Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

Phone: 02 6265 0197 Email: assist@dsd.gov.au

HANDBOOK 8

NETWORK SECURITY

Version 1.0

Objectives

801. Network security involves the protection of an agency or internal network from threats posed by authorised or unauthorised connections. This handbook focuses on those network security issues that are relevant to the protection of Government systems. Reference is made to other DSD documents that detail network security issues and in particular this handbook should be used in conjunction with the **Gateway Certification Guide** which deals with agency separation and internetwork connectivity using gateways.

Interconnection of Networks

802. The interconnection of networks is an increasing trend in government and private industry. It is no longer an easy task to draw a boundary around an organisation and apply controls to the boundary to protect internal assets.

803. Commonly when one owner decides to connect their network to another they do not consult (or are even aware of) the owners of other networks already connected. Thus a network can rapidly become linked, albeit indirectly, to an installation with a very different security policy.

804. There is the obvious danger that connections made in such an extended network may increase the risk of a security compromise, with the owners unaware of the risk. In some instances Commonwealth agencies have discovered their computing systems have, by this method, become connected to the Internet. It is therefore a reasonable assumption that the security risks are likely to rise as a result of the interconnection of networks.

805. Network connections should therefore be protected, at a level based on the risk. The assumption must be that the connecting parties are to a certain degree hostile and have to be strictly constrained to the access for which the connection was agreed. The connecting parties will, after all, have their own security policies and risk management philosophies, and these may vary considerably. Each security management domain will need to apply stringent logical access controls, and should strongly consider using firewalls and related technologies to defend their 'perimeter'.

806. A significant risk is that agency security staff may not be aware of all connection points inbound and outbound from an agency network including:

a. Dial-in or dial-up connections

b. Leased lines

This lack of awareness constitutes a significant vulnerability on the part of agencies. The ability to maintain an accurate picture of the network connectivity and apply appropriate controls to access points is an important countermeasure. Tools which assist in detecting network attached devices and the presence of modems are available.

Firewalls

807.   This section discusses a common network security tool, the firewall. The purpose of a firewall is to provide controlled and audited access to services between two or more networks. It does this by permitting, denying, or redirecting the flow of data across the firewall.

808. A firewall may also support anonymity for internal network hosts, through a function known as 'address translation'. The address translator substitutes the address of the firewall in IP packets delivered to the external network so that the internal network topology is hidden from the external network, thereby reducing the risk of an attack on the internal network. The minimum essential functional requirements for a firewall product are as follows:

a. All communications traffic to and from the internal network must be routed through the firewall as the only route into and out of the internal network.

b. The default condition of the firewall should be to deny all connections to (and sometimes from) the internal network. Only explicitly authorised connections should be allowed.

c. The firewall must provide a trusted path for its management. This may be via a physically secure dedicated management console with an identification and authentication system, or via an approved, remote, cryptographically protected system.

d. The firewall must provide sufficient audit capability to detect breaches of the firewall's security and attempted network intrusions. Ideally it should also provide real time alarms.

809. There are three different types of firewalls, namely a packet filter, a circuit filter, and an application filter. These are explained as follows:

a. Packet filtering is undertaken on the contents of the IP packet header. The filter information is therefore limited to the source and destination address and the TCP/UDP port number. A packet filter does not operate on the contents of the packet, ie the data.

b. A circuit filter applies packet filtering as described above, but verifies information based on TCP or UDP packet header information. In this manner, it is able to make more detailed decision on whether individual packets form part of a valid TCP sequence. Note however, that a circuit filter still has no knowledge of which user is requesting access to services.

c. An application filter uses proxies to apply filter rules based on the data content and sometimes the user. A dedicated program called a 'proxy' or 'proxy server' is used to effect the application filter policy rules. A common application filter is a web proxy, which can be used to restrict the internal (or Intranet) web pages that are published out to the Internet.

810. Agencies publishing material on public information servers should firewall the public information servers from the external network, and also firewall their internal network from the public information servers. These public information servers may be placed in a De-Militarised Zone (DMZ), which may be achieved by placing the external network, public information servers, and internal network on three different physical ports of the firewall.

811. It is strongly recommended that Commonwealth Government agencies seek advice from DSD prior to purchasing and installing a firewall. DSD can advise on the vendor's claims for the security features of a firewall product, and can confirm that it has been configured properly on installation. The AISEP (see **Handbook 2 - Evaluated Products**) evaluates firewalls against an agreed security target. In each case a certification report is produced detailing the security target, the configuration that has been evaluated, and any constraints imposed by the evaluators on the firewall's implementation and use. Certification reports are available from DSD.

