

## **Disclaimer**

This technical disclaimer is provided on an “as is” basis solely for guidance. It is not intended to cover network security comprehensively, but to provide an overview of the subject. There is no guarantee that the guidance provided will be suitable for your network environment. NISCC does not accept liability for any loss or damage whatsoever arising from, or in connection with, the usage of information contained within this technical note.

## **Introduction**

1. In light of an increasing trend of incidents and vulnerabilities affecting the Internet infrastructure (eg SNMP), this technical note is intended to provide best practice advice to the NISCC constituency on securing Internet facing networks against external attack.
2. This note covers the following topics:
  - General network security guidance
  - Securing a local area network
  - Securing a wide area network
  - Securing Internetworks

## **Network Security Guidance**

3. It is recommended that your organisation has a security policy agreed by senior management and that the security policy is implemented. Although the contents of your security policy will vary depending on organisational type and business function, a security policy should identify the value of the information that the organisation stores on its IT systems, and should identify the risk to those assets if lost through internal and external attack.
4. The security policy should address areas such as identification and authentication, access control, accounting and auditing and information flow. Risk should cover information confidentiality, integrity, availability and non-repudiation claims as appropriate. For example, if a system contains financially sensitive customer details, there is a foreseeable risk that disclosure of the details would result in loss of confidence in the business and could lead to financial insolvency. If the risk to an asset could lead to business failure, security of the information stored is critical, and appropriate measures should be taken to mitigate the risk. These measures will vary, but will in general include personnel, procedural and physical as well as technical measures.
5. For government readers, conformance with ISO 17799 is part of HMG INFOSEC Policy; and conformance with this standard is expected. For other UNIRAS constituents, conformance with a recognised organisational security standard such as ISO 17799 is recommended. Standards of this kind describe models for defining and implementing security policies in an organisation. However, it needs to be stressed that no policy-based standard can offer a guarantee of network security simply because the threat from external networks is continually evolving; active monitoring and testing will be needed if the threat is to be minimised.
6. In the case of securing networks from attack, the assets that need to be valued are those that can be accessed directly or indirectly by an external attacker and those that can be accessed by unauthorised users internally. Direct access relates to gateway computers or routers connected to external networks, while in general indirect access relates to computers on the same network as the gateway. If information of differing criticality is stored on the same network, partitioning the network into segments based on criticality may be beneficial. In the case of a network used to store information of differing criticality the limit of a network can be decided by the information flow policy on gateways used to segment the internal network.

7. One common type of network partition is called a De-Militarised Zone (DMZ for short). This is a partition, which is designed for services that are offered to external users, such as web servers. DMZs are typically implemented on a separate network segment to the internal and external networks via a gateway firewall. It is also possible to locate the DMZ between a boundary router and a firewall. Storage of sensitive data on a DMZ is not recommended unless further measures are taken to protect that data.
8. Once the value of your information assets has been determined, the next step is to evaluate the threat of successful external attack. To assess threat, you will need to map out your network topology and identify all of the external interfaces to the network. External interfaces include gateways, routers and dial-up connections. This can be achieved by physical inspection and by the use of network discovery and management tools. (Some popular network products are SolarWinds network discovery tools, <http://www.solarwinds.net/>, and Peregrine information tools, <http://www.scl.co.nz/>.) The routing tables on your gateways and routers will also provide information on the routes used. It is recommended that you keep an up-to-date map of your network topology. This map should include network infrastructure devices such as bridges, router and switches.
9. The external threat will be a function of:
  - The number of external connections from your network
  - The likelihood of attack from the external networks (which should always be treated as high from an internet connected network)
  - The services that are offered to external networks
10. The last step is to perform a vulnerability analysis on the network protocols that you would like to deploy and the implementation of those services that you intend to use. Good sources of some generic and specific vulnerability information are:
  - <http://www.uniras.gov.uk/>
  - <http://www.cert.org>
  - <http://www.securityfocus.com/>
  - <http://icat.nist.gov>
  - <http://cve.mitre.org>
  - <http://www.sans.org/>
11. It is recommended that when selecting software for a service for which you have a business need, that you consider the vulnerabilities in the software and the history of vulnerabilities within that software.

### **Securing a local area network**

12. Once you have identified the information assets and the threat, you will need to consider the measures that can be used to implement your security policy. Information flow and access control policies are the most central to network security, although authentication and auditing are equally important. To control information flow, you should restrict the flow across designated gateways. It is recommended that no computers should be able to connect to other network segments or to other networks except via these gateways. If you have to allow dial-up access to your network, it is recommended to use a remote access server and ensure that the strength of authentication and access control is appropriate for the access allowed.
13. Information flow and access control policies between networks segments and other networks should be determined on the gateways. It is possible to use a router as a gateway but the use of a specialist firewall is recommended in addition to routers (if required) because they generally offer greater security checks.
14. Firewalls are devices that restrict information flow based on the source and destination of the traffic, the network service and conformance with the communication protocol standard. Firewalls vary in filtering techniques, and can be classified into basic packet filters, dynamic packet filters, stateful inspection firewalls and application proxy firewalls. The firewall types vary in security and performance, with application proxy firewalls being the most secure and dynamic inspection firewalls having a good balance between security, performance and flexibility.

