Full paper in Proceedings of the 16th Annual NACCQ, Palmerston North, New Zealand, July, 2003 (eds) Mann, S. and Williamson, A. www.naccq.ac.nz

# How Safe Is Your Network? : A Guide to Practical Security Solutions

Hira Sathu
Caroline King
UNITEC Institute of Technology
Auckland, NZ
hsathu@unitec.ac.nz

## ABSTRACT

This paper considers the security threats to small and medium sized enterprise (SME) networks that are typical of New Zealand. As increased numbers of businesses take to connecting internal networks, the threats to their security begin. Further connection of their internal network resources, using the Internet infrastructure, to their vendors, suppliers, customers, partners etc. ushers in a number of benefits. However, this also brings in a set of new threats. As technology improves, so does the need for often more complex / elaborate security measures. Estimates for the expenditure on security are expected to rise in the near future to between 7% and 15% of the total IT budget of organisations. The need for a well-orchestrated e-Security plan is essential to minimise loss of revenue, but is often overlooked by the less aware. As a result, many networks lack the security required to operate in a professional business-like manner, let alone defend against the growing industry of hackers. This paper assesses a range of electronic threats, focuses attention on network security and suggests mitigation strategies corresponding to these threats. Two approaches are discussed: the phased approach and the layered approach, the latter having been the subject of an earlier study. The layered approach is now complemented by the phased approach, which recommends a logical consideration of the steps for incorporating security in networks. These two proposed approaches do not set aside the traditional approaches, but complement network security by forcing organisations to look at network design processes more deeply, and to include preventatives to minimise chances of network security breaches.

### Keywords

Small and Medium Enterprises, Network Security, Firewalls, Virtual Private Networks, Tunnelling, Network Address Translation, Encapsulation, Encryption, Intrusion Detection Systems, Subnetting, and Hacking Terminology,

## 1. INTRODUCTION

In New Zealand, Small and Medium Enterprises (SMEs - 100 employees or less) account for 98.3% of all businesses. (Fredericks and Watthayalage, 2002). Collective conclusions of various studies point to a very quick adoption of Internet and related technologies by SMEs in New Zealand. (ibid). The same study presented statistics about awareness and use of various Networking, e-technologies and Virtual Private Networks (VPNs) by SMEs in New Zealand. (See appendix) A comparative study of figures reveals that the awareness of the well-publicized security technology such as VPN by SMEs in NZ is low (45%). The deployment of this technology by them is even lower (10%). The already low survival rate of these enterprises compared to the bigger firms would only further plummet if due attention were not paid to the safety and security of their networks. Estimates for the year of 2000's expenditure on Security that lay between 2% and 8% were expected to rise to between 7% to 15%. The authors have identified through experience, and gleaned from discussions at forums like the New Zealand Information Security Forum and New Zealand Security Association, numerous issues that affect businesses.

A review of the literature, attendance at seminars and discussions with senior network engineers have served to identify the issues that are most important for SMEs and to provide realistic solutions. This paper introduces some general threats to which these adopters of network technology expose themselves, and goes on to discuss some practical solutions. The subsequent sections cover, in greater detail, the threats and mitigation strategies that may be applied to a well-orchestrated security plan for other enterprises as well. The paper emphasizes the nature of network security as an ongoing process rather than a one-time solution that may be procured from the market as a piece of hardware and/or software solution.

## 2. GENERAL THREAT ASSESSMENT

The moment a business connects two or more computers into a network, the security ramifications change from that of a stand-alone computer. Additional awareness of the threats that need addressing, range from monitoring of the transmissions over the media, (wired and wireless) by unauthorised persons, to appropriate allocation of permissions to the shared resources on the network and its monitoring. There is also the human perspective, which is perceived by many as the single biggest threat. This could include employees whose job functions have been changed or employees who are no longer working for the company. Their login account permissions to resources should have been changed when their position or status changed. Inattention to this means that these employees' access to the network resources pose a large threat. Social engineering of employees, where only rudimentary login and password protection exists, further increases the threat from within the network.

Threat assessment takes a different dimension when an organisation connects to the Internet. Although providing benefits, a web presence or email communication opens the organisation to external threats, in addition to the internal threats. These threats may result in potential damage to a business by loss of confidentiality, integrity of data or even the availability of its system resources and services to the rightful users.

