example mitigation strategies. It is provided to further explain the threats referred to in the main paper.

Threats may be to the Internet infrastructure, or may affect Internet users and therefore public confidence. All of these threaten e-government. Threats listed may be amplified by adverse media coverage or by activism on the Internet.

It is hard to create a scheme to categorise threats. Because of the complex technical environment on the Internet, and the way in which some techniques exploit human frailties and technical weaknesses simultaneously, any classification is likely to have overlapping categories. The list below aims to be comprehensive rather than mutually exclusive.

1. Viruses/Worms
2. Spam
3. Identity Theft
4. Inadequate Government IT Security
5. Phishing
6. Copyright lawsuits
7. DRM etc
8. Cracking
9. Spyware
10. De-centralised Internet Governance
11. Pornography / Child Abuse
12. Fraud and scams
13. Fear of surveillance
14. Availability of 'Dangerous' Information
15. Insulting Behaviour and Defamation
16. Denial of Service Attacks
17. Trojans

Each of the threats in the table above are described below in more detail, together with example mitigation strategies. These should not be taken as actual proposals, rather as talking points.

Threat Type: Viruses / Worms	Threat To: Infrastructure
Potential Impact: Very High	Likelihood: Medium to High

Summary

There are frequent, serious attacks on the infrastructure of the Internet through the medium of self-replicating code. The potential impact of these is very high. Effects range from trashing individual users' files to abusing users' machines so as to damage Internet infrastructure. These attacks have also disabled non-Internet based systems such as ATM networks. The accompanying publicity potentially affects overall views of the Internet and its usefulness. Perpetrators are seldom traced.

Mechanism

In biology, a virus is an inert particle containing a piece of DNA - nature's way of representing information on how cells should function and reproduce - which tries to make as many copies of itself as possible by using the cells of a host organism. Computer viruses²⁷ are a close analogy to this. They comprise a program – a set of instructions to a computer – which tries to copy itself into any computers it encounters. A “successful” computer virus consumes large quantities of computer and Internet resources through unchecked replication, and human time in the efforts required to fight it. However, computer viruses sometimes also maliciously delete or publish computer files, or use commandeer computers for other noxious purposes such as sending spam or attacking third parties.

The threat from viruses is greater than that from hacking or cracking because of the way in which the undesirable program replicates itself automatically. While the effects of hacking may be more insidious, they are limited to what one or a few individuals can accomplish in a limited timeframe. The magnitude of the impact of a virus attack is in principle limited only by the number of machines available.

Cause

Viruses are written by individuals. Sometimes they create new viruses from scratch, sometimes modifying an existing one, or sometimes using a virus creation kit available from the Internet. The authors of many widespread viruses have never been identified. Those that have been caught have often been found only because they boasted about it. Typically they are young men who claim they wish to demonstrate security weaknesses, and who do not seem to accept responsibility for the impact of their demonstration. Many countries have now passed laws under which virus writers may be prosecuted. Prison sentences have been handed down for some who have been convicted under these laws.

Computer viruses gain entry to computers by exploiting weaknesses in software or by tricking humans into bypassing security. Exploiting software weaknesses is relatively easy. Security holes are continually being discovered in widely-installed software. Although responsible vendors issue fixes for these problems, there is always a delay between the discovery of a problem and the fix. Even when fixes are issued many users do not download and apply them.

²⁷ Worms and viruses differ in their mechanism of using their computer hosts. While viruses insert themselves into pre-existing harmless programs on the host computer, worms run independently of other programs. The biological analogy is with tapeworms. Worms and viruses have the same effects and are not distinguished in this analysis.

Tricking people into running attachments is also relatively easy. Some viruses such as “I Love You” entice recipients to find out more by clicking the attachment. Others claim to be from authority figures such as ISPs.

Example Mitigations

Improved patching of software
Software vendor product liability for security holes
More prosecution of malefactors
Email ‘stamps’
‘Walled gardens’ – i.e. filter everything unusual at ISPs
Anti-virus software
“Hardening” systems

Threat Type: Spam	Threat To: Public Confidence
Potential Impact: Medium	Likelihood: High

Summary

The volume of unwanted commercial email, known as spam, is now greater than that of other mail. Spam is drowning out legitimate mail and decreasing the usefulness of email in general. It also makes people less likely to shop online because they are reluctant to give out their email address.

The goods or services being offered in spam are often of dubious taste or legality. Much spam is offensive to many people, and causes particular concern when sent to minors.