812. DSD has identified a continuing need for network security perimeter (or gateway) protection. This protection is essential when an agency connects to a public network such as the Internet. It may also be required when one agency connects to another because the different business needs of the two agencies may mean that they have different, potentially incompatible security needs. The large number of threats to systems, data and applications, and the high or even extreme level of threat likelihood dictates that managed safeguards are required to protect agency information systems so as to minimise the risk of intrusion or compromise. To this end, DSD has produced a **Gateway Certification Guide**. The primary purpose of the Guide is to provide agencies seeking DSD certification of their gateway facility with details of the requirements that they must fulfil. In addition, the Guide provides direction and ideas to those agencies considering secure gateway design, development or management issues, and can be used as a reference for independent "verification" of any gateway system.

813. The DSD Gateway Certification Process aims to provide a Commonwealth Agency, or a Service Provider to Commonwealth Agencies with an independent assessment that their Gateway has been configured and managed to industry best practice and that safeguards are implemented and operating effectively. This assurance will afford clients using the gateway services a level of trust in the service. Certification is a voluntary process and this guide is designed to assist agencies that wish to pursue certification (or to recertify) to prepare for the DSD review.

Virtual Private Networks

814. The Virtual Private Network (VPN) functionality of firewalls or related products allows for the encryption of information between two or more sites. It is used to set up an effective secure channel using public communications network such as the Internet. Since the channel is encrypted, the data is not likely to be compromised through lack of confidentiality or integrity protection measures, however, it is subject to the same availability problems as the public communications network. The encrypted data shares the public communications media, but is logically separated from the public network by encryption. End-users are unaware of the encryption process. The VPN tunnel eliminates the cost of dedicated encryption links between different communicating sites.

815. It is important that the security functionality claims offered by VPN vendors are verified by an independent party. This is particularly the case for VPN products that are used for critical system or data protection. The VPN functionality may already form part of an evaluated firewall architecture as found in the **Evaluated Products List**. Alternatively, the VPN functionality may have been removed from an evaluated functionality as it was found to be unsuitable for Australian Government use, or was removed from evaluation by the vendor.

816. The use of a virtual private network provides confidentiality of data in transit, and some assurance that the connection originates from a known end point. It is worthwhile to note that additional countermeasures may be required to:

a. authenticate the originator of the connection

b. provide access control within the agency network

c. audit the actions of the party obtaining access

d. maintain the integrity and availability of agency systems eg. against malicious content.

e. Prevent leakage of data of a higher classification to a lower classified network or system.

Security Filters, One-way gateways, Switches

817. Under some circumstances it is possible to install a 'security filter' between two separately classified systems, to control the flow of classified data which is presented for transmission across the interface. Such a filter is programmed to

scan the data and allow or disallow the transmission in accordance with a security policy. In this manner, a filter may be designed to prevent certain information leaving a classified or sensitive network, and may be termed an "output filter". Similarly, an 'input filter' may be used to limit the input from a potentially high-risk environment to a sensitive or classified network. An example of such as filter may be to remove executable programs or all attachments from incoming emails.

818. An output filter can generally only be effective if it is possible to rely on the classification label of the data presented for transmission. This means that there must be a strong guarantee that:

a. The classification label received by the filter is the same as was affixed by the person who classified the document; and

b. No more highly classified information has become attached to the data as it passed through the transmitting computing entity.

819. These criteria can only be met if either the transmitting entity is a "trusted computing system" of the appropriate level or the text of the data and its classification have been sealed in some way such that any modification to the text after it leaves the originator is detectable. In some cases it is possible to scan a text for certain words and thus determine whether or not it is below a particular classification. This is commonly known as a "dirty word search".

820. One-way gateways (diodes) can sometimes be used to protect a connection between systems of different classifications, when it is only necessary to pass information from the lower classified system to the higher. An example would be the connection of an UNCLASSIFIED news service to a PROTECTED level system. If the communications protocol is sufficiently simple a one-way gateway can be achieved by breaking the electrical or optical connection on the return path. Clearly, it is essential to mark the connecting cable most carefully to ensure it is not inadvertently replaced, or the diode used in reverse. Note that in this basic form (ie. the breakage of the connection on the return path) only provides protection for the confidentiality of systems on the high side. Dependent on the protocol passing through, availability and integrity of systems on the high side may not be protected without additional countermeasures. It is recommended that sites implementing one-way gateways examine the security enforcing functions provided by the device and the nature of the protocols passing through.