Quoting Australian Computer Emergency Response Team (AusCERT) "No matter what security systems you have in place or how secure your existing systems might be, new threats and vulnerabilities emerge every day and provide new opportunities for your network to be attacked. What may be considered a secure network configuration today may change tomorrow if a new vulnerability is discovered in the operating systems, applications or protocols deployed on your network." (AusCERT, 2003)

An always-on connection from a family of DSL technologies, Telecom NZ 's JetStream for example, exposes systems to hackers who attempt to gain information using sniffers to identify the active systems on a network and follow up with port scans, worm probes, Spam and denial of service. A related issue to this unwanted clogging of your access pipe, is receiving inflated bills (Adams, 2003).

Some generic practical solutions to mitigate threats from outside the organisation or from within the unclassified part of the internal network to the confidential /secured part of the network are covered in the succeeding paragraphs.

## 3. PRACTICAL SECURITY SOLUTIONS

Some practical solutions to cover the above threats are listed below:

♦ Laying and securing of the cable media in a way that is not easily accessible and prone to tampering. Some suggestions include the laying of these between walls, floors and ceilings. Choice of the media itself would depend upon the physical security environment of the network deployment.

♦ Where additional jack points exist, these should be disconnected from the hub, switch, router or even a patch panel. The use of switching technology overcomes the broadcast nature of packets in networks using hubs.

♦ Physically securing the networking components, like hubs, switches, routers and other central facilities like servers, from common user access is recommended where possible.

Where wireless networks are deployed, the use of common security features like the Network Name (AP Name), password and the MAC address authorisations, needs to be complemented with encryption. For enhanced security requirements, systems using dynamic encryption keys are preferable over those using static key encryption. On account of the frequent movement of wireless client nodes, the potential for loss of laptop computers is high, thereby compromising the security of any confidential data on the system. Even where the data is encrypted, the location of the key on the system, once the hurdle of login and password is crossed, enables decryption. However, some modern systems (laptops) incorporate a crypto-processor chip on board which can only be

used to encrypt and decrypt data after authentication with a bio-metric (finger print) authentication. Other aspects that could aid in security to varying degrees include the aerial design, signal strength used etc. These are possibly beyond the purview of a common user.

A basic solution for external threats discussed above could include, software based firewalls from Norton, McAfee, PGP, Sygate and Zone Alarm from among the many vendors offering similar solutions. Some of these solutions are even free for personal/home users. Many router vendors bundle firewalls with their routers. Network Address Translation (NAT), another basic security measure, hides the internal network address (es) by presenting a public address that can be configured on most routers. VPNs provide another defence while communicating over the Internet or any unreliable Public data Network. Likely scenarios utilising VPNs would include a head office communicating to remote branches or employees in remote locations accessing computing resources over this unreliable public network infrastructure. Deploying a VPN concentrator, also referred to as a VPN gateway, for the establishment of VPN tunnels is a popular approach. Organisations that wish to deploy multiple security solutions like NAT, VPNs and firewalls would do well to choose a common vendor for these multiple security requirements. This overcomes scenarios like a VPN across a firewall that may be taken advantage of by hackers. Some popular solution providers are CheckPoint, NetScreen, Cisco, and 3 Com. The final choice would depend upon the customer's specific requirements.

E-mail has become a ubiquitous means of communication; it has therefore been considered separately. Both the issues of the confidentiality of the content and that of verification of the sender can be resolved. Most email packages enable the use of the private key for encryption of the originator's signature, and encryption of the email contents and the signature by the public key of the destination addressee. The receiver of the message decrypts the complete message using his private key and uses the sender's public key for decryption and signature verification. Some packages like MailMarshal SMTP take care of virus scanning, blocking Spam, control of attachment file type, and scan content of messages. Quoting from Marshal Software website (MailMarshal, 2003) "MailMarshal Secure complements the capabilities of MailMarshal SMTP by adding automated privacy to business email".

Additional precautions that go a long way in improving security are: changing the default configuration settings on the switches, routers and browsers; not leaving dial up modem on; using dynamic addresses where possible. However, organisations that have the luxury of IT departments can monitor traffic and consider a more detailed analysis of threats, mitigation strategies and approaches to be used. Some of these approaches are covered in the following sections.

# 4. SPECIFIC ATTACK TRENDS AND CATEGORISATION

Taking stock of the recent trends in technology and the ensuing new attacks, Arjen de Landgraaf of Co-Logic, New Zealand, (Landgraaf, 2002) describes the new playing field as one where the speed of launching and the sophistication in the delivery of the attack creates a plethora of problems for networks which have a minimal security infrastructure. Often there is an asymmetry in the attack that involves a distributed denial of service (DDOS).