Mechanism

Spammers use specialist software to send millions of e-mail messages at once. E-mail addresses are harvested from web sites and chat rooms, and potentially from product registrations at corporate websites. Addresses can also be deduced by the so-called dictionary attack in which a spammer’s server tries all likely names and common email conventions at a remote mail server seeking live addresses.

Sending spam requires special techniques. Spam is a violation of ISPs’ terms of service and spammers’ accounts are often terminated for this reason, but because of the volume of mail they represent an otherwise good customer for an ISP. Despite stated policies to the contrary there is evidence that certain large US ISPs act as gateways for spammers.

There are other ways to send large quantities of spam. In particular, spammers often use misconfigured mail systems belonging to unsuspecting third parties to copy a single message to a large mailing list. There is also concern that viruses which convert users’ PCs to spam servers may be written.

Spam emails almost invariably contain false “from” addresses, and other false header information designed to obscure their origins. It is difficult to trace much of it despite its volume.

There are free and commercial products to filter spam. These may take some effort to install and maintain, although this is increasingly being done by ISPs. Spammers respond by trying to create their messages so that they will not trigger filters. Spam filters and spammers are

engaging in a kind of arms race. This explains spammers' frequent use of odd punctuation and nonsense words in an attempt to evade filters while their messages remain readable by humans.

Various sites offer real-time facilities to help identify spam. They are designed for use by ISPs, and effectively answer the question: is this piece of mail coming from a site known to host spammers. Many ISPs use services like these to cut down the amount of spam their users receive. Recently, these sites have been the targets of denial of service attacks intended to hinder their operations.

Comment

For a long time, many companies and industry bodies resisted the classification of all unwanted commercial e-mail as spam. One person's spam, they argued, is another's marketing material. This attitude has changed over the last twelve months and most legitimate businesses now make very clear what use is intended of customer e-mail addresses, and allow opting out of communications.

An opt-out regime has problems. Critics point out that this would permit every business to email every individual at least once until asked to desist. Also, unscrupulous senders may use the opt out reply as evidence that the mail address is active and send yet more spam. For this reason, people are encouraged not to opt out. A preferred alternative is opt-in, in which people have to ask to receive communications. Some go further and insist on double opt-in, in which the user must reply positively to a test message, as is practised on many e-mail lists.

Spammers sometimes claim that all the addresses on their lists have opted in. This is unprovable at best, and highly unlikely.

Example Mitigations

- Educate people to never buy things from spam
- Keep improving filters
- Legislate in line with other governments
- More filtering at ISPs
- Encourage wider implementation of greylisting?
- Whitelisting and blacklisting

Threat Type: Identity Theft	Threat To: Information, Public Confidence
Potential Impact: High	Likelihood: Low

Summary

In the US, identity theft appears to be a fact of life. A survey by the Federal Trade Commission showed that almost 5% of Americans were victims of identity theft in the twelve months to April 2003. The Internet facilitates this theft by providing a way to find out a lot about people without them knowing, and by allowing the unscrupulous to pose online as people they are not.

Mechanism

In the US, citizens are used to providing their social security numbers to companies and government agencies as a condition of doing business. Social security numbers are used as a de facto identifier by government agencies and businesses. Lists of citizens' names, addresses and other identifying information are routinely made available on the web, e.g. by state driver

licensing authorities. There is a very high incidence of abuse of this information to access victims' funds, incriminate them, or cause other harm to their reputation or well-being.

According to a US survey run by Brightmail,²⁸ an email filtering company, identity theft takes an average of 600 hours of each victim's time to sort out. In the UK, the Home Office estimates that identity theft costs Britons £1.3 billion annually and is growing at 165% per annum. This is mostly plastic card related fraud and not specific to the Internet, but the Internet assists the process by making it easier to obtain the information necessary to steal someone's identity.

In New Zealand, by contrast, incidences of identity theft are rare, possibly because the Privacy Act has given people an expectation that they do not and should not provide unrelated information to companies. The same Act also obliges companies to protect personal information and not to abuse it. However, an experiment by a newspaper²⁹ showed that it was possible in New Zealand to get a driver's licence in another's name, even that of a celebrity. The LTSA has since revised its procedures.

Comment

Not currently a major issue in New Zealand, but one which should be monitored.

Threat Type: Inadequate Government Security Threat To: Public Confidence, Information

Potential Impact: Medium

Likelihood: Medium/Low

Summary

Poor safeguarding of personal information could damage the uptake of government services online. For example, on rare occasions personal records have been found at landfill sites, which has caused concern. If people are concerned about government security and about Internet security, they are doubly unlikely to use e-government services.