821. KVM (keyboard/video/mouse) switches, in conjunction with a one-way gateway, can avoid the need to have bidirectional gateways between higher and lower classified networks. However, this approach requires users to adapt their work practices to comply with the restrictions of this technology. In particular, in order to transfer data from the higher classified system to lower classified one, an airgap transfer such as tape or floppy disk transfer must be used. The switch should provide the following functionality:

a. There should be a very low risk of data being leaked from the higher to the lower classified system via the KVM switch, or via any of the components being switched.

b. It must not be possible to attack the high system from the lower classified system via the KVM switch.

c. There should be a clear and unambiguous display of which system the user is connected to.

d. The switch must be tamper evident.

Multi Level Networks

822. A Multi Level Network or system is one in which there are authorised users on the network that are not cleared to have access to the highest classified data stored or processed on the network. The term may also apply to those users who are cleared to access data, but are not briefed for a particularly sensitive compartment within the classified data. The two modes of multi level networks can be summarised as follows:

a. Multi Level Mode: Not all authorised system or network users are cleared to the highest classification of data.

b. Compartmented Mode: All authorised system or network users are cleared to the highest classification of data, but not all users are briefed for all compartments.

823. Multilevel systems will require the application of evaluated products, so as to minimise the risk of inadequately cleared staff accessing classified information. These evaluated products will usually be at the EAL4 or greater rating (see **Handbook 2 – Evaluated Products**). The protection profile (functionality) and the level of assurance required depend (in part) on the level of classification of the system and the level of clearance of all system users. DSD can assist with determining the appropriate level of assurance, the security objectives and perhaps the protection profile of a multilevel system. It is important to note that the successful application of a multilevel system requires not only the correct (evaluated) products, but, perhaps more importantly, the discipline to manage the ongoing security configuration. Consequently, the resources required for the development and maintenance of a true multilevel system are not trivial, and can be quite expensive. ***It is therefore strongly recommended that any plans for developing a multilevel system be made in close consultation with DSD***.

824. Compartmented systems may be protected using varying degrees of access control and an audit strategy. In cases of high risk the use of trusted encryption products eg. PKI may be used to reinforce the privacy of information in a compartmented system.

Wireless LANs

825. Wireless Local Area Networks (WLANs) are experiencing a period of substantial growth in the marketplace. System managers are therefore likely to

consider migrating to a WLAN infrastructure. As the "wireless" suggests, transmissions on WLANs are made using radio frequency methods, and obviate the need for expensive cabling infrastructures. Mobile (wireless) computers access the network through an "Access Point" (AP), in a method similar to the way mobile telephone systems are operated. The AP sends and receives local area network traffic via radio, and therefore acts as the method by which wireless computers communicate with the wired network infrastructure. A typical AP may function at distances of up to a few hundred metres. The Institute of Electrical and Electronic Engineers (IEEE) has developed the IEEE 802.11 as an international standard for WLANs. The 802.11 standard specifies a number of technical parameters for operation of WLAN compliant devices.

826. The security threats posed by WLANs may include:

a. ***Confidentiality and integrity***. It may be possible for an attacker to intercept communications between a mobile computer and an AP, and thereby capture sensitive or classified information not intended for a third party. Note that normal LANs also work in this "broadcast" mode, although intercepting communications on a standard LAN requires physical access to the cabling infrastructure. Conversely, it may also be possible for an attacker to insert information into an authentic transaction, without the knowledge of the legitimate users.

b. ***Authentication***. Unless mobile platforms are securely authenticated, an attacker may simply connect the WLAN using an 802.11 compliant device and become an "authorised" station on the WLAN.

c. ***Availability***. 802.11 compliant devices operate either in the infrared or the 2.4GHz radio frequency range. The 2.4GHz range is a frequency band set aside for use by industrial, scientific or medical equipment. As such, it is possible that an attacker could "jam" the band and thereby disrupt communications. Alternatively a WLAN's communications may be inadvertently disrupted by another device operating in this band.

