New Zealand Security of Information Technology Publication 202

THE SECURITY OF LOCAL AREA NETWORKS

CHAPTER 1

INTRODUCTION

LAN Architecture

101. Organisations have traditionally depended upon centralised minicomputer and mainframe processing and proprietary wide area networking for access to information systems resources. However, the emergence of methods in the 1980s for connecting personal computers (PC) which are physically co-located has led to the development of much more sophisticated communications systems. Local Area Networks (LANs), as the PC communications systems are known, have become a major information systems architecture within many organisations, providing a substantial proportion of the corporate data communication needs.

102. This document is aimed at departmental information systems management, LAN administrators, security officers, LAN users and others who have a responsibility for protecting information processed or stored on a LAN. The purpose of this document is to help the reader understand the need for LAN security and to provide guidance in determining effective LAN security controls.

103. A LAN typically consists of a number of servers and a number of workstations connected together through some form of cabling (Figure 1) to carry data according to a LAN packet transmission protocol, and under the overall control of a LAN Operating System. More advanced LAN architectures may consist of a number of discrete LANs, connected via a router or bridge to other LANs.

Servers

104. There are a range of server types that can be incorporated into a LAN, either individually hosted on their own server computer or, more commonly, running as applications on a shared host computer. The basic types of LAN server are:

a. **File Server**. This form of server provides access to files on the server from workstations, with a workstation seeing part of the file server as one or more PC pseudo-disk drives, e.g., the workstation PC may be configured with a C: local disk and have access to a file server drive as D:. File server drives operate at the application level as if they were local drives.

b. **Mail Server**. A Mail Server provides an electronic post box and message store into which electronic mail can be directed and held until called for by a user operating at a LAN workstation. The Mail Server is not seen at the DOS/Windows level, but only through access from a workstation mail package.

c. **Communications Server**. The Communications Server is used to provide a central modem resource that a user on a LAN workstation can access for dial out services. This type of server allows for centralised control over dial-out services, and through sharing avoids the requirement for a modem at each workstation.

d. **Print Server**. The Print Server is used to connect printers onto the LAN and allow shared use by LAN workstations. The LAN Operating System allows local printer output ports to be mapped to network connections for remote printing across the LAN. This facility allows a number of different types of printers to be connected to the LAN and printers to be shared to reduce hardware costs. Many users utilising the same printer can justify the cost of high quality, fast printers.

Workstations

105. Any form of desktop computer can be connected to a LAN for use as a workstation. The primary workstation type, and the workstation type focused on in this publication, is the Microsoft Windows based IBM-compatible PC. There are a smaller number of LANs in Government which also connect Macintosh and SUN UNIX workstations. The security aspects of these workstations are not specifically discussed, but much of the doctrine provided in this publication also applies to such systems. Workstations can be installed in one of two main ways: as diskless workstations which contain a special chip known as the Boot-PROM which allows the workstation to start up without a local disk; or fully configured workstations which start up from their own hard disk. The workstation requires, in addition to its normal DOS and/or Windows software, a special LAN operating system module to allow connection to LAN resources.

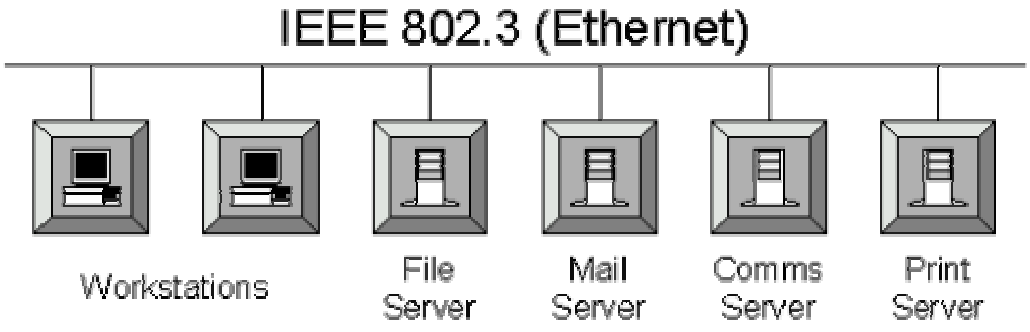

Figure 1: Basic LAN Architectural Components

Configurations, Cabling, and Protocols

106. LAN components can be connected together using a variety of metal cabling (thinnet, thicknet, coaxial, and shielded or unshielded twisted pair), fibre or wireless cabling, and can be connected in a star, ring, or bus configuration (the recommended LAN architecture shown later in Figure 5 shows a star configuration). Figure 2 shows a comparison of the three topologies.

107. A star topology, as the name implies, is a physical star with all workstations and servers attached to a network hub which is the center of the star. All traffic passes through the center no matter which two network devices are communicating. The characteristics of a star topology are:

a. Adding another node to the network is easier because all that is needed is another cable run from the new workstation to the hub.

b. Cable problems have a lesser impact on network operations because the only workstation affected is the one attached to the faulty cable segment.

c. It is easier to determine cable problems in the network because all cables terminate at the hub.

d. More cable is required to cover the same physical space or number of workstations because each cable run goes from the workstation all the way back to the hub.

e. The hub is potentially a single point of failure for the network.

108. With a ring topology, several workstations and servers are connected to a single cable that forms a continuous ring. All traffic travels the same direction on the ring and passes through each node. Each node acts as a repeater for traffic on the network. The characteristics of a ring topology are:

a. Less cable is required because cable is only installed from node to node.

b. No space is required for a central hub.

c. A failure (or loss of power) of any node will cause a failure of the entire network because all traffic passes through and is repeated by each node.

d. Problem determination is harder because each node and cable segment must be inspected independently to determine the failed component.

e. Changes to the network, such as adding another node, also require the entire network to shut down because the ring must be broken.

109. A bus topology also employs a single cable that all nodes are attached to. The characteristics of this topology are:

a. The cable is terminated at each end.

b. Traffic travels both directions from the sending node and is removed from the network when it reaches either end of the cable.

c. A node taps on to the network rather than becoming part of the physical connection between its adjacent nodes. Therefore, the failure of a single node does not cause the entire network to fail.

d. This topology often requires the least amount of cable because the cable is installed from node to node, and the cable does not double back to form a ring.

e. The bus topology is a simple, reliable architecture.

f. This topology can be easily extended to include more nodes.

g. It is difficult to locate problems as the whole cable must be inspected.

110. Because of the advantages of the star topology for problem determination, repair, and flexibility, hybrid topologies have been developed. These hybrid topologies combine the advantages of star topology wiring with advantages of ring and bus topologies. They are the star-wired ring and the distributed star, or tree. In each of these cases, the physical topology is a star. Using the star-wired ring topology, the network hub simulates a ring with very long connections to the attached nodes. In the case of the distributed star, the cables that emanate from the hub are bus topology segments and the hub also acts as a bridge between the buses.

Issue	Bus	Ring	Star
Network	small	small, fast	multimedia
Complexity	low	moderate	moderate
Performance under load	moderate	moderate	excellent
Overhead	low	medium	high
Impact of Workstation failure	none	disruptive	none
Expandability	easy	disruptive	limited

Figure 2: A Comparison of LAN Topologies

111. LANs use a packet broadcast transmission protocol, i.e., a packet is sent to all stations on the LAN with the expectation that all but the station which is in the packet address field will ignore the packet. The most commonly adopted LAN transmission protocol is specified in the IEEE 802.3 standard issued by the Institute of Electrical and Electronic Engineers, and is commonly seen implemented as the Ethernet system. Ethernet can operate on several cable types, each with its own advantages, disadvantages, and technical limitations. A comparison of cable types is given in Figure 3. The common cable types are as follows:

a. Thinnet (IEEE 802.3 10Base2). 10Base2 defines a baseband cable plant capable of transmitting information at 10MB/sec. for 200 meters before requiring regeneration. 10Base2 uses thinnet coaxial cable, a 0.2" diameter cable also know as RG-58 A/U.

b. Thicknet (IEEE 802.3 10Base5). 10Base5 defines a baseband cable plant capable of transmitting information at 10MB/sec. for 500 meters before requiring regeneration. 10Base5 uses thicknet coaxial cable, a 0.4" diameter cable.

c. Unshielded twisted-pair (UTP) (IEEE 802.3 10BaseT). 10BaseT defines a baseband cable plant capable of transmitting information at 10MB/sec. using (UTP) cable.