Mechanism

Poor government or commercial IT security can be exploited many ways. Hackers can compromise insecurely configured systems. In some cases, web servers can be set up so badly that they provide unintended information to anyone willing to experiment with web page addresses.

There have been many examples:

A US Federal Government department (the Department of the Interior) has now twice been directed by a court to take down its web presence because its porous IT security was exposing citizens' data on the Internet.

The UK Government was embarrassed when a document it released in Microsoft Word form was shown to contain a history of who had drafted it and when.

Government departments in several countries including New Zealand have had their web servers compromised from time to time and the home pages replaced.

²⁸ Now part of Symantec, www.symantec.com

²⁹ Taking Names, *ComputerWorld New Zealand*, 1 March 2004, www.pcworld.co.nz/PCWorld/PCW.nsf/UNID/44A39CF803B2E824CC256E450076526C

While website defacements are generally obvious, this does not have to be the case. Information on a US newspaper's website was altered by a hacker with the intention of improving the share price of a company.

Comment

The New Zealand Government is highly aware of risks in this regard. It already provides services to departments through the GCSB and CCIP and the security.govt.nz website. It also publishes *Security in the Government Sector*³⁰, a manual covering risk mitigation in this regard.

Threat Type: Phishing	Threat To: Public Confidence
Potential Impact: Medium	Likelihood: High

Summary

Phishing is persuading people to enter their bank account details or other information which can be used to steal from them or abuse them into a faked official website.

Mechanism

In the most common variation, people receive an email purporting to be from their bank, encouraging them to sign on to the bank's website to verify their status, or to confirm that their account has not been compromised, or some other security-related reason. A link to the webpage is provided in the email.

This link, while superficially similar to the bank's address, is based offshore and is operated by a third party. The webpage at its address may resemble the bank's website in detail, and its cunningly constructed URL can appear to be a bank URL.

Phishers have found a way to include an SSL certificate on their website, so that the user gets to see the padlock icon in the bottom of their browser.³¹ Until now banks have advised their clients that this padlock was an indicator of the correct website.

Scams such as this are generally noticed quickly and banks watch for suspicious overseas transfers. To defeat this, phishers generally recruit New Zealand bank account holders beforehand to pass money on in return for a commission. This activity is an offence under New Zealand money laundering laws, but there is little public awareness of this and no-one has been prosecuted so far.

Some of these emails can be very persuasive. In one scam circulating in the US, the recipient is informed that their account is the subject of possible abuse by terrorists. It appears to be from an office of the US Government and cites the Patriot Act, which is security legislation passed after the events of 11th September 2001. The mail requires the account holder to verify their identity by 'signing on' to the account using a bogus web link.³²

³⁰ On the world wide web at www.security.govt.nz

³¹ SSL's Credibility as Phishing Defense Is Tested, *Netcraft* 8 March 2004, news.netcraft.com/archives/2004/03/08/ssl_credibility_as_phishing_defense_is_tested.html

³² E-mail scam uses anti-terrorism hook, *CNN* 26 January 2004, edition.cnn.com/2004/TECH/internet/01/26/email.scam

Comment

This is a “social engineering” threat more than a technical one. It relies on persuading people to take an action which compromises their security. However, the action appears reasonable, and this disjuncture could cause loss of confidence in the Internet.

Example Mitigations

Using a ‘bank.nz’ domain name which would only be available to registered banks
More education / awareness
Online banking security improvements, recognising that this would make it harder to use online banking
Greater liability to fall on banks for abuse of online facilities
Prosecution of intermediaries
Direct action to spoil scams by seeding with incorrect information, then watching for logins.
Email filtering at ISPs.
International co-operation at a Law Enforcement level

Threat Type: Copyright Lawsuits	Threat To: Public Confidence
Potential Impact: Medium	Likelihood: High

Summary

Some people use the Internet to trade copyrighted works, particularly music, video and software. Copyright owners object to this and attempt to discourage the practice through highly public legal action against participants.

Mechanism

Because of legal threats by copyright holders, web sites do not usually permit the unlicensed distribution of copyrighted materials. Instead, most such distribution is done through peer to peer (P2P) applications such as KaZaA. These involve the user downloading some (usually free) software which makes contact with other users running the same software on the Internet. Users can then search each other’s collections and swap files.

