Network Security: A Layered Approach

UNITEC Institute Of Technology
Auckland, New Zealand
hsathu@unitec.ac.nz

Hira Sathu

ABSTRACT

The paper uses the OSI 7 Layer Model approach to focus attention on network security. Problems with some of the traditional approaches to network security are discussed. The proposed methodology does not set aside the traditional approaches but complements network security by forcing organisations to look at network processes deeply. The discussions of the capabilities at each of the layers highlight the concerns in network security. Some measures that could be applied at each layer of the communication process to overcome these concerns are mentioned. It is expected that this approach would eventually develop a matrix of capabilities and measures that could be used by organisations to minimise chances of network security breaches. This matrix is expected to be dynamic, as newer tools/measures would be included as and when they become known. This matrix can be used, as a template to assess businesses network security, to develop the overall security policy and even to the redesign of the business processes.

KEYWORDS

Firewalls, Virtual Private Networks, Tunnelling, Network Address Translation, Encapsulation, Encryption, Network Management Systems, Intrusion Detection Systems, Subnetting, and Hacking Terminology.

1. INTRODUCTION

Network Security keeps gaining greater importance as businesses rely heavily on electronic means of communication. The upsurge in e-commerce has only further strengthened the case for ensuring that a secure network infrastructure is in place. In spite of the best intentions to secure networks, traditional approaches to network security reveal holes that still remain in the initial design. The tendencies to concentrate in one area, while leaving others unattended often lead to gaping holes. The approach to network security continues to be viewed within the overall context of information security. Understanding what can go wrong, is the first step to executing a healthy and successful security implementation. The paper focuses on drawing attention to most network communication processes at different levels. Action

taken at each of the levels reduces the vulnerability to some threats only and not to others, thereby acting like additional lines of defence. This is a discussion paper with an innovative approach to analysing network security. This is expected to lead to a network security matrix, which aids in reviewing the security policy and business processes.

2. TRADITIONAL APPROACHES

Traditionally the approaches considered herein fall under the Onion Skin Model and evolve as organisations grow. The Onion Skin Model approach by Martin (1973) views overall information security as concentric security rings around the data. The rings starting from the inner to the outer are; computing, security in the data processing systems, physical security, administrative controls, legal and societal environment. In proposing this model Martin himself pointed out that the model is clearly incorrect. He goes on to state that the use of administrative policy or the physical access controls however well implemented could have no impact on the risks associated with the access over the network infrastructure. This model is suited to the centralised mainframe environment. The present day networks are decentralised, therefore the application of this approach (old skill) would be challenging (Baker, 1995).

In the formative years, the tendency by users and IT staff had been to place emphasis on security parameters only in the application. During the early years of client server systems, security involved the authentication of the users over the network. This was by way of rights granted to the users and specification of types of permissions over the resources on the network. More recently this has developed to include these rights and permissions being authenticated over the entire resources on the enterprise network.

In most cases network security in organisations evolves more as an afterthought. The network security beefed up by organisations subsequent to attacks like: denial of service, virus attacks, breaches of confidentiality etc. are well known. The reason for this is the lack of perception of security risks over the network not being fully visualised at the outset. The methodology considered below is based on highlighting the communication processes over the network to forestall the shortcomings in the traditional approach. The approaches though useful are simplistic and therefore need to be supplemented by the network security methodology recommended herein.

3. THE METHODOLOGY (OSI7)

This methodology is based on the Open Systems Interconnection 7 Layer Model put forward by the International Standards Organisation. This model breaks down the complex communication processes into a hierarchical set of seven layers with specific functions for each layer. A network security approach based on the OSI 7 Layer Model is considered herein bringing forth the correspondence with the appropriate OSI layer. Where possible, suggestions for network security are mentioned to minimise the chance of any gaping holes. This approach has already proved useful in the understanding of the network security issues and concepts by students in the academic environment. It is expected that this approach should also prove useful in the business world for designers and consultants in network security.