112. Optical fibre is the newest medium in the commercial LAN market and has the greatest potential as a transmission medium. Many types of fibre optic cable are available (e.g., single mode, multimode), providing varying bandwidths and transmission speeds. The components for fibre optic cabling, such as optoelectronics and connectors, are relatively expensive although the emergence of plastic optical fibre, which is easier to install and maintain than glass fibre, is helping reduce costs. The principal advantages of fibre optics with present-day transmission technology are its high bandwidth, sturdiness, and security. Optical fibre is immune to both physical and electrical influence from the environment. Copper corrodes; glass and plastic do not. Copper conducts electricity; glass and plastic do not. Fibre optic cable is difficult to tap surreptitiously; with current technology, breaks and significant movement in a fibre optic cable can be isolated to within a single inch over a mile or more of cable.

Issue	Twisted Pair	Coaxial	Fibre
Overall cost	low	medium	high
Installation	easy	hard	very hard
Bandwidth	low	medium	high
Interference	susceptible	susceptible	not susceptible
Wire tap	easy	moderate	hard

Figure 3: A Comparison of Cable Media

113. Three additional protocols exist, but are less commonly encountered: MAP/TOP (IEEE 802.4), ARCNET, and Token Ring (IEEE 802.5). General Motors' implementation of the Manufacturing Automation Protocol (MAP) using the IEEE 802.4 access method supports a transfer rate of 10MB/sec over broadband cable, but there is also a specification for achieving 5MB/sec over shorter distances using a less expensive medium. Arcnet architecture (similar to IEEE 802.4) specifies token passing on a broadband bus, but Arcnet uses baseband technology. It has a data transfer rate of 2.5MB/sec and uses RG-62

coaxial cable. There are two versions of token ring LANs: one operates at 4MB/sec and the other at 16MB/sec. Both versions can use UTP cable for the transmission medium. They can also use shielded twisted-pair (STP) cable, which offers improved reliability and greater signal distances. IBM has also developed a number of cable types for building wiring, many of which can be used with token-ring LANs. Token ring supports IBM type 1, IBM type 2, IBM type 3, IBM type 6, and IBM type 9 cable.

Wireless LANs

114. Wireless LANs are gaining prominence because of the projected increase in all mobile communication systems generally and are likely to be particularly popular for use in buildings where the infrastructure precludes the use of cabling systems, where the physical locations of workstations frequently change, and where new users are often added to the network. The main advantage of a Wireless LAN is that the entire installation is portable and once a network has been moved a couple of times the user may well have recouped the initial outlay. There are three types of wireless LAN transmission media: spread spectrum technology, microwave, and infra-red. The first two employ electromagnetic wavelengths around the radio area, and infra-red employs electromagnetic wavelengths at just outside those detected by human vision:

a. Spread Spectrum. Spread spectrum technology, the most widely adopted wireless technology for wireless LANs, employs a technique in which the signal carrying the data is propagated over a broadband. Spread Spectrum is capable of transmitting over a range of 100 to 800 feet. Although not dependent on ''line of sight,'' obstacles between signal source and target do limit range. The data transmission rate using this technique is fairly low, typically about 2M bps.

b. Microwave. Microwave is also not restricted by a ''line of sight'' requirement between signal source and target. The rate of transmission that can be obtained by this method-in excess of 10M bps-puts it in the Ethernet class.

c Infra-red. Infra-red relies totally on ''line of sight'' for successful transmission and the positioning of workstations in relation to the base unit must be carefully planned.

115. The advantages of wireless LANs lie in technological convenience rather than any saving in costs. Although a completely cableless scenario does represent a cost saving, the initial expense of wireless LAN equipment can offset this saving. A wireless LAN offers the added advantage of physical portability, not available to a conventional cabled LAN. For example, moving networks or network components from one office to another is simplified.

Access Methods

116. The access method is the set of rules the workstations and servers use to put traffic onto the network and to retrieve traffic from the network. This is referred to as the media access method (MAC) because it describes accessing the physical media. The two primary LAN access methods are CSMA/CD and Token Passing. A comparison of these two protocols is provided in Figure 4.

117. CSMA/CD. In a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) network, every node monitors the network media, ''listening'' for traffic. If no traffic is detected for a predetermined length of time (which varies by network node), the node may transmit traffic onto the network. The sending node continues to monitor the network media, and if it determines that its transmission has collided with another node's transmission, both nodes wait their predetermined lengths of time and try to retransmit. Ethernet is an implementation of CSMA/CD. It is similar to, but varies subtly from, the IEEE 802.3 CSMA/CD definition. The Ethernet architecture is a joint vendor standard developed by Digital, Intel Corp., and Xerox Corp. Ethernet is the most commonly used LAN communications architecture for communications between workstations and servers. This is the preferred architecture for the scientific and engineering communities and is increasingly popular in the business environment as well. Ethernet is a good choice for networks that support ''bursty'' traffic-characterised by occasional bursts of heavy traffic. It is less appropriate for networks that support constant moderate or heavy traffic. Ethernet will support Transmission Control Protocol/Internet Protocol (TCP/IP), the communications protocol that is the standard for communicating among workstations and servers under the control of the UNIX operating system.

118. Token Passing. Token ring networks use a transmission protocol based on the concept of tokens. In these networks, only one node (the one with the token) is allowed to transmit at a time. The token travels around the network giving each node its opportunity to seize the token and transmit. When a node transmits, the token carries the message to the receiver, then returns to the sender to confirm delivery of the message. At this point, the token continues to travel around the network to offer the next node the opportunity to transmit. MAP/TOP is also a token-passing access method.

Issue	CSMA/CD	Token
Message length	short	moderate-long
Traffic volume	low	high
LAN length	short to avoid collisions	limited by media
Performance	poor under high load	excellent
Packet overhead	high	high
Access delay	moderate-long	moderate
Impact of station	none	disruptive

failure		

Figure 4: Protocol Comparison

Transport Protocols

119. There are four commonly encountered higher-layer packet transport protocols which are used on local area networks. These are NETBIOS, TCP/IP, Appletalk, and IPX.

120. **NETBIOS**. NETBIOS is a low level protocol standards originally introduced by IBM in 1985 with the early PC LAN systems. It was designed to provide a small and efficient protocol stack optimised for use on departmental LANs. It provides for only local communications, and requires gateways for connection to external hosts. NETBIOS sits above the NETBUI protocols, which themselves sit on top of the Network Device Interface Specification (NDIS) lower layer protocol. NETBUI implements the NETBIOS v3.0 name, session and datagram command support.

121. **TCP/IP**. The Transmission Control Protocol/Internet Protocol (TCP/IP) was developed in the 1970s by the Department of Defense's (DOD's) Defense Advanced Research Projects Agency (DARPA). TCP/IP is the standard for wide area networking, and has been popularised through its use in the Internet. Many companies support the use of TCP/IP protocols in their local area networks to allow direct desktop-Internet connectivity.

122. **AppleTalk**. This is a proprietary protocol specific to Apple networks that is simple and is supported automatically in every Macintosh computer. AppleTalk uses both open and proprietary protocols to communicate among the seven layers of the OSI model. It is a popular architecture; in 1992 there were more than 2 million AppleTalk nodes installed on more than 250,000 networks.