The original P2P service, Napster, was aimed at sharing music and was restricted to exchanging MP3s (a form of digitised music). Napster became very popular before being shut down by a court order obtained by representatives of music copyright owners. However, file trading continued to increase through newer services which, unlike Napster, were designed to have no central operations hub and thus be more resistant to legal attack.

When suing the later P2P services proved difficult or impossible, the RIAA (a body representing the music industry) started to sue individual users who were sharing copyrighted music files on P2P services. As part of their strategy they made these suits highly public, including supporting an advertisement featuring some of the children they had sued which was shown during the 2004 Superbowl final.³³

Comment

Peer to peer applications are not of themselves illegal or reprehensible. They can be, and are, used for everything from hosting materials found politically unacceptable in some countries, to distributing new releases of free software without a central high bandwidth server.

³³ Pepsi ads wink at music downloading, *USA Today* 23 January 2004, www.usatoday.com/tech/news/2004-01-22-sb-pepsi_x.htm

The strategy of copyright owners of public prosecution and humiliation may cause people to view the Internet negatively, especially parents who are not sure what their children do on the Internet.

Some argue that, according to current New Zealand copyright law, many activities which are widely pursued are unlawful. For instance, using an MP3 player requires one to make a digital copy of a CD or other music source. (This is lawful in the US under the so-called ‘fair use’ provisions of copyright, but no similar provision exists in New Zealand law.) Copyright owners or their representatives could sue end users for this activity, even in cases where the CD had been legitimately purchased and the music on it was played only by the purchaser.

Example Mitigations

Public education and awareness about copyright
Tools for parental control
Walled Gardens

Threat Type: Digital Rights Management etc	Threat To: Public Confidence
Potential Impact: Medium	Likelihood: High

Summary

Digital rights management and similar technologies will prevent users from doing things they might consider reasonable (it would be unnecessary otherwise). If this is imposed without reference to users, or is abused by copyright owners or software vendors, a backlash may result.

Mechanism

Digital rights management and trusted computing are generic names for technologies which prevent the user from controlling certain aspects of their own computers. This done to enforce the protection of copyright. It carries a number of risks, such as the potential for users not to be able to access material they consider they own or have a right to. This could occur for several reasons including poorly implemented or old software, disputes with copyright owners, or an attempt to make unlicensed copies of copyrighted material.

As software is revised old data may become inaccessible. Files may be in old formats which are no longer supported. In some cases these formats are not publicly documented making extracting the text from them uncertain. Commercial pressures may lead software vendors to deliberately “orphan” formats in order to maintain an advantage in market share.

Comment

Thus far many fielded DRM systems have been cracked.³⁴ However, this is likely to get rarer and those systems which have not been cracked will come to dominate the market.

Example Mitigations

Public education
Government refusal to accept protected files in email

³⁴ For example: Apple Inc’s iTunes and the CSS system used to protect content on pre-recorded DVDs have both been cracked.

Threat Type: Cracking	Threat To: Public Confidence
Potential Impact: Medium	Likelihood: High

Summary

Cracking (also sometimes called “hacking”, although this term has other meanings) is gaining unauthorised access to computers. It causes considerable damage to the confidence of those who depend on the system in question.

Mechanism

Weaknesses are often discovered in software. Sometimes security weaknesses are published before the vendor fixes or “patches” them. In some cases these weaknesses are not published at all but are used by their discoverer or associates to penetrate security. These weaknesses may be exploited via the Internet, allowing an attacker to read or alter files, or to commandeer the computer for his or her own ends.

There are many documented cases of crackers using commandeered machines with high-bandwidth connections, sometimes in military installations, to store and serve collections of digitised music or unlicensed software. Compromised machines may be used to attack others machines by spraying them with large amounts of traffic, or to send spam. There are also cases of espionage being conducted via cracked machines.³⁵

Comment

Cracking is a very serious threat to machines which are not kept patched, and whose logs are not regularly checked for signs of unauthorised access. However the number of machines which a limited number of crackers can compromise is also limited; so this threat affects machines and the data on them more than the structure of the Internet. The incentives to protect machines against hacking fall on those who suffer if the machines are not protected.

Example Mitigations

- Walled Gardens
- Keep patching
- Active monitoring systems
- Design security into systems from start
- More effort to prosecute offenders

Threat Type: Spyware	Threat To: Public Confidence
Potential Impact: Medium	Likelihood: Medium

Summary

Spyware is software which covertly transmits a user’s personal information from his or her computer to some other destination on the Internet.