The proposed methodology emphasises the security in data communication. This by no means implies that the physical and other security measures to be adopted at the source and destination of the network are trivial. In fact this approach has a relation to the Onion Skin Model approach for Information Systems security that has been used in the past. It concentrates on the inner layers (Physical, Computing and DP Systems) of this model and uses the layered approach of the OSI structure thereby considering the security issues at deeper levels with suggested solutions. In most popular communication protocols, very often the functionalities of upper layers are collapsed. Accordingly, the OSI layers are considered jointly for appreciation of the security issues without losing sight of the likely security threat as a consequence of the communication processes involved. To evolve a comprehensive network security infrastructure each of the layered components is considered with other variables in the security equation remaining constants. However, some security measures may be dropped only after a careful cost benefit analysis. The methodology adopted is described in the following four sections.

4. PHYSICAL AND DATA LINK LAYERS

Considering Layers 1 and 2 of the OSI model first, draws our attention to issues relating to media type, its 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. Where it is possible to install guided media, use of fibre optic cable is recommended as compared to unshielded or even shielded twisted pair cables. Calling line identification or calling back routines to verify remote calling nodes is recommended at this layer. Some design issues could include use of keyboard locks and screen saver passwords. Use of finger print readers incorporated into laptops before booting is Intel's Protected Access Architecture (IPAA), useful for both standalone and network data security (Hancock, 2000, pp 202-221). Action taken to prevent information about remote access (modem) phone numbers and IP address of routers and other network devices being passed to unauthorised persons must be taken. There are modems that dial back and others that also encrypt information being sent and received. (Farley, Stearns & Hsu, 1996, pp185-203). Some of the measures mentioned herein when viewed stringently fall even before the Physical Layer say Layer 0 but their significance while considering the Physical Layer details is only logical.

As for the unguided (wireless) media, it is further insecure and additional security needs to be built into the system. The higher speed wireless LANs that are greater than 10 MBPS are more secure than the lower speeds in the range of 1 to 2 MBPS. In wireless networks packet switched networks are efficient replacements for circuit switched networks. However, user access to these networks that are always on, needs to be verified with frequent password changes. Use of encryption software on all mobile devices is recommended.

At these layers when we analyse the topology of the media, the Bus topology using CSMA-CD (broadcast method) is the least secure and therefore necessitates stringent monitoring of the physical layout. This is due to the broadcast access method that is easy to tamper with using nodes on the network with appropriate Network Interface Cards (NIC). Comparatively the Ring and Star topologies have an edge over the Bus topology. Where Star-Bus and Star-Ring topologies are deployed, a secured location for these is recommended. In this regard it may be of interest to note that insiders are commonly cited as a major source of attack (Cohen, 1995, pp 114).

The wireless networks, which are in star topology and use CSMA-CA (broadcast with overheads) access method, are open to interception therefore additional measures need to be adopted for ensuring network security at this layer. As reported by a freelance technology writer Katz-Stone, (2001) "…your 802.11 Wireless Network has no clothes", and reports William A. Arabagh & his Colleagues suggestion about security flaws in popular LANs being more pervasive than previously supported. This report also questions the robustness of Wired Equivalent Privacy (W.E.P). One such measure is to allow only nodes with pre-specified MAC-addressed NICs hooking on to the network incorporated into the LAN design. Even when WEP is enabled MAC addresses appear in the clear to a sniffer's delight. Wireless cards can also be reconfigured via software for MAC addresses, making masquerading as a valid user easier. Shared key authentication can be easily intercepted and used to derive encryption codes in use, and then used to generate a valid authentication response message.

The practice of establishing communication over serial line interfaces using SLIP or PPP also gives rise to security breaches at this layer. PPP is more popular on account of its lending itself to enhanced security besides versatility of use. Security is strengthened by use of Password Authentication Protocol, however use of Challenge Handshake Authentication Protocol (CHAP) is a better bet since the chances of password spoofing over the communication media are marginalised.

At this layer there is also a need to consider "Tunnelling" for further security where these LANs are connected over the Internet to form MANs or WANs. Tunnel Modes could be either end-to-end or gateway-to-gateway or even a hybrid of the two. For higher security requirements end-to-end modes are recommended as the service providers are removed from the network security equation. With regard to the choice of the tunnelling/encapsulating protocol, PPTP (Microsoft proprietary protocol) is

useful for low security requirements. This has both the tunnelling and encryption in built. 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, which is discussed in section 5 below.

5. NETWORK AND TRANSPORT LAYERS

The issues discussed here relate to layers 3 and 4 of the OSI model. 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, situations where subnetting is adopted enhance the subnet security, as the knowledge of the IP address does not reveal the network and node identification. This is more by default than by design, since the primary motivation for subnetting may have been efficient address allocation.