123. **IPX**. Novell provides a proprietary Internetwork Packet Exchange (IPX) protocol, originally derived from the Xerox XNS protocol, as its native protocol for NetWare LANs. The use of IPX protocols is necessary to allow advanced features of NetWare, such as System Fault Tolerance (SFT-III), to be used. This is also sometimes referred to as Internet Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

LAN Interconnectivity

124. LANs provide the means to connect a number of devices together. However, it is also necessary sometimes to connect LANs or LAN segments together, which may also involve interconnection of different communications architectures. There are four principle technologies used to connect LANs together, the choice of which to use depending upon the differences in the architectures being connected: Repeaters, Bridges, Routers, and Gateways.

125. **Repeater**. A repeater is used to boost the signal of the traffic on the network and to connect network segments of the same architecture. A repeater works at layer 1 of the OSI Reference Model, the physical layer, and therefore requires the connected networks to use the same communications protocol, the same logical link control, and the same media access control. A repeater passes every message from the originator's network segment to the other segment, and vice versa (even if the recipient is on the same network).

126. **Bridge**. A bridge is used to connect networks which have different architectures. It operates at layer 2, the data link layer and is protocol independent. The bridge is able to receive packets on either network and transmit them into the other. In addition, it regenerates the signal when it moves packets between networks. Bridges need to learn about the devices that are on each of their two networks and can then determine (by monitoring the addressing information in the data packets) whether a message requires transmission to the other network and operates, therefore, as a packet filter to reduce the amount of traffic transmitted between networks. Multiple levels of bridging can be implemented, but each bridge must know about all devices in all the network, not just those on the networks directly connected to the bridge. Bridges can be local or remote, where local bridging consists of multiple networks connected to the same bridge. Remote bridging consists of multiple networks, each connected to a bridge which are in turn connected to each other across a WAN. There can be only one path between any two bridges, because multiple connections could result in duplicate messages or messages being received out of sequence.

127. **Router**. Routers operate at layer 3, the network layer. The communications protocol must be the same on both sides of the router, but lower layers (layer 2, the data link layer, and layer 1, the physical layer) can be different. The principal difference between routing bridges and routers is that the router is actually an intermediate destination of the message with a responsibility to determine the destination address of the next router in the path and replace its own address with that of the next router, and as a result, there can be multiple paths between routers for greater network reliability. There are two methods for determining the next node to receive the message: transparent routing and source routing. Transparent routing implies that routers dynamically establish the location of destinations. Source routing is used primarily in token-ring networks and requires that the routing information (not just the destination address information) is included in the packet. In a source routing network, each network node (workstation or server) is required to learn about the entire network and paths. This creates overhead on the network node and on the network, but source routing can be more efficient because a sending node will choose the most efficient route for its messages. As the standards for layer 3 are more immature than those for layer 1 and layer 2, network designers and installers selecting routers must ensure compatibility with other network components.

128. **Brouter**. Bridge/Routers (Brouters) provide both a routing and a bridging service. Bridging of source route messages is more efficient than transparent routing because the bridge does not have to determine the routing information.

129. **Gateway**. Gateways are used to connect networks that may have different architectures. For example, they are used primarily for connecting Ethernet or AppleTalk LANs to the installed base of IBM SNA architecture networks and mainframes or to connect IBM Token-Ring or AppleTalk LANs to Digital VAX clusters and DECNet networks. Gateways provide translation and conversion and can function at any or all of the seven layers of the OSI reference model. Many different protocols can be used at any or all layers. A gateway contains complete communications protocols stacks for the two environments that are being connected along with a custom application layer program to convert from one communications stack to the other. The advantage of the use of gateways is that systems with different architectures can communicate with each other without changing the technology of the communicating systems. The disadvantages to the use of gateways is the additional overhead that is placed on messages moving from one architecture to the other, and the fact that not all features of one of the architectures are necessarily present on the other architecture.

Concentrators and Hubs

130. The increasing use of star configurations has led to a high growth in the deployment of hubs. Formerly classified as media products, hubs have evolved from simple wiring concentrators used for basic cable management into sophisticated communications frameworks. Hub functions now include bridging and routing, and they can act as a central, intelligent, and possibly security, device at the center of a network which may be made up of Token-Ring as well as Ethernet circuits. Hubs today can often accept varying media, with the most important market at the moment being for 10BASE-T connection.

131. One of the significant features offered by some hubs is the facility to replace the data in some packets as they are being broadcast through the hub (see paragraph 409), providing one of the more important LAN security countermeasures.

Interface Cards and Transceivers

132. The most common interface between a PC and the network's transmission cable is a network interface card. These printed circuit boards fit inside a PC cabinet, generally into an accessory expansion slot on the motherboard. The transmission cable will usually attach directly to the card, or a short drop to the main cable might be used. The major consideration when installing an interface card is whether the PC power supply can handle the extra load, the interrupt addresses currently being used, and the number of direct memory access (DMA) channels already in use.

133. Stand alone network transceivers may be required in addition to network interface cards. For example, ''thick'' Ethernet LANs that use heavily shielded coaxial cable generally require a special transceiver to link a PC to the LAN. Thin cable interfaces are usually made directly to the interface card, using

''T'' and/or barrel coax connectors. Transceivers are also available to connect interface cards designed for one type of media to a different type (e.g., coaxial to unshielded twisted pair).

Network Operating Systems.

134. While there are a number of network operating systems (NOSs) currently available, the two that are used most widely in Government are Novell NetWare and Microsoft Networks (which has evolved from the IBM LAN Manager product). While the NetWare has traditionally been the most popular NOS in Government, the increasing deployment of Windows-NT servers is causing a significant shift towards Microsoft Networks. These two operating systems are discussed in more detail in Chapter 2.

Alternative Networking Architectures

135. Sun's NFS is a de facto standard mechanism for sharing files among network devices attached to a SUN workstation network operating TCP/IP protocols. Under Sun's NFS, a user can make any network-attached device either a client or a server by issuing the appropriate commands or system calls. The NFS protocol has knowledge of the locations of all mounted file systems and all clients have access to all mounted file systems. A client can issue UNIX I/O commands against these files without having to know where the file system physically resides.

136. Sun's NFS takes advantage of another Sun de facto standard, Remote Program Calls (RPC). Sun's RPC provides a standard way for programs running under the control of different operating systems to request services of each other without having to adhere to the unique call processing of the different operating systems. When a client requests a service, Sun's RPC on the client translates a request into the standard format and sends it across the network. Sun's RPC on the server translates the request into a format understood by the receiving operating system and delivers it to the requested service. When the requested service is complete, Sun's RPC on the server converts the response to the standard format and sends it back across the network. Sun's RPC on the client translates the response into the format understood by the client.

137. These services and protocols have gained wide acceptance because they are freely available in the public domain. Source code for them can also be licensed from a number of sources. It is estimated that more than a million computers now run TCP/IP with these value-added services. While much of the advice regarding Local Area Network threats and vulnerabilities provided in this publication is relevant, specific advice on UNIX networking is addressed as part of UNIX security.

LAN Security

138. Effective LAN security is achieved through correct management policies and procedures, and the proper design and administration of security mechanisms to ensure that:

a. the LAN's hardware and operating system integrity is maintained;

b. data stored, processed or transmitted on a LAN is protected from interception;

c. data is not inserted into the LAN covertly;

d. data stored, processed or transmitted on a LAN is protected from unauthorised deletion and modification;

e. the LAN service is maintained; and

f. the identity of the sender and receiver of a message can be authenticated.