Mechanism

Spyware ranges from commercial software which requires an online registration, and which passes information about the machine it is installed on back to base; to completely covert “Trojan” programs installed via viruses or hacking attacks, and which monitor keystrokes or

³⁵ *Cuckoo’s Egg* by Clifford Stoll, Pocket Books.

passwords and send these out on the Internet. Other programs watch surfing patterns in order to target advertising to the user.

While commercial software providers might object to their products being labelled spyware the fact remains that many such programs require or encourage an online registration during which various information is transmitted across the Internet. It is not in general clear to the user what information he or she is sharing with the program owner.

Some free software and shareware also contains spyware. An example is the popular KaZaA file-sharing program, which as well as sharing files also shares computer resources such as network capacity, CPU cycles and disk space for undescribed purposes under the control of the program owner. This could come as a particular surprise, say, to a parent who was unaware of the existence of KaZaA on their machine.

There is a risk to public perception of the Internet through spyware, as well as the obvious one of the risk to the privacy of information. Spyware can be used to facilitate identity theft.

Comment

There may be an analogy to the development of attitudes on spam. Until recently, many companies maintained that direct email marketing was a completely legitimate tool which they intended to exploit. With the rising volumes of this, and the increasingly extreme and fraudulent messages being sent through spam, most reputable companies have now rejected unsolicited email as a tool.

Spyware has yet, perhaps, to annoy as many people as spam currently does, although there are signs that it is becoming nearly as prevalent.³⁶ If it succeeds, companies which use intrusive software registration and monitoring schemes may change their own view on the desirability of these arrangements, fearing guilt by association. The New Zealand Privacy Commissioner recently signed an international declaration³⁷ that software should not transmit any personal information across the Internet without permission.

Example Mitigations

Anti-spyware tools exist which can help identify and remove spyware. (Currently anti-virus tools do not consider spy ware viruses and so do not do this, but may do so eventually.)

Legislation?

PC Maintenance

Privacy Act already makes this unlawful

Threat Type: De-centralised Internet Governance Threat To: Public Confidence

Potential Impact: Medium / High

Likelihood: Medium / Low

Summary

Various bodies and companies assert control over parts of the Internet and try to exercise it through technical and political means. This threatens the Internet's stability and usability.

³⁶ See, for instance, www.webpronews.com/news/ebusinessnews/wpn-45-20041015DellsSpywareSurvey.html

³⁷ Resolution on Automatic Software Updates, 25th International Conference of Data Protection and Privacy Commissioners, Sydney 2003. www.privacy.gov.au/news/ressof_print.html

Mechanism

No-one owns the Internet. It was designed to have no central point of failure – data is routed automatically through the network via any available path. As originally designed, the Internet lacked any central service or facility whose failure would cripple its operation. All machines on the Internet ‘knew’ the address of every other machine, by means of a shared file which was updated every night. The Internet operated like this through the late 1970s and early 1980s until the Domain Name System (DNS) was created.

The DNS is the facility which converts names such as `www.govt.nz` into addresses of actual machines. It replaced the shared file of machine names. The DNS uses a database of names which is distributed across the world. It relies on “root servers” which are centrally operated, although they are geographically diverse.

The policy and the operations of the DNS have often been the subject of controversy. Internationally, ‘.com’ names are registered by a private company, Verisign, under contract to a non-profit body called ICANN. Verisign unilaterally changed the way in which the DNS operates in a manner which provided Verisign with opportunities for further revenue, but which caused problems for other services on the Internet. After direction from ICANN, Verisign withdrew this change, but threatens to reimplement it and has sued ICANN over the issue. The outcome is a lack of certainty about the way in which a key part of the Internet operates, which makes building on it harder.

Some people question the legitimacy of ICANN itself. It was created in 1998 by the US government, and is supposed to be open and transparent, and to reach decisions in a consensus manner. ICANN has always been the subject of claims that it was unrepresentative and unresponsive.

New Zealand has had its share of controversy over domain names. The operator of the ‘.nz’ domain name space, InternetNZ, has had stormy meetings and negative publicity over the operation of the DNS, although the situation now appears to have been resolved.

Some countries such as China recognise the importance of the Internet to economic growth but seek to control their citizens’ access to information on it. Typically such countries use technical means to try to filter information entering and leaving the country via the Internet, with limited success.

Comment

The largest concern is that the DNS becomes unstable as result of interference by some of these parties for political or commercial reasons.

Example Mitigations

Play a part in the political processes around ICANN and enforce accountability.
Monitor New Zealand Internet DNS operations and policies.