Security schemes vary depending upon the choice of the addressing schemes deployed. Use of IP version 6 addressing scheme brings with it security-rich features. As described in RFC 1825 (Atkinson, 1995), Authentication Header and Encapsulation Security Payload are definite advantages IP version 6 incorporates within itself. However, the overall benefits would be seen once the protocol gains universal acceptability and adaptability. Active research is on, to provide scalable multicast key distribution for audio and / or video conferencing using IP version 6.

Use of packet level and circuit level firewalls provide the first place where small to medium businesses generally address their security requirements. The packet level firewalls by design are positioned where a local or a campus area network connects to a WAN. These are generally incorporated in the edge routers or separate systems. Packet level firewalls are most efficient, but provide only a basic level of security by replacing/filtering the source network addresses. This is very similar to Network Address Translation (NAT) feature available in most modern routers. The Stateful inspection based firewalls provide higher levels of security. Herein the inspection of the session and state of the communication process enables much better control over the process.

Virtual LANs also go towards securing a LAN group, as the geographical location is independent of the logical network associations. These virtual networks could be established in a variety of ways (Mandeville, 1997, pp57-66). At the physical layer the port address comes in handy with the MAC address at Layer 2. Use of network layer addresses is very common for nodes physically on different networks. The uncommon application-based VLANs are helpful for the ever-burdened network administrators.

Secure protocols like IP Sec have become a standard for Virtual Private Networks (VPN) encryption and Layer Three tunnelling. The protocol has an agreed method of key exchange with authentication that proves the source. This enables data integrity of a high order with every packet being signed. Two different modes in IP Sec enable a choice between transport and tunnelling modes. The later mode is used between two tunnel partners that exchange data on a regular basis like routers, gateways or domain controllers. The security here is further improved due to the encapsulation of the IP packets within another IP packet.

Most Internet Applications are now released with embedded security features. For example Netscape and Internet Explorer support Secure Socket Layer (SSL), which protects web traffic (Nichols, 2000). SSL operates at Layer 4 of the OSI stack. Thereby it establishes secure connection between the end-to-end parties between the TCP / UDP ports used for the session. For protection of credit card transactions over the Internet some vendors support Secure Electronic Transaction (SET) which takes care of authorisation and nonrepudiation.

6. SESSION AND PRESENTA-

TION LAYERS

Establishment, authentication and the encryption of sessions corresponding to layers 5 and 6 of the OSI model are considered here. Conventional login and password are not considered adequate for high security requirements as these are easily guessed and compromised. 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 here is that both the knowledge of, and the possession of, secure ID token cards is required to compromise the security. Separate authentication servers like the RADIUS or TACACS+, where the number of users is large, are used to overcome latency / load on the remote access servers. In highly sensitive requirements, use of biometric authentication like retinal or fingerprint scans may be an additional authentication factor considered before permitting a session. The networking and processing overheads need careful consideration.

Use of various encryption schemes before transmission of data over the network would keep a check on mail theft, sniffing, snooping, smurfing and thereby maintain the privacy and the integrity of data. The choice of the encryption would depend both on the degree of security and the business requirements. As of early 2001, triple DES would be considered a high-end symmetrical encryption scheme. Public Key Infrastructure in the field of encryption is gaining further ground (Nichols, Ryan & Ryan, 2000, pp 604-629) in view of the ease of key administration and incorporation of digital signature, making it a very popular choice for both internal and external networks. Windows 2000 uses a system of Enterprise Certificate Authority (CA) for its internal communications or a standalone CA for outside use. Windows 2000 environment makes use of the Kerberos authentication Scheme that encrypts the authentication process over the network and use a centralised key distribution system. Secure automated key distribution schemes aid effective and efficient key distribution.

Recent advances in securing communication over the Internet now enable authentication and encryption. Secure multipurpose Internet Mail extensions (S-MIME) are available for securing email traffic. Quoting Stewart and Scales (2000, pp 536) “Public Key Encryption is also available on the Internet. Secure Socket Layer (SSL) and Transport Layer Security (TLS) use certificates for both clients and servers for authentication, confidentiality and data integrity.”