139. Effective LAN security requires the proper combination of security policies and procedures, technical controls, user training and awareness, and contingency planning. A formal security policy governing the use of LANs should be in place to articulate Executive requirements for the protection of the LAN itself and the information transmitted across it. A security policy is a concise statement which identifies critical information, establishes the responsibility for protecting information, and states the organisational commitment to IT security. In particular, the LAN security policy should stress the importance of, and provide support for, LAN management. Further information relating to security policies is provided in NZSIT 101: Information Technology Security Policy Handbook.

140. Effective LAN management requires an adequate level of funding and staff resources. Lack of user awareness regarding the security of the LAN can increase risk to LAN-borne information. Users who are not familiar with the security mechanisms may use them improperly and inadvertently compromise security. Users must be given the proper guidance and training necessary to maintain an acceptable level of protection in the LAN environment.

CHAPTER 2

NETWORK OPERATING SYSTEMS

Novell NetWare

201. Novell NetWare is a multi-tasking, server-based network operating system that supports all the major network configurations and transport protocols. Of particular importance in NetWare networks is Novell's own Internetwork Packet Exchange (IPX) protocol, originally derived from the Xerox XNS protocol.

202. Novell has optimised NetWare for use as a server operating system by incorporating many design features traditionally associated with larger computing environments. It is built around a multi-tasking kernel capable of supporting the demands of multi-user network operation and uses a method of driving the disk read head called ''elevator seeking'' that assigns priority to read requests based on the current position of the read head, to minimise head movement and provide the fastest response. It also uses disk caching in which frequently accessed data is kept in RAM on the server, and also employs a ''read-ahead'' capability that caches data in anticipation of future read requests. A background write scheme allows disk writes to take place when no other disk activity is in process, thus speeding read access times. NetWare can also address multiple hard disk channels simultaneously, so that several reads can take place at once. File Allocation Tables (FATs) for files larger than 2MB are indexed by NetWare to reduce search time.

203. NetWare uses several methods to ensure the reliability of disk operations. Read-after-write verification, duplication of directory structures and FATs, and Hot Fix disk error correction are standard, while System Fault-Tolerant (SFT) features, such as disk mirroring and a Transaction Tracking System (TTS) rollback capability, can be implemented at the network builder's discretion in NetWare 4.0 deployments.

204. NetWare security is implemented at several levels-password, account, file, directory, and internetwork security are all provided. System administrators set up user profiles that specify resources and rights available to each user, as well as dates, times, and locations from which a user can log on. Passwords are encrypted before they pass over the network cabling and are stored on the server in encrypted format. Security features are supported for all client workstations regardless of whether their native operating system is DOS, Windows, OS/2, or UNIX.

NetWare 3.11

205. Early in 1991, Novell launched a new version of its high-end product, originally called NetWare 386 but later renamed to NetWare Version 3.11. NetWare 3.11 is a 32-bit multi-tasking operating system designed for Intel 80386- and 80486-based hardware platforms.

206. NetWare v3.11 is built around a central kernel called the System Executive. All network services, server-based applications, and server utilities are implemented as modules that can be added to or removed from the system without bringing the server down. These NetWare Loadable Modules (NLMs) access system functions using the C-Library (CLIB). The OS/2 File Requester, the NetWare Print Server, and MHS store-and-forward message services are supplied with NetWare v3.11, and additional NLMs are available for Apple Macintosh connectivity, Network File System (NFS), and OSI FTAM file transfer. Access to CLIB function calls allows third-party vendors to offer NLMs for their own server-based applications such as database management systems.

207. A major vulnerability in NetWare 3.11 was highlighted in 1993 with the publication of the details of an attack on the login authentication exchange which allowed a user to gain supervisor privileges. This resulted in the emergency release of the NetWare 3.12 upgrade.

Netware 3.12

208. NetWare 3.12, a minor upgrade applied as a patch to NetWare 3.11, has been released. The most significant change provided by this patch is the use of encryption to protect passwords in transmission as users are logging into the network.

NetWare 4.0

209. NetWare is available for a wide range of hardware and software environments, including DOS, Windows, OS/2, Macintosh, and some variants of UNIX. There are ''native'' versions of NetWare for both the Sun SPARC and the Hewlett-Packard PA-RISC processors.

210. The Directory Service is a feature of Novell NetWare 4.0 that is designed to enable both network managers and users to have access to all the data, resources, and services that they need without having to worry about where on the network they are located. The user will have a single login that, subject to the usual security clearance, will enable him to locate and access those services that he requires. The administrator can now accomplish tasks such as transferring a user's access rights, together with his data if necessary, from one location to another in one operation.

211. Data compression and archiving facilities are available to reduce the amount of server space taken up by old files. Files unused for a pre-defined period may be compressed and then, after a further pre-defined period, be automatically archived to tape or CD-ROM.

212. NetWare 4.0 includes advanced SFT integration and full mirroring of one server to another. SFT is used to maintain network services whatever faults may develop on the fileservers using an independent secondary server that is ready to replace the primary server at a moment's notice. To achieve this mirroring, the NetWare fileserver is split into several components, on the one hand those that make no direct hardware calls and on the other those that are tightly linked to the server itself. SFT is supported only for IPX/SPX running on DOS or OS/2 clients.

NetWare Lite

213. NetWare Lite provides a low-cost, simple, peer-to-peer network, where each workstation on the network can be designated as client or server, or both

at once, obviating the need for a dedicated fileserver. NetWare Lite can run as a NetWare client and be fully integrated with NetWare services. Few NetWare Lite systems exist within Government.

Microsoft Networks

214. The flagship Microsoft Networks operating system incorporated into Windows NT provides a LAN Manager style networking operating environment suited to local area networks of all sizes. The Windows Network Administration program gives administrators a unified tool for managing multiple servers from a Windows desktop, and Windows Network Application Starter enables users who have no network knowledge to run applications off the network and configure Windows desktops for their users. Microsoft Networks' support for running multiple server applications, either on a single server platform or on multiple servers, is among the strongest of the most prominent network operating systems. Access to Microsoft Networks requires entry of a userid/password. User-level security allows access rights to individual user accounts of read, write, create, delete, execute, change permissions, and change attributes for files and directories. Share-level security allows users without an account to access network resources via password. Administrators can set valid logon times, valid workstations, mandatory periodic password changes, account expiration dates, and group memberships.

215. At a lower level, the Windows for Workgroups peer-to-peer networking system runs as a Microsoft Networks client and provides built-in networking functionality for a small number of users, and is scalable through interconnection of workgroups. Compared with other peer-to-peer networks, Windows for Workgroups offers a very limited choice of security settings. There are only two levels of file access-full access and read-only-with or without passwords. Beyond giving selected individuals passwords for file access, there is no scope for assigning different access privileges to different users or groups of users.

216. Microsoft, in conjunction with Sybase and Digital Communications Associates (DCA), has also brought to market a pair of major client/server applications that run on Microsoft Networks. The Microsoft SQL Server is a database server for PC networks, used to control mission critical data and enable users to access the database; the DCA/Microsoft Communications Server ensures connectivity between LANs and host and peer computers.

Other LAN Operating Systems

217. There are many other LAN Operating systems currently in use, although they are unlikely to maintain any significant market presence in the future. These include the Banyan VINES LAN, LANTASTIC, and OS/2 LAN Manager.

CHAPTER 3

LAN THREATS AND VULNERABILITIES

Terminology

301. For a LAN to be configured to provide an adequate level of protection for the information it processes, the threats under which the LAN operates must be understood. In this context, a threat is a general type of event which, if realised as an incident, could potentially cause damage to the LAN. Threats can be malicious, such as the intentional modification of sensitive information, or can be accidental, such as an error in a calculation or the accidental deletion of a file. Threats can also be acts of nature such as flooding, wind, lightning, and earthquake. The damage caused by the occurrence of a threat event is referred to as its impact.