Threat Type: Pornography / Child Abuse Threat To: Public Confidence

Potential Impact: Low

Likelihood: Medium/High

Note: this risk refers to the damage to mainstream Internet use caused by publicity about prosecutions for illegal and unsavoury activities; not about the activities themselves.

Summary

Publicity on Internet safety and child pornography arrests may damage confidence in the use of the Internet for other purposes.

Mechanism

The Internet is not safe for unsupervised children due to the activities of stalkers and potential child molesters. It is also used to trade child pornography. Both of these unacceptable uses are countered, in part, by publicity. Internet safety is promoted, rightly, to reduce the chances of children falling prey to stalkers or other undesirables. Those trading child pornography are punished publicly in order to deter others. The result is that publicity about the Internet often seems to focus on its negatives uses.

Comment

This is less of an issue than it used to be. Since the Internet has become mainstream, people are aware of its benefits and reporting does not concentrate so much on its sensational aspects.

Example Mitigations

Education on risks.

Support “Safety” groups.

Prosecutions.

Threat Type: Fraud and scams	Threat To: Public Confidence
Potential Impact: Medium	Likelihood: High

Summary

Through the Internet, people can be exposed to a wide variety of others, some of whom are fraudsters. These people can also use the Internet to obscure their real identities.

Mechanism

The main differences between Internet based scams and frauds and other kinds are the numbers of people who can be reached and the international dimension. In principle, the Internet allows every would-be fraudster across the globe to contact every potential victim. In practice, the limitations of language and the difficulties spamming everyone reduce the number of opportunities somewhat, but the number of attempts to defraud are still vastly greater than they could be without the Internet.

The Internet allows fraud to be conducted across borders, which makes it hard both to trace and prosecute offenders. It also makes restitution unlikely.

According to Brightmail³⁸, 8% of all Internet email is unsolicited promotion of fraud of one kind or another. Often they involve seducing the recipient into doing something illegal, or at least unethical, for a promised reward. When the fraud is realised the victim is less likely to complain because this exposes their own cupidity. The ubiquitous “Nigerian” scam is an example. Phishing is a form of Internet based fraud.

³⁸ www.brightmail.com, a mail filtering company which also generates statistics on the spam it filters. The figure quoted here is calculated from their January 2004 report that spam was 60% of all email, and frauds 13% of all spam. Brightmail has since been acquired by Symantec.

Comment

Along with the problems of spam in general, this could badly affect the usefulness of email as a medium for business and government.

Example Mitigations

Education (“if it looks too good to be true, it probably is”)

Prosecution / cooperation with overseas forces

Threat Type: Fear of surveillance	Threat To: Public Confidence
Potential Impact: Medium	Likelihood: Medium

Mechanism

Information flowing across the Internet is in most cases visible to anyone with the necessary technical skills and access, including technical staff at ISPs and telcos through which traffic passes. The technology to encrypt (i.e. using codes to conceal) communications on the Internet is reasonably well developed. High-quality email encryption has been freely available for many years. However it is not often used, to the extent that encrypted email would “stand out” to anyone observing traffic flows on the Internet.

Most web traffic is not encrypted, although some websites which handle banking and e-commerce use a more secure way of communicating with users which codes the information passing to and fro.³⁹

Encryption as used on the Internet only protects information while it is in transit. Information could be stolen or copied at either end, or at any intermediate servers where might be stored temporarily. Even when files are encrypted while stored, which itself requires a degree of technical ability, a determined attacker can often get the contents.⁴⁰

Comment

There are two issues – the perception that privacy could be invaded, and the actuality of any real invasion. There are no documented cases of credit card fraud due to interception of credit card numbers in transit. (There are many due to poor security leading to e-commerce sites being cracked.) Some banks explicitly indemnify their card holders against third party abuse of their card due to leakage on the Internet. The actual risk of interception causing problems for people seems very low.

The use of interception by law enforcement is something which society debates, but most people would agree that the capability is necessary. Concern over this would not appear to hinder use of the Internet by most people.

Example Mitigations

Education on facts

Discussion with bankers

Internet safety focus

³⁹ When using a secure site there is a padlock visible on a web browser. However, a padlock does not guarantee safety.

⁴⁰ For instance: FBI Hacks Alleged Mobster, *Wired News* 6 Dec 2000, www.wired.com/news/politics/0,1283,40541,00.html

Threat Type: Availability of ‘Dangerous’ Information Threat To: Public Confidence, Infrastructure

Potential Impact: High

Likelihood: Medium/Low

Summary

Concerns are sometimes raised about the availability of ‘dangerous’ information, such as bomb making recipes, on the Internet, and about disinformation or opinion being presented as fact.