These attacks can be categorised into three main groups, namely:- attack on the use of the system, attack on the data and unauthorised access attack.

An attack on the use of the system usually takes the form of flooding the victim's network with illegitimate packets or emails until the overload causes a network failure. Denial of Service (DOS), Distributed Denial of Service (DDOS) and mail bombs fall into this area. These are usually advantaged by lack of filtering and by not limiting the number of half-open ports. Some examples of DOS and DDOS types of attack were experienced by Yahoo.com and Amazon.com in early 2000 (Schneier, 2000).

An attack on the data can take several forms, such as malware and downloading of false software. Malware (malicious software) is so called because the primary aims of these attacks are to propagate and to destroy data. These are commonly spread through email attachments and programs downloaded from the Internet. Included in this category are virus, Trojan horse and worm attacks.

Damage caused by malware may include the destruction of File Allocation Tables (FATs); decreasing the space on hard disks by duplicating files; formatting specific tracks or entire disks; destroying parts of programs and files; sending a copy of itself to e-mail

addresses in the global address list, causing e-mail systems to crash and saturating the network bandwidth; scanning for passwords and other loopholes, then sending these back to the attacker. The last of these is commonly used to enable man-in the middle attacks, which involve the Telcos, ISPs or VAN providers, and the damage includes theft of packets, hijacking of ongoing sessions or the introduction of new mis-information. There are cases where the original software from the vendors itself is flawed. A case in point is the Web-based Distributed Authoring and Versioning (WebDAV) component of Microsoft Internet Information Web Server (IIS Version 5.). This flaw allowed an attacker to run malicious code on such a (vulnerable) server. To overcome this flaw, Microsoft does offer a patch. Other related areas of concern with software are the software updates and patches themselves being the cause for the problem. Downloading and installation of infected / tampered program code from a malicious site only adds to the security risks.

Unauthorised access attacks are caused by lax security or malware. These include password and intrusion attacks. Sophisticated means, such as a combination of malware, Packet Sniffers and Trojan Horse programs can effectively breach e-Security. Intrusion attacks use known vulnerabilities to penetrate networks and perform unauthorized tasks. Gartner Research Group (Gartner, 2003) estimates that 90% of attacks exploit well-known vulnerabilities. Network reconnaissance using DNS queries, ping sweeps and port scans are some primary steps taken by hackers before venturing into a specific attack. Trust exploitation by intruders takes the form of one successful attack on a vulnerable server being extended by compromising the other servers that have trustee relations with the vulnerable server already attacked.

# 5. MITIGATION TECHNIQUES

The techniques discussed above in Section 3 can accomplish mitigation of the threats to only a basic level. For a hole-proof network design, a comprehensive set of mitigation techniques needs to be adopted as discussed below.

Insistence of adherence to procedures may seem trivial, but is very effective. Passwords should be individual, encrypted, never revealed and updated regularly to prevent unauthorised access problems. Forbidding chain emails can prevent both network congestion and the spread of viruses. Ensuring that no software or updates may be loaded unless bearing a seal from “Verisign” or equivalent certifying authorities, or direct from the supplier, will ensure that the software itself is not infected. Allowing only a small number of half open ports to be open simultaneously will prevent many of the flooding attacks.

A firewall could be used to validate the source, content, protocol etc. of the incoming packets, and filter such packets. These could take care of DOS and DDOS attacks where the intruder is attempting to consume valuable resources. The packets soliciting ICMP echo type replies, such as Ping of Death, are filtered when the number is over a given threshold. Anti-spoofing actions, to mask the identity of the intermediary and the final victims would limit the efficacy of DOS and DDOS attacks. It makes good design practice to consider filtering for DOS / DDOS attacks at the upstream end at the ISPs / Telcos. The process of detecting unauthorized use or an attack upon a computer or a network through Host based Intrusion Detection Systems (HIDS) or the Network based Intrusion Detection Systems (NIDS) is a proactive approach to mitigation of e-security threats. These function firstly as a feed back mechanism to inform the security staff about the effectiveness of the network and / or the host components, and secondly to provide a trigger for gating mechanisms that determine when to activate planned responses to an incident eg ping sweeps and port scans. Trust exploitation can also be prevented when a HIDS is configured to provide alerts or even terminate an exploitation process when a port redirection is attempted.