302. Threats on their own do not result in security risks. Threats have to be associated with a vulnerability in order to be effective. Vulnerabilities are weaknesses that are exploited during an incident which results in some security-relevant impact on the LAN. For example, unauthorised access to a LAN could occur by an outsider guessing an obvious password, i.e., exploiting the poor password choice - a vulnerability - by a user. Reducing or eliminating the vulnerabilities of the LAN will reduce or eliminate the associated threats to the LAN. For example, a software module or procedure which helps users choose robust passwords will reduce the incidence of poor passwords, and thus reduce the threat of unauthorised LAN access. This module or procedure is commonly known as a security countermeasure.

303. A security service is the collection of security mechanisms, supporting data files, and procedures that help protect the LAN from specific threats. Typical LAN security services include identification and authentication, access control, and audit. Security mechanisms are the technical controls used to implement security services. For example, a token based authentication system (which requires that the user be in possession of a required token) is a mechanism which can be used to implement an identification and authentication service, to protect against unauthorised LAN access.

304. The specific threats and vulnerabilities associated with generic LANs are discussed in the remainder of this Chapter.

Unauthorised LAN Access

305. One of the major functions of a LAN is to provide access to shared resources. It is necessary to control and account for the use of the resources as unauthorised LAN access can result in a variety of impacts such as denied or reduced resources available to legitimate users and unauthorised disclosure of material. Unauthorised LAN access is, by itself, a form of electronic trespass which often allows other threats to be realised. The common methods used to gain unauthorised access are as follows:

a. Password sharing allows an unauthorised user to have the LAN access and privileges of a legitimate user; with the legitimate user's knowledge and acceptance.

b. Password guessing can be achieved in a number of ways, and includes the problem of passwords being written down in diaries or on Post-It stickers and left by the workstation. Other guessing attacks include automated access attempts using a database of common userid/password combinations or automated password generation software. Knowledge of individuals also assists if personal details have been used as the basis for the password. Access to the LAN through dial-in modems provides an attractive vector for launching password guessing attacks.

c. Password capturing is a process in which a legitimate user unknowingly reveals their userid and password. This may be done through the use of a trojan horse program that appears to the user as a legitimate login program but is a 'front-end' process which copies passwords. Password may also be captured through the use of malicious software operating as a Terminate-and Stay-Resident (TSR) program. Such software may be put into the terminal as a virus-like program or by access to unattended workstations.

d. Password interception may occur during the login process if the login exchange is transmitted across the LAN in an unencrypted form. Data transmitted across the LAN, including userid/passwords during login, is broadcast to all workstations and may be read at any workstation by the use of a sniffer program. Interception can occur through connection of a rogue workstation onto the LAN through a standard, accessible connection point, wiretap into the LAN cabling, or TEMPEST attack on electro-magnetic radiation emitted from any of the LAN components.

e. Opportunity access to a LAN may occur if an attacker gains physical access to a workstation on a LAN in which identification and authentication is not enforced, or to an unattended terminal that has been left logged in. This is also of particular concern if LAN password are stored in batch files and allow automated login.

f. Known system holes and vulnerabilities that have not been patched can be exploited if access to an unattended terminal is possible.

Unauthorised Use of LAN Resources

306. A LAN allows multiple users access to shared resources. However, access to some resources may be restricted, for security reasons, to limit cost, or to ensure proper utilisation of a limited resource. This requires discretionary access controls to be applied to each of the LAN resources.

307. Unauthorised use occurs when a user, legitimate or unauthorised, accesses a resource that he or she is not permitted to use. It may occur simply because the access rights assigned to the resource are not assigned properly, or because the access control mechanism does not provide a fine enough

distinction between various resources. It may also occur if a security hole exists and has been exploited.

Unauthorised Disclosure of Information

308. One of the major uses of discretionary access controls on a LAN is to provide control over access to the information held on the LAN servers. Authorised LAN users generally have full access to only some of the information on their LAN file or mail server, and all LANs offer protection for information on a need-to-know basis. Disclosure can occur if an authorised user releases material to an unauthorised third party - but this is a personnel security issue, not a LAN security issue. Unauthorised disclosure from a LAN security perspective occurs as a result of an unauthorised individual gaining access to the LAN or directly to information that is not encrypted on magnetic media, screens, or print-outs. This occurs through the following vulnerabilities:

a. improper access control settings, which allow unauthorised access to information by an authorised user or an interloper;

b. physical access to the server which may enable scavenging of information;

c. oversight of monitors due to bad positioning near windows or in or high traffic areas;

d. theft or oversight of printout due to print servers located in unprotected or high traffic areas;

e. theft of backup media stored in accessible areas; and

f. EMR interception of information processed by the system, in particular that displayed on screens.

309. Disclosure can also occur if LAN traffic is compromised through listening and capturing traffic transmitted over the LAN transport media, either by tapping into an accessible network cable or carrying out a network sniffing attack from a LAN workstation. Such sniffing programs are readily available, simple to use, and undetectable. They exploit the vulnerability of the LAN transmission broadcast protocol and are the single most serious attack on LAN systems.

Unauthorised Modification of Data and Software

310. Unauthorised modification of data or software occurs when unauthorised changes (additions, deletions or modifications) are made to a file or program. Undetected modifications may result in corrupt databases, incorrect spreadsheet calculations, system instability, and various other impacts. 311 Unauthorised changes can be made in simple command programs such as batch files or JAVA scripts, in utility programs used on multi-user

systems, in major application programs, or any other type of software. They can be made by unauthorised outsiders, users authorised to use the system, and even administrators authorised to make software changes but not this particular change. Unauthorised software changes can be the means of launching attacks in any one of the other threat categories. The most common unauthorised software change is the PC virus. Virus attack generally use networks as a host and infection vector to attack workstation PCs rather than attacking the LAN servers.

312. The unauthorised modification of data and software can occur when write/update permission is granted to users who are only authorised to have read privileges. It can also occur if malicious software is able to enter the LAN, directly via the central LAN administration point, from a communications connection, or via a user workstation.

Spoofing of LAN Traffic

313. Messages transmitted across LANs contain sender and recipient addressing information. LAN users can be fooled into thinking information came from other than the sender through an attacker modifying the originating address information. Messages can also be diverted or copied and sent to an unauthorised recipient if the packet destination address can be modified. This is a significant problem, as an attacker on a workstation external to the LAN, who therefore cannot attack the LAN directly through sniffing, can use a malicious modification program that has been inserted into a workstation on the network to be a vector for extracting data from the LAN. LAN protocols do not provide any form of authentication of addresses.

Specific LAN Component Vulnerabilities

314. In addition to the general vulnerabilities discussed above, there are a number of specific vulnerabilities associated with each of the components of a LAN system:

a. **LAN Servers.** LAN servers are as vulnerable to attack, natural disaster, or accident as any computer device. In particular, the disk subsystems on file and mail servers are as vulnerable to scavenging as any PC disk and require the same cryptographic protection or physical containment.

b. **LAN workstations.** LAN workstations are often fully fledged PCs with all the vulnerabilities common to that technology (see NZSIT 200: PC Security). In particular, LAN workstations having floppy disk drives allow malicious software to be introduced onto the LAN and sensitive data to be extracted from it. Users may install modems in their workstations without authorisation, and lead to external exposure of the LAN. LAN workstations can also be used to mount sniffer attacks, whereby a workstation intercepts data being broadcast across the LAN regardless of whether it is for that particular station (this is a

well known attack on LANs and there is a wealth of public domain sniffer software).

c. **Cabling.** There are three main vulnerabilities to cabling: tapping to intercept information; cutting the cabling to disrupt communications; and intercepting compromising emanations from the cable, through electromagnetic radiation or crosstalk. The various types of cabling are more or less susceptible to these vulnerabilities. Fibre cabling, in particular, has a low vulnerability to interception and compromising emanations, while wireless LANs are highly vulnerable to interception.

d. **Bridges, Routers.** The major vulnerability of bridges and routers is their subversion through remote re-configuration in such a way as to allow unauthorised access into the LAN.

e. **Hubs.** The major vulnerability affecting hubs is the potential for physical access to the hub allowing additional, unauthorised connections to be made.

f. **Network Interface Cards.** The major vulnerability associated with interface cards is their potential for emitting compromising emanations. This is particularly the case with some fibre interface cards, due to the circuitry used to covert optical signals to electrical form.

g. **LAN Operating Systems.** LAN Operating Systems have all the common vulnerabilities associated with any multi-user operating system. Of particular relevance to any LAN security review is:

(i) the strength of their user authentication and discretionary access mechanisms,

(ii) the protection provided to their security subsystems (in particular the password files), and

(iii) residual information from previous users' activity being recoverable from disk.