827. The fact that 802.11 compliant devices operate using infrared or "spread spectrum" communications does, in itself, offer some level of security against attackers. The two methods of spread spectrum communications, namely direct sequence and frequency hopping, were developed in part to mitigate the risk of communications being jammed or intercepted. However, whilst spread spectrum methods will provide a degree of protection against "denial of service" attacks, they may not provide sufficient strength against attacks on confidentiality or integrity of WLAN traffic. The 802.11 specifies an optional encryption algorithm entitled Wired Equivalent Privacy (WEP) designed to mitigate the risk of compromise by eavesdropping on WLAN traffic. In the words of the 802.11 standard:

IEEE 802.11 specifies an optional privacy algorithm [wired equivalent privacy (WEP)] that is designed to satisfy the goal of wired LAN "equivalent" privacy. The algorithm is not designed for ultimate security but rather to be "at least as secure as a wire".

828. This is significant since most wired LAN systems are not necessarily as secure as users require. The WEP algorithm in the 802.11 standard also specifies a reasonably strong form of authentication, that is part of the WEP option. Users considering the use of wireless LAN infrastructures should note the requirements of **Handbook 9 - Cryptographic Systems**. Products implementing the 802.11 standard would need to be evaluated through the AISEP to be considered suitable for Australian Government use. For use of Evaluated Products see **Handbook 2 - Evaluated Products.**

Remote Users

829. The growth in remote connectivity emerges from a varying range of requirements including:

a. external public users accessing published information

b. authorised users accessing restricted information on a secure web/ftp server

c. remote users conducting online transactions

d. remote users accessing communications facilities eg. ISP services

e. telecommuters – working from home

f. Mobile staff eg. sales/mobile customer service centres

g. Systems administrators providing after hours on-call support

h. Vendors performing system support/maintenance

i. Authorised users accessing internal systems via a third party network

830. The range of these requirements will determine the level of access available and the level of countermeasures to be applied. The level of controls to be applied may range from:

a. network/link level encryption

b. hard disk encryption

c. strong authentication eg. cryptographic tokens

d. access control systems

e. auditing

f. physical security at remote access point

g. tamper evidence

h. user awareness and procedures

i. network access control servers

j. dialback/roaming dialback

831. Depending on the classification of data stored on and accessed from portable systems, the very nature of the portability and usage environments of remote systems requires stringent controls to be applied. It can be generally assumed that perimeter security is minimal. Based on a risk assessment for remote access, it is recommended that a special purpose security plan be developed for remote users.

Grades of Network Security Implementations

832. The following grades of network security implementation in Government are detailed below.

a. **Grade 1**

i. DSD should be consulted in situations where logon access by staff cleared one or more levels below the highest classified data is required.

ii. An evaluated firewall should be used where a connection one classification level down is required (as long as the lower network is not the Internet). It is recommended that gateway management be as per the **Gateway Certification Guide**.

iii. Connections to the Internet should be as per the requirements of the **Gateway Certification Guide**, and certified as such by DSD.

iv. The use of an approved filter or one-way gateway connection to lower classified systems should be in consultation with DSD.

v. The use of Virtual Private Network (VPN) functionality should only be considered where the products have been formally evaluated. This is especially so for the cryptographic functions (see **Handbook 9 – Cryptographic Systems**) of the VPN. A risk assessment should be conducted in order to ascertain specific security requirements for VPN and other remote access systems.

vi. The use of Wireless LAN functionality should only be considered where the products have been formally evaluated. This is especially so for any cryptographic functions (see **Handbook 9 – Cryptographic Systems**).

vii. Evaluated products are selected at an appropriate assurance level for the classification of the system. Refer to Handbook 1 for the standards regarding the appropriate levels.

b. **Grade 2**

i. DSD should be consulted in situations where logon access by staff cleared one or more levels below the highest classified data is required.

ii. Firewall connections to networks and systems at the ***same*** classification are recommended to be as per the requirements of the **Gateway Certification Guide**.

iii. The use of an approved firewall, filter or one-way gateway connection to lower classified systems should be in consultation with DSD. Restricted services should be provided between the lower classified and higher classified systems. There ***should be NO unauthorised connections to the Internet***. Additional countermeasures such as content filtering and intrusion detection systems should be deployed in association with the firewalls/gateways.

iv. The use of Virtual Private Network (VPN) functionality should only be considered where the products have been formally evaluated. This is especially so for the cryptographic functions (see **Handbook 9 – Cryptographic Systems**) of the VPN.

v. The use of Wireless LAN functionality should considered in consultation with DSD.

vi. Evaluated products are selected at an appropriate assurance level for the classification of the system. Refer to Handbook 1 - Standards for the standards regarding the appropriate levels