7. THE APPLICATION LAYER

The security at Layer 7 also referred to as the application layer is considered here. This can take on different forms. In the area of firewalls, application layer firewalls are most secure but are demanding by way of network resources. Increased latency in the network becomes a major issue while using a multiple rule-based firewall.

There are also specific application servers running in the network that may require varying levels of security access as in case of a Data Base server; these would be over and above the basic network security and considered to be embedded in the application itself. This has been covered earlier as one of the traditional approaches. These security measures would continue to exist varying with the security needs reflected in the business requirement

Network management applications by design require the network components to be seen by the management system. This gives rise to security issues vis-à-vis ease of network management systems (NMS). If the community string for the NMS is known, any router can be used to poll for information on that community. Observing steps to safeguard the knowledge of community strings like using names that are difficult to guess by intruders would be a minimum requirement. Study of previous hacker attacks reveal that they rely on the very tools that facilitate network monitoring, configuring, accounting and troubleshooting. Quoting firewall gurus (Chapman & Zwicky, 1995, pp 39-40) “…major security risk with SNMP is that someone else might be able to take over control of your network equipment…..”. This makes essential that intruder detection systems (IDS) should generate alerts any time the use of such tools is resorted to by an outside agency. The future network management tools would need to incorporate features that do not permit any third party monitoring tools being used once a network management is in place without the explicit knowledge/permission of the network manager. To

take benefit of any third party tools should necessitate disabling of the network management system first.

For permitting remote access to mobile and telecommuting users the use of remote control applications like Carbon Copy, pcAnywhere becomes a security hole. This software allows access to network resources by passing the firewall; resulting in a backdoor entry to the private network. To forestall this, additional authentication service may require to be implemented in the network for allowing this access. Appropriate security needs to be incorporated for restricting access to users depending upon their needs hierarchy within the business applications.

IDS applications often provide specific automated responses for rule violations: flags and warnings for system administrators, automatic user privilege suspensions, automatic email or pager notifications, or a simple but specific notation in a log. These reports help in creating a more accurate picture of network usage, which will allow for more appropriate rule creation, an increased ability to plan for future network usage and a refined ability to predict and counter network attacks.

8. CONCLUSION

The over insurance of network security and its adoption may lead to perceived or real production inefficiencies. Real production inefficiencies due to incorrect implementation of redundant layers of security that defeats the very purpose of the network's existence should be avoided. This can be taken up once the elemental considerations are over, and only then should these be considered together to check for redundancies at the overall network security level. The aim of the paper is to emphasise the security issues at different levels of the communication process and use the OSI 7 layer model for this. However, the implementations in the real world would vary depending upon the communication protocols used in the network, the perceived threat and the management's appreciation of security. It is emphasised that the use of the traditional approaches may form the basic Information Security framework and the recommended layered approach is used for network security to plug any holes noticed after a careful consideration of the network communication processes. This approach to Network Security also emphasises the concept that security of a network is only as strong as its weakest link and therefore necessitates a look at the weaker links in the chain. This would eventually result in increasing the aggregate level of Network security of the organisation. To reinforce this, picture a wireless LAN or an easily accessed physical LAN with the most sophisticated firewall in place being hacked into without the need to overcome the firewall first.

This paper is expected to lead to a matrix of capabilities at each of the networking layers with suggested measures. Organisations could use it as a template for verifying the network security they have in place. This in turn may lead to then reviewing their network security policy or even changes in their business processes. The details of these are expected to be the subject matter of a further paper by the author.

REFERENCES

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

Baker, R. H. (1995) Network Security, US, McGraw Hill, Inc

Chapman,D.B. and Zwicky, E.D. (1995) Building Internet Firewalls, US, O'Reilly & Associates

Cohen, F.B. (1995) Protection and Security on the Information Superhighway, US, John Wiley & Sons

Farley, M., Stearns T. and HSU J. (1996) LAN Times Guide to Security and Data Integrity, US, Osborne McGraw Hill

Hancock, B. (2000) Security Views, Computers and Security Vol.19, No 3

Katz-Stone, A. (2001) Open Book: 802.11b Security Gaps Expose Wireless LANs April 2001 (http://www.8wire.com/articles/print_articles.asp?printAIDE=1958)

Mandeville, R. (1997) VLANs: Real Virtues, Australian Communications, August

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

Stewart, J.M and Scales, L (2000) Windows 2000 Foundations, US, The Coriolis Group