315. There are other LAN vulnerabilities which occur, often taking advantage of security flaws in the LAN login or management protocols. For instance, in the supposedly secure NetWare 3.12 login, the three-phase login establishment protocol can be interrupted and hijacked by another workstation on the network, which subsequently gains access to the LAN in a masquerade of the original workstation. As such attacks are specific to LAN configurations and are identified on a regular basis, the GCSB should be consulted at the LAN design stage to advise on currently known vulnerabilities of the planned architecture.

CHAPTER 4

SECURITY SERVICES AND MECHANISMS

General

401. One of the major cost-effective security countermeasures that can be adopted for most departmental LANs is the physical protection of the LAN servers, hubs, routers, bridges, and cabling. An access controlled or lockable room or vault within departmental premises provides an adequate level of physical protection for LANs processing unclassified and unclassified but sensitive material. See Chapter 7 for special considerations in the use of LANs for processing classified information.

IEEE 802.10

402. A security service is the collection of mechanisms, procedures and other controls that are implemented to help reduce the risk associated with threat. The international standard providing guidance on LAN security is IEEE 802.10: Interoperable LAN/MAN Security (SILS) which provides security specifications for IEEE 802 local and metropolitan area networks. This standard provides specifications only for the use of a Secure Data Exchange facility which includes the following security services:

a. data confidentiality, though encipherment of the data packet prior to its broadcast across the LAN;

b. data integrity, through the use of an Integrity Check Value (ICV);

c. data origin authentication, through the use of a station-id in the protected header; and

d. access control, through the use of external key management services.

403. The Secure Data Exchange protocol packet which is sent across the LAN within an Ethernet or other frame is built as follows:

404. The clear header provides a security association identifier and a management defined field which can be used to establish and maintain the cryptographic environment. This would typically involve the use of an external key management system. IEEE 802.10 does not dictate any specific key management or cryptographic algorithms.

Other Security Services

405. SILS provides four basic communication security services. However, LAN management and system designers also need to be concerned about wider

access control, and supporting the requirement for individual accountability. The logging and monitoring security service provides the means to trace LAN usage. This is also important in providing some level of intrusion detection as a second line of defence should access control services be compromised.

406. A further security service, Non-Repudiation, is not considered in the context of LAN security. Non-Repudiation is the security service used in messaging systems, through which the entities involved in a communication cannot deny having participated. Specifically, the sending entity cannot deny having sent a message (non-repudiation with proof of origin) and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery). However, this is usually an application level security service and need not be considered specifically in the context of LAN security.

Data Confidentiality

407. The data confidentiality service is required when there is a threat of interception across LAN cabling or from workstations carrying out a 'sniffer' attack.

408. Protection from this type of attack can be achieved through encryption of the physical communications path (e.g. link encryption), encryption of the virtual path (e.g. VPN), application-level encryption (e.g. S/MIME e-mail or SHTTP), and/or through network routing controls.

409. One of the major vulnerabilities which can breach data confidentiality is the broadcast nature of LAN communications. However, some LAN hubs can provide a packet masking capability, where the data in a packet is overwritten with random information if the packet is being broadcast from the hub to a workstation(s) other than the destination. This is one of the more common methods used to protect against sniffer attacks.

410. Data confidentiality may also be required for some of the more sensitive files held on the file server. This, however, is an application security issue.

Data Integrity

411. The data integrity service is primarily concerned about protecting LAN packet broadcasts from unauthorised modification. An ICV is initially calculated by applying a hashing or cryptographic algorithm to the data. It is then appended to the packet. The packet data is verified by applying the same algorithm to the received data and comparing the new ICV to the one appended to the packet. If the two ICVs are equal, then the data is proved to have been received correctly; if not, an unauthorised modification is assumed. It is usual to protect the ICV in some way, or to use a secret key in the ICV calculation so that an attacker cannot recalculate an ICV for a modified

message. It should be noted that data integrity is an automatic side-effect of data confidentiality.

412. A wider LAN integrity service may also be required in some cases to protect data and software on workstations, file servers, and other LAN components from unauthorised modification. This service can also be provided by the use of hashing or cryptographic checksums at the application level.

Data Origin Authentication

413. The addresses in ethernet packets are not routinely validated and therefore provide no assurance of packet origin. As detailed in the SILS standard, data origin authentication can be easily provided under a secure LAN architecture by including the source address as part of the (encrypted) packet data field.

414. If the data origin authentication service is required in a non-SILS LAN, it must be provided by the use of mechanisms at the application layer.

Access Control

415. The primary means of providing LAN access control is to verify the identities of users through logon to the Network Operating System. This typically involves passing a userid and a password from the workstation to the network operating system server, a process often referred to as the authentication exchange. The userid is then used in subsequent resource control and logging mechanisms to provide further access control and user accountability. More sophisticated authentication mechanisms, as detailed in NZSIT 204: Authentication Mechanisms have yet to emerge as common LAN features.

416. Password based authentication mechanisms are susceptible to the passwords being monitored and captured. This may be avoided if data encipherment is used for the password exchange. While not providing data confidentiality, LANs such as Novell Netware 3.12 and 4.x do provide, as an option, encrypted authentication exchanges. LANs should always be configured to protect against login password sniffing, either by full encipherment, partial encipherment, or hub masking. As with any system, default passwords supplied with the LAN should be changed.

417. As for any system, it is important to protect the security subsystem. The architecture of specific LAN Operating System's security subsystem will differ for each LAN. However, the subsystem will reside on the main LAN Operating System disk, and will contain the security software modules, system security settings, user identifiers and passwords, user privileges, and system accounting and audit data. All these items require protection from user interference. This is normally done through discretionary access controls, with the security components having a higher security level than that allocated to

normal users. However, users do have access to the login subdirectory of the file server prior to their authentication; the contents of this directory should be minimal.

418. Once authenticated, a user will come under discretionary access control within the LAN. These access control mechanisms usually support access rights based on the owner, a specified group of users, or all users to files or directories. Generally, directories can be specified as shared or not. If shared, they appear as separate logical drives. Within these drives, some LANs allow files to be specified as no access, read-only access, read-write access, execute access, update access, and append-only. A LAN operating system may implement user profiles or access control lists to specify access rights for many individual users and many different groups. Using these mechanisms allows more flexibility in granting different access rights to different users to achieve more stringent access control.

419. Privilege mechanisms exist on LANs which can be used to allow authorised users to override access permissions. In all cases, LAN administrators should employ the concept of least privilege, where users are provided with the minimum privileges necessary to carry out their job. Where users require additional privileges occasionally, these should be temporary allocated and removed as soon as they are no longer necessary.

420. In addition to access controls on the LAN, it may be necessary to consider access controls on LAN workstations. Such mechanisms are described in NZSIT 200: PC Security. LAN workstations may also need password-protected timeout mechanisms to protect unattended workstations from unauthorised access.