# 6. PHASED AND LAYERED APPROACHES

The study of e-security needs to be complemented by suitable comprehensive approaches. The two approaches, phased and layered, outlined below, are neither self-fulfilling nor mutually exclusive and need to be fine-tuned for each business case.

## 6.1 The Phased Approach

The phased approach takes a view of the overall system from the following perspectives: -

Phase 1: Threat Assessment - the consideration of which assets need to be secured, the threats to these assets, and the prioritisation of the security requirements. Threat assessment here would need to consider how much time, money and effort the business is ready to spend to protect these resources.

Phase 2: Policy Development - the creation of a formal statement of rules and procedures by which people are given access to an organization’s technology and information assets. Defining what is valuable and the steps to protect them establish the

framework for this phase, which is evolutionary and may continue through other phases. Some examples of policies covered here would include Remote Access Policy, Password Policy, Audit policy, Email policy, Internet Access policy, Monitoring Policy and the Encryption Policy.

Phase 3: Security Architecture - defines the security environment for the organization based upon the previous two phases. This involves consideration of firewalls, virus protection, filtering, encryption, and intrusion detection systems (IDS). Deciding which resources are placed in the private (more secure) part of the network and those, which are in the De-Militarized Zone. The architecture here would involve the need for dual firewalls as against a single firewall. The design for virus protection being implemented centrally, on individual desktops or both is evaluated. The implementation strategy for HIDS and NIDS is covered here.

Phase 4: Technology Solutions - the technology selection is based on the security architecture. Proposed selection criteria could include functionality, operating system (security level provided by it), industry recognition /support, cost and administration involved. Each of these is given a weighting. Likewise suppliers /vendors of the technology (Hardware and / or software) would be considered and their products given a weighting for each of the above features. A weighted average matrix can then be compiled for each of the technologies from available options for comparison and ultimate selection.

Phase 5: User Education - the inculcation of physical security procedures among the staff. This is achieved by educating them as to the areas of sensitivity, such as using unclassified communication channels, and the action that staff are to take when informed of emails and other applications that lead to e-Security problems. Often, breaches in e-Security are as a result of poor awareness among the employees. Therefore, there is a need for staff to be made aware of the importance of security and adherence to policies. Any ambiguity in the interpretation of the policies should also be removed during the education phase.

Phase 6: Auditing And Monitoring - Security policies are only useful if they are monitored. The e-Security environment needs to be audited regularly to ensure that the security requirements still meet the defined standards. The futility of intrusion detection systems, when not monitored, is an obvious example in this regard. Whenever changes are made in the network design, the changes in the monitoring and auditing policy must be reviewed to ensure the effectiveness of the security system.

## 6.2 The Layered Approach

This approach is based on the OSI 7 Layer Model and emphasises the security in the data communication process. This approach is related to the Onion Skin Model (Martin, 1973) approach for Information Systems security, which concentrates on the inner layers. Our model uses the layered approach based on the OSI structure, thereby considering the security issues at deeper levels and suggesting solutions. A detailed description of this methodology is described in the author's paper (Sathu, 2002). Briefly, the levels considered are :-

- Physical and Data Link Layers (Layers 1 and 2) - herein attention is drawn to the issues relating to media type, topology and the Media Access Control Protocol (MAC) used. The appropriate selection of media should depend upon the layout of the business and its physical security environment. Some design issues include use of keyboard locks and screen saver passwords, use of finger print readers (Hancock, 2000), use of encryption software on all mobile devices, and tunnelling. International Telecommunication Union (ITU) tunnelling standard L2TP is the protocol of choice for highly secure set-ups and is very well complemented by good authentication and encryption schemes when used along with IP Sec.

- Network And Transport Layers (Layers 3 and 4) - use of network layer addresses for internetworking and routing involves disclosure of the source and destination addresses. This opens up opportunities for hackers to pose as genuine nodes on the network. It is therefore necessary that the knowledge of the layer three (network) address, IP for instance, should be on a need-to-know basis. Considering the IP addressing scenario, a situation where subnetting is adopted, enhances the subnet security. Other methods include use of packet level, circuit level and stateful inspection firewalls, and the choice of the addressing schemes. eg use of IP version 6 addressing scheme's Authentication Header and Encapsulation Security Payload has definite advantages (Atkinson, 1995). Most Internet Applications, for quite some time now, have been released with embedded security features. For example, Netscape and Internet Explorer support Secure Socket Layer (SSL), which protects web traffic (Nichols, Ryan and Ryan, 2000). SSL operates at Layer 4 of the OSI stack. Thereby it establishes secure connections between the end-to-end parties between the TCP / UDP ports used for the session.