Mechanism

There is a very wide range of people who have access to Internet publishing facilities. Some publish information they do not consider dangerous (but others might), some publish information which is dangerous but caution others not to use it. In practice there is little or no evidence of easy access through the Internet to accurate, dangerous information which is not already available through other channels, e.g. a public library.

Quality of information on the Internet is variable. In particular, a recipe for, say, ricin that might be found on the Internet may well not be complete or correct. There is no way of knowing this for certain unless one already knows how to make ricin.

‘Dangerous’ information – or any other kind – is only any use if you have an understanding of its quality. Because of its very nature, any ‘dangerous’ information on the Internet is likely to be published in such a way that its quality is very hard to check.

There is also a concern that information about infrastructure could be used by those seeking to threaten it. In the UK and the US information about some government facilities and utility networks has been removed from the web in the last few years.

Comment

Whether or not publishing information about infrastructure causes a risk to that infrastructure is a matter for the owners and operators of that infrastructure.

Example Mitigations

Literature survey or other attempt to find information – compare with other public sources such as public library, encyclopedias.

Discussions with Police

Threat Type: Insulting Behaviour and Defamation Threat To: Public Confidence

Potential Impact: Medium

Likelihood: High

Summary

There are many cases of email being used to harass, and web sites set up to insult people.

Mechanism

Email harassment is not new. It can include insulting messages sent to the target, and anonymous defamatory postings on email lists and newsgroups. A savvy attacker can forge email ‘from’ the target to expose them to ridicule. It is also possible to sign up the target’s email address to mailing lists used for the distribution of material they will find offensive.

There have been many cases of this, but it is often obvious who the perpetrator is. Forging email is easy but doing it undetectably is much harder. Often perpetrators have been caught and punished.⁴¹

In other cases, people have created websites to lampoon and insult their victims. This has occurred among school children in New Zealand, and has been dealt with by schools.

Comment

Although this is a problem, it is dealt with currently via harassment legislation. Other technologies such as SMS are also a channel for this.

Example Mitigations

Keep pressure on to behave well online
Education at school level
Internet Safety

Threat Type: Denial of Service Attacks	Threat To: Internet Infrastructure, Public Confidence, Agency Confidence
Potential Impact: Medium / High	Likelihood: High

Summary

Denial of service attacks can effectively shut down web servers and can damage Internet infrastructure. Until recently they have been acts of vandalism, but they are coming to be used for extortion.

Mechanism

In a denial of service (or DoS) attack, a target machine is flooded with requests it cannot meet. The requests may be structured to waste resources on the target machine or to exploit weaknesses in its software. Whether or not this is successful, the sheer volume of traffic may overwhelm the target machine and its link to the Internet.

Sending large volumes of attacking traffic requires resources and may also be traceable. Attackers get round this by using other people's computers as intermediaries. Many such computers can be used, which greatly amplifies the volume of the attack, gets someone else to pay for the resources used, and hides the perpetrator very well. This is called a distributed denial of service (DDoS) attack.

To mount a DDoS, an attacker needs a supply of well-connected machines that will do his or her bidding. With the rise of consumer broadband, and the traditional base of machines in Universities, there are large numbers of machines with permanent high volume Internet connections. Some of these are not well-secured. Attackers can gain control of such machines by cracking them individually. There is also evidence that many of the viruses which have flooded the Internet are designed, in part, to provide a "back door" into large numbers of machines so that an attacker can get the machine to participate in a DDoS⁴² or to send spam.

⁴¹ 'High' award for cyber-slur, *The New Zealand Herald* 1 September 2001, www.nzherald.co.nz/storydisplay.cfm?storyID=213086

⁴² Worms pour through MyDoom back door, *The Register* 10 February 2004, www.theregister.co.uk/content/56/35450.html

In February 2000, DDoS attacks crippled Yahoo, Amazon and CNN's web sites.⁴³ The perpetrator, a Canadian teenager, was identified nearly 12 months later after he bragged about it.⁴⁴ Other attacks have been made on Internet infrastructure. In October 2002 a the largest DDoS attack seen at the time degraded operations of the Domain Name root servers⁴⁵, which are a key part of the Internet infrastructure. Observers noted that the attack, while huge, was poorly focussed and had the potential to do more damage than it actually did.⁴⁶ Since this attack, more root servers have been commissioned and further steps have been taken to protect them.