421. LAN access via modems will certainly require access control - an unlisted telephone number is totally inadequate. It is strongly recommended that token based authentication be used for remote dial-in access in all cases. LAN access via a permanent connection should be controlled through the use of a firewall to allow only the necessary types of protocol packets to be passed through to the LAN to avoid attacks based on some of the unnecessary protocols.

Logging and Monitoring

422. LAN Operating Systems provide the option for logging security-relevant events in an audit file. The type of events that are recorded is usually discretionary, and administrators need to balance the amount of audit information required with the overhead costs of its storage and reduction to meaningful audit information. The audit file provides the basis of the following functions:

a. accounting for LAN resource usage, to support cost recovery and output costing regimes;

b. system performance data, to allow resources to be maintained at the optimum level to increase system availability and responsiveness;

c. detection of unauthorised or unusual activity patterns, to allow a trace back to identify intruders or authorised staff exceeding their privileges.

423. A regular regime of audit file analysis and review should be established.

Intrusion Detection

424. The science of intrusion detection is still in its infancy, and the intrusion detection systems that have been deployed are all prototypes. Nevertheless, some LAN Operating Systems do incorporate simple intrusion detection mechanisms such as real-time alarms for multiple failed logins. These facilities should be activated to provide additional assurance of system integrity. Departments wishing to use more sophisticated intrusion detection should contact the GCSB.

CHAPTER 5

LAN SECURITY ADMINISTRATION

General

501. LAN security cannot be adequately achieved unless the threats have been correctly identified and appropriate countermeasures designed into the LAN. However, even if the LAN is correctly designed, it may still not be secure. The discretionary security controls provided within the Network Operating System need to be correctly set up and monitored throughout the life of the system to ensure that inadvertent vulnerabilities are not introduced. An example of this problem is user accounts not being de-activated when employees leave.

502. A prerequisite for LAN administration is the establishment of a LAN usage and security policy. The issues that need to be addressed include who will have access to the LAN, what the file server directory structure will be, what access controls will be implemented for information stored on the LAN, what access controls will be implemented for shared resources such as facsimile and mail, and the responsibilities for administering and auditing the LAN.

503. Each version of each LAN Operating System implements its discretionary access controls in different ways. This Chapter provides generic advice on LAN administrative requirements, but departmental LAN administrators should contact the GCSB for further advice on their specific LAN system. A summary LAN security checklist is provided at Annex A.

Security Policy Controls

504. A LAN Security Policy needs to address many of the security issues detailed in NZSIT 101: Information Security Policy Makers Handbook. A risk analysis should be carried out to determine the priority for implementation of the controls.

505. The primary consideration will be to decide which users are allowed access to the LAN, and establish a user registration scheme based on user identifiers and passwords (more sophisticated LANs may also allow security tokens such as PC-Cards to be used). Users should be provided with guidance on how to generate good quality passwords and the reasons for protecting them as part of a general LAN security training and awareness programme. Procedures should also be established to ensure that user identifiers are revoked as soon as a user no longer requires access to the LAN.

506. The level of material approved for processing on the LAN should be clearly stated in the policy. The extent of protection provided to material should also be detailed, including any special considerations relating to data privacy or classified information.

507. Procedures for virus checking, and general controls on the introduction of software onto the LAN, should be established. Policy should also be established covering the rules on copying licenced software and sensitive data. In particular, LANs handling classified data should operate under strict data export controls.

508. The LAN policy should also make it clear that LAN traffic monitors/recorders/sniffers may only be used if authorised by the LAN Administrator. Users should be made aware of the disciplinary action that will be taken should they abuse their privileges in this or other ways.

LAN Administration

509. The specific requirements of LAN administration will include monitoring the implementation of the security policy, including regular reviews of security reports, and running the user registration system. The LAN administrator should also ensure that the correct configuration of the security features of the LAN are maintained through regular LAN audits. The LAN administrator is responsible for securing the LAN environment within the site, and ensuring it only has approved interfaces to outside networks.

510. The LAN administrator will be responsible for the installation of all central software on the LAN, and for checking any user software for viruses or other malicious code. A regular data backup regime needs to be implemented, and a plan developed for recovery in the event of a major system outage. The recovery plan may also need to be tested occasionally to prove its workability and to ensure continuing staff familiarisation.

511. One of the important tasks of a LAN administrator is responding to emergency events and providing event notification. This may involve follow up intruder tracing with other LAN and external network administrators.

512. The LAN administrator should develop a LAN usage guideline which advises LAN users on various aspects of secure and responsible behaviour on the LAN, including:

a. reading and understanding the LAN security policies and procedures, particularly relating to data backup regimes;

b. using LAN security features to protect the confidentiality and integrity of their own information;

c. selecting good passwords;

d. ensuring that passwords are not written down or disclosed to others; and

e. notifying the LAN Administrator when a security violation or security system malfunction is noticed and not attempting to exploit such malfunctions.

CHAPTER 6

RECOMMENDED LAN ARCHITECTURE

General

601. There will always be specific considerations in the design of any LAN, and no one LAN architecture can be implemented which will suit all situations. However, in the case of a mid to large sized departmental LAN, there are some basic architectural recommendations which will held improve security and avoid many of the common LAN vulnerabilities. Two such architectures are shown, schematically, in Figures 5 and 6 and, if properly operated, will result in a secure, cost-effective LAN at little inconvenience to users.

602. In addition to the recommended physical architecture, a LAN should have be supported by a system security policy which either provides the baseline security mechanisms outlined in NZSIT 101: Information Technology Security Policy Handbook, Chapters 4-6 (also see Annex A to this publication) or is based on the results of a specific risk analysis. Further, an active security administration regime with regular audits should be in place.

Recommended Architecture

603. The recommended architectural components which assist security are: user identifiers and passwords for LAN login; the use of masking hubs to avoid compromising LAN packet broadcasts; the use of diskless workstations to avoid

uncontrolled insertion of software, uncontrolled removal of data, and protection of access to the PC; and the use of a firewall for all external interconnection (if required) to minimise the potential for unauthorised access to LAN resources.

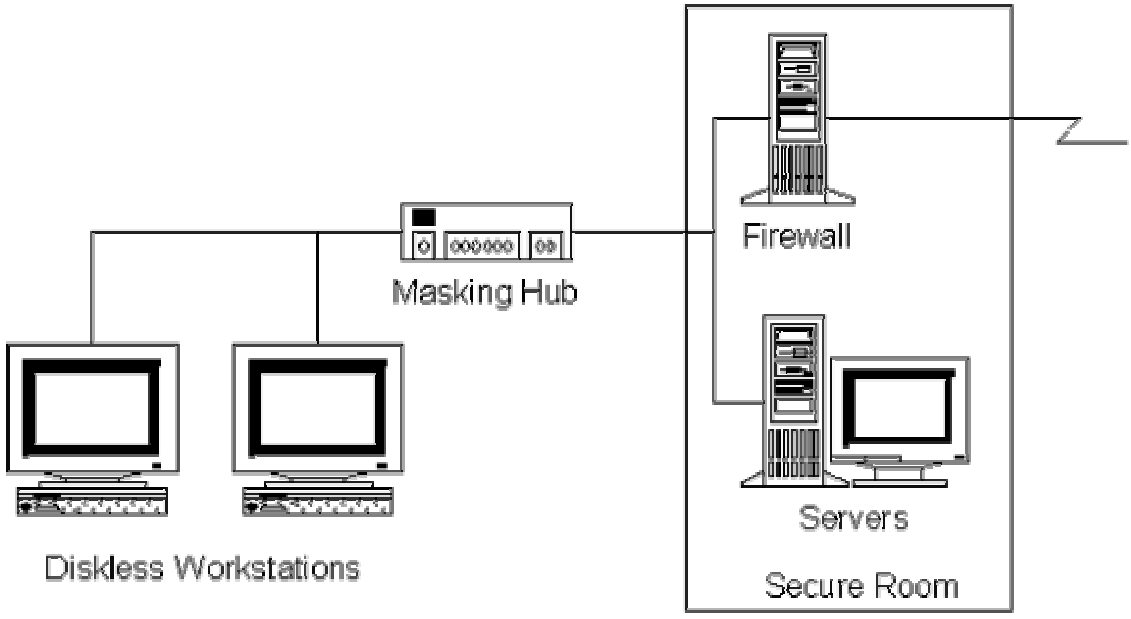

Figure 5: Recommended LAN Architecture

604. Diskless workstations can be configured to boot from a PROM and hence operate fully from the file server. While the best security option, such workstations can result in excessive LAN traffic if significant use of graphical displays occurs. It is preferable in such circumstances to provide workstations with an internal hard disk for operating system files, but no floppy disks. User file storage should be provided on the central server to allow centralised backup regimes for data backup and recovery. The workstations should, ideally, be configured to disallow local processing if a valid network login is not provided.