- Session and Presentation Layers (Layers 5 and 6) - the establishment, authentication and the encryption of sessions are considered here. Multiple factor authentication schemes and password encryption

should be used. Two-factor authentication using either challenge response or the time synchronisation systems is now commonplace, the principle being that both the knowledge of, and the possession of, secure ID token cards are required to compromise the security. In highly sensitive requirements, use of biometric authentication, like retinal or fingerprint scans, may be an additional authentication factor to be considered before permitting a session. Use of secure shells (SSH), along with various encryption schemes, before transmission of data over the network would keep a check on mail theft, sniffing and snooping, thereby maintaining the privacy and the integrity of data.

♦ The Application Layer (Layer 7) - the consideration of security at the level closest to the user. Application layer firewalls are most secure but are heavy on network resources. Increased latency in the network becomes a major issue when using a multiple rule-based firewall. Varying levels of security access, required by specific application servers running in the network, such as a Database server, would be over and above the basic network security, and considered to be embedded in the application itself.

In the network management systems using community string names that are difficult to guess is the minimum requirement to avoid a "...major security risk with SNMP" (Chapman & Zwicky, 1995) where "someone else might be able to take over control of your network equipment."(ibid).

To forestall security breaches during remote access to applications, the implementation of additional authentication services, such as RADIUS and TACACS+, may be required in the network.

# 7. CONCLUSION

The use of an appropriate mitigation strategy after a threat assessment would be the correct approach for most large organisations. Many small and even medium enterprises cannot afford the luxury of an IT department or the services of a security consultant to work out its exact or specific security needs. Keeping this in view, a general awareness of threats and some basic solutions have been covered in this paper. There is a chance of some companies going to extremes with security, which may result in poorer response times for both internal and external connections and much higher costs. If we assume a business where the performance or throughput is the greater issue and security requirements are not particularly stringent, the use of simple packet level firewalls (incorporated in the router), that do not examine the deeper content of the packets, is sufficient. Numerous new firewall products emerge regularly. The important issue when installing any product is the correct configuration, update and application of current patches, where necessary, rather than a poorly configured firewall solution that comes with plenty of features and expenses. Hence, all approaches for network security should consider the threat assessment, selection of the mitigation strategies and the cost-effective implementation of the solutions.

# REFERENCES


Adams, G.(2003) "Always on; always dangers", TUANZ Topics, 13(2): 11-14

Atkinson, R. (1995) "Security Architecture for the Internet Protocol". http://www.cis.ohio-state.edu/cgi- bin/rfc/rfc1825.html

AusCERT (2003) Accessed March 8, 2003. <http://www.auscert.org.au/render.html?it=1924>

Chapman, D.B. and Zwicky, E.D. (1995) "Building Internet Firewalls" US:O'Reilly & Associates, pp 39-40

Fredericks, H. and Watthayalage, D. (2002) "Small and Medium Enterprises: An Assessment of Strategic Use of the Internet & e-Technologies for Creating Value & Enhancing Competitiveness". Proceedings of the National IT Conference Colombo, Sri Lanka, 10-11 July, pp 69-89

Gartner Research (2003) Accessed May 16, 2003. <http://www4.gartner.com/DisplayDocument?id=389173&ref=g_search>

Hancock, B. ( 2000) "Security Views, Computers and Security" , 19(3):202-221

Landgraaf, A. D. ( 2002 )"Secure New Zealand", NZISF seminar, June 2002.

MailMarshal (2003) Accessed 12 May, 2003. <http://www.marshalsoftware.com/secure>

Martin, J. (1973 ) "Security Accuracy and Privacy in Computer Systems, US:Prentice Hall.

Nichols, R.K., Ryan, D.J. and Ryan, J. J.C.H. (2000) "Defending Your Digital Assets", US:McGraw Hill, pp. 604-629

Sathu, H. (2002) "Network Security: A Layered Approach", NZ Journal of Applied Computing & Information Technology 6(1): 60-65

Schneier, B. (2000) "Secrets and Lies: Digital Security in a Networked World", US:John Wiley & Sons Inc

# APPENDIX

**Figure 1: Source: Fredericks. and Watthayalage (2002) p84**
**Figure 2: Source: Fredericks. and Watthayalage (2002) p84**
**Figure 3: Source: Fredericks. and Watthayalage (2002) p85**