Attacks have continued, and most attackers have not been caught. Sometimes attacks have caused problems to businesses, especially those which rely on their Internet presence. Extortion is a recent trend. Attackers, claiming to be Russian mafia, have crippled payment sites and demanded payment to desist.⁴⁷ They have threatened Internet sports gambling sites that they will attack during major sporting fixtures.⁴⁸ Some arrests have been made but this problem persists.

Virus writers also can use their creations to launch a DDoS attack. The MyDoom worm of February 2004 caused each machine it infected to repeatedly reload a particular website which then had to be removed from the web. A later variant of this virus attacked Microsoft's web page, but was unsuccessful in removing it from the web.⁴⁹

Compromised machines are referred to as zombies or 'bots', after the kind of robot program they run. There are several types including 'Agobot' and 'Phatbot'. These programs listen for instructions on specific channels on Internet Relay Chat (IRC) servers. Networks of compromised machines, or 'botnets', are made available for a price for sending spam or other nefarious purposes.⁵⁰

Comment

Denial of service attacks can stop the websites of all but the most well-resourced companies. This could threaten the very existence of smaller e-tailers. It has gone beyond a nuisance and is becoming a serious problem with the arrival of organised crime.

Example Mitigations

Individual well-resourced sites can make some capacity provision but this option is not available to most.

Better pursuit and prosecution of offenders

Rate limiting

Anti-spoofing measures

Black-hole routing (manipulating routing tables to get rid of traffic from certain sources)

⁴³ Yahoo Attributes a Lengthy Service Failure to an Attack, *New York Times* 8 February 2000, www.nytimes.com/library/tech/00/02/biztech/articles/08yahoo.html

⁴⁴ 'Mafiaboy' hacker jailed, *BBC* 13 September 2001, news.bbc.co.uk/1/hi/sci/tech/1541252.stm

⁴⁵ Massive DDoS Attack Hit DNS Root Servers, *Internet News* 23 October 2002, www.internetnews.com/dev-news/article.php/1486981

⁴⁶ Comments by Paul Vixie, one of the architects of the Domain Names System, www.ripe.net/ripe/mail-archives/eof-list/2002/msg00065.html

⁴⁷ E-commerce targeted by blackmailers, *BBC* 26 November 2003, news.bbc.co.uk/1/hi/technology/3238230.stm.

⁴⁸ Super Bowl fuels gambling sites' extortion fears *Infoworld* 29 January 2004 www.infoworld.com/article/04/01/29/HNsuperbowl_1.html

⁴⁹ Microsoft Unfazed by MyDoom's DDoS Attack, *eWeek* 3 February 2004, www.eweek.com/article2/0,4149,1507230,00.asp

⁵⁰ Phatbot arrest thows open trade in zombie PCs, *The Register*, 12 May 2004, www.theregister.co.uk/2004/05/12/phatbot_zombie_trade/

Threat Type: Trojans

Threat To: Public Confidence, Internet Infrastructure

Potential Impact: Medium

Likelihood: High

Summary

This is another way for viruses and spyware to proliferate. It also provides compromised machines for sending spam and contributing to DDoS attacks.

Mechanism

Trojans are named after the legendary wooden horse left before the gates of Troy, and which appeared to be a gift but in fact contained hostile troops. In computer terms, a trojan is a superficially desirable piece of software which has covert negative effects. An example is the Sub7 remote access trojan. This might be disguised as something else, perhaps by renaming it, and a user persuaded to download it. Alternatively it might be emailed to a user by a person or a virus. The user is induced, by standard social engineering techniques, to execute the file which apparently does nothing. The Sub7 trojan is now running invisibly on the user's machine. It has added itself to the programs which the computer runs when starting up, so rebooting will not get rid of it.

The Sub7 trojan allows a remote attacker – anyone on the Internet – to take any action on the computer. They could read, change or delete files, turn on the computer's microphone or web camera, and install other software such as tools for spamming or running a denial of service attack. The attacker can see all the keystrokes pressed on the machine and so can read userids and passwords.

Sub7 is now several years old. There are alternative remote access trojans such as QaZ and Infector. Anti-virus software will usually detect these trojans (although the trojans try to disable such software), but trojans are often altered by attackers so that anti-virus tools do not recognise them.

Comment

Trojans present two main risks: that people's security and privacy might be compromised by a Trojan on their machine; and that spammers and DDoS attackers routinely use them to compromise large numbers of machines with which they cause damage on the wider Internet.

Example Mitigations

Education

Virus scanners

Prosecution of offenders

Firewalls