Recommended Interconnection

605. Permanent interconnections on the LAN must be monitored in some way. While routers are commonly used, they provide inadequate protection and fully configured firewalls should be used. Alternatively, temporary interconnections can be provided through a communications server offering a number of shared modems, configured with a strong one-time authentication system such as the Watchword or SecureId tokens or the Government variant SmartCrypt package to ensure positive identification of incoming calls.

Wireless LANs

606. The high vulnerability of wireless LANs to passive interception makes their use in Government unattractive. Specific security advice on wireless LANs has been promulgated as Security Notice 1/95, a copy of which can be found in NZSIT 109: Information System Security Notices. The guidance provided, in summary, is:

a. infra-red wireless communications are suitable for use within departmental buildings to connect unclassified and unclassified-but-sensitive LANs;

b. advice from the GCSB should be sought by NZ Government departments if they are planning to use wireless LANs outside of departmental buildings or for processing classified information.

CHAPTER 7

SPECIAL CONSIDERATIONS FOR LANS PROCESSING CLASSIFIED INFORMATION

General

701. The use of LANs to process classified information requires special consideration to be taken in the establishment of the LAN security policy, in particular the controls on user access, and the selection of security countermeasures.

702. All hard disks on the workstations and servers connected to the LAN are to be considered as holding information at the maximum sensitivity level of all information processed on the LAN. Servers are to be located in a vault or strong room appropriate for the storage of material of this sensitivity. Workstation hard disks are to be either removable and locked away in the appropriate container as detailed in the publication Security in Government Departments, or protected by a cryptographic subsystem that is approved for the protection of material of that sensitivity. The GCSB is to be consulted for advice on cryptographic subsystems for computer storage.

703. LAN operating systems do not provide sufficient assurance of information separation to permit shared use of a server by staff not cleared to access the highest level of material that is processed on the LAN, i.e., LANs can operate in dedicated, system-high mode, or compartmented mode, but cannot be deployed as a communications component of multi-level secure systems.

704. Classified LANs are not to be connected to unclassified networks or to other networks handling material of a higher maximum classification. Current interconnectivity and filtering technologies, such as routers, mailguards, and firewalls, provide insufficient assurance for the protection of classified information from the unclassified domain. Air gap procedures must be used when transferring information from an external network into the classified LAN,

and rigorous manual review procedures are to be used to protect against inadvertent spillage of classified information when transferring information through an air gap out of a classified LAN.

705. Under no circumstances are modems to be directly installed on classified LANs. The only approved configuration for modems on classified LANs is shown in Figure 6, where the modem is connected on the BLACK side of an approved encryptor.

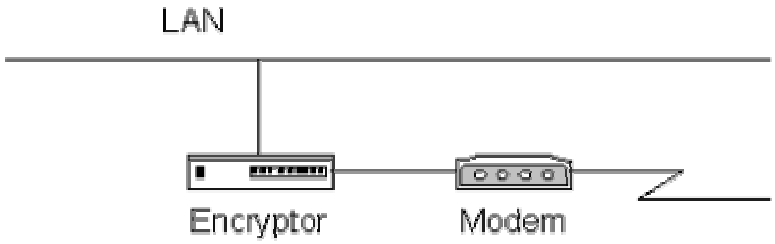

Figure 7: Permissible Configuration for Secure LAN Modem

706. In all cases where LANs are used to process classified information, a TEMPEST threat assessment is to be undertaken in accordance with NZCSI 403: TEMPEST Countermeasure Assessment. This analysis will dictate whether emission limited or TEMPEST rated equipment needs to be used. It should be noted that where workstations are required to the TEMPEST rated, they must be ordered fully configured with all required cards, as opening a TEMPEST PC case will compromise its TEMPEST integrity.

707. Fibre cabling and passive hubs should be used for LANs processing classified information, unless a full risk analysis justifies the use of alternative, less secure components. Wireless communications must not be used to connect LANs processing classified information without prior approval from the GCSB.

LAN Transmission Confidentiality

708. The transmission of classified information requires that approved communications circuits be used. Circuits can be approved by approved encryption products, or may be approved by virtue of their physical security. It is strongly recommended that an approved transmission encryption mechanism be used on all LANs processing classified material.

LAN Management Issues

709. All LANs processing classified information should be subject to certification and accreditation procedures (see NZSIT 102: The Certification of Government Computer Systems) and should operate under a strict usage

monitoring regime. The LAN should also be subject to regular independent inspections to provide additional assurance of its integrity.

710. Network audit or configuration software should be used on a regular basis to monitor the LAN configuration.

711. Ideally, an IEEE 802.10 compliant LAN should be used to support the processing of classified information. However, there has been little vendor effort to incorporate these security measures to date. In the interim, additional protection can be provided through the use of approved software encryption and authentication systems.

ANNEX A

LAN SECURITY CHECKLIST

1. An information security policy is a concise statement of official information values, protection responsibilities, and organisational commitment. This policy is one of the key components of an overall computer systems security program. It is this policy statement that can drive the initial security requirements for a LAN. However it may be appropriate to address LAN security goals, responsibilities, etc. with a separate policy to be used in conjunction with the existing broader policy. Full details of the issues involved in development of security policies can be found in NZSIT 101: Information Technology Security Policy Handbook.

2. The attached summary checklist includes the major controls and responsibilities that should be considered for incorporation into a LAN security policy. These cover items in the LAN security policy, LAN administrator responsibilities, and user responsibilities.

LAN Checklist (Generic)

Site:_____ Date: _____

A LAN Security Policy exists	
LAN Standard Operating Procedures exist	
LAN Incident Response procedures exist	
A current LAN Risk Analysis exists	
The LAN Administrator has completed the GCSB LAN Security Course	
The LAN Server is located in a secure room	
LAN workstations are diskless	
The LAN has an uninterruptable power supply	

LAN cabling is secured against unauthorised access	
Imported diskettes are virus checked before use	
Files imported from network connections are checked before use	
The file server is regularly scanned for viruses	
A formal user registration process exists	
No obsolete user accounts exist	
User password checks show no weak passwords	
Users have minimum-privileges	
NetAudit configuration checks are clean	
Network audit logs are activated	
Network logs are regularly reviewed	
Intrusion detection is activated	
Clear policy exists on the use of LAN traffic monitors/recorders/sniffers	
Authentication exchanges are protected	
Network data transmissions are masked/encrypted	
No unauthorised interconnection exists (especially modems)	
Workstation timeout is invoked	
A file server backup regime exists	
Backup tapes are securely stored	
Off site copies of backup tapes exist	
All software is being operated within its licence agreements.	
All personal information is protected in accordance with the Data Privacy Act	