15. A well-configured firewall should enforce your information flow and access control policy, but a firewall can only be as secure as the network services that the security policy allows through the firewall. For instance, there is no guarantee, even with an application proxy firewall, that if you allow, say, web traffic through to a web server which has an exploitable vulnerability, that an attacker will not gain unauthorised access to your web server, and from there to other hosts on your network (or network segment).
16. Assurance against attacks on network services is best gained by independent, third-party evaluation of the proxy or packet content filters employed for those services against a reputable security standard (such as Common Criteria, ISO 15408) by an accredited organisation. Risk can be mitigated to some extent by placing more than one type of firewall in series, which is part of a “defence in depth” strategy.
17. Intrusion detection systems and network traffic flow programs form a further layer of the defence in depth strategy. Intrusion detection systems are useful to identify and block attacks on your network or on particular computers on the network, but are liable to false alarms. Network traffic flow programs enable administrators to detect unusual or suspicious traffic on the network, but they do require active monitoring and analysis of any reports produced.
18. The principle for determining information flow and access control on firewalls is:
- Deny all network services by default
  - Allow only those services that you have a considered business need to allow
19. There are some network services which should not be allowed across an external boundary without a high degree of trust existing between the networks. This should include ICMP packets of Types 5 (router redirects), 8 (“pings”) and 12 (parameter problems) directed inbound. Routing protocols should also be blocked at the external gateway. Table 2 provides a list of TCP and UDP services, which should normally be blocked. It omits services like file transfer, mail, web and news, but if you do not need to offer any of these services, they should also be blocked at the gateway.

Service Name	Standard Port Numbers	Comments
“Small” Services	1-19 (TCP & UDP)	
Telnet	23 (TCP)	
Time	37 (TCP & UDP)	
Whois	43 (TCP)	
Domain Name	53 (TCP) and (UDP)	(UDP) used for name server lookups; (TCP) for information transfers. Block DNS if not needed.
Bootp	67 (UDP)	
Tftp	69 (TCP & UDP)	
Finger	79 (TCP)	
Portmapper	111 (TCP & UDP)	Disable portmapper on UNIX machines to prevent RPC port number lookups
RPC endpoint mapper	135 (TCP & UDP)	Disable portmapper on Windows machines to prevent DCOM RPC port number lookups
NETBIOS	137-139 (TCP & UDP), 445 (TCP & UDP)	Used on Windows for resource sharing
SNMP	161-162 (TCP & UDP)	
Xdmcp	177 (UDP)	UNIX only, X Display Manager
Berkeley “r” commands and intranet only services	512-518 (TCP & TCP)	UNIX only
Route	520 (TCP)	The route server in UNIX
Uucp	540 (UDP)	UNIX only

RPC over HTTP	593 (TCP & UDP)	Microsoft Windows
Mount	635 (UDP)	The UNIX NFS mount server
MS SQL Server	1433 (TCP), 1434 (UDP)	Used by Microsoft SQL Server
Oracle Listener	1521 (TCP)	Used by Oracle database servers
NFS	2049 (TCP & UDP)	UNIX only
UpnP	1900, 5000 (TCP & UDP)	Microsoft Universal Plug and Play
X	6000-6063 (TCP)	X Windows, UNIX only
IRC	6667 (UDP)	Internet Relay Chat
Default RPC ports	32773-32785 (TCP & UDP)	Default ports for RPC services. UNIX only.
Well-known Trojan Ports	12345-6, 31337 (TCP & UDP)	Netbus & Back Orifice

20. The presence of these services should also be checked on computers on your network. For UNIX, “netstat -anp” can usually be used to determine the services that are running on the local computer and the ports to which the services are bound, while “rpcinfo -p” will determine the RPC services that are running. It is recommended that all unnecessary services be removed from your computers. For Windows, system tools can be used to determine which applications are running, while third-party tools like “fport” (see <http://www.foundstone.com/>) can be used to map applications to port numbers. “netstat” can be used on Windows computers to identify the ports that are open.
21. To maximise security on each computer it is also recommended that a best practice secure configuration be used where possible. These may be available for some operating systems from your technical security authority; but both the US National Security Agency (NSA) and the National Institute for Standards in Technology (NIST) have published readily accessible best practice guides (see <http://nsa2.www.conxion.com/> and <http://csrc.nist.gov/itsec> for further details).
22. Care also needs to be taken with the routers and bridges on your network, especially routers at the network perimeter. As with other computers, it is important to check that routers are not running vulnerable or unnecessary network services. In particular, finger should not be running and telnet should be disabled for remote administration unless there are other measures to protect the router. Secure shell is a more secure remote management tool; but any remote management is riskier than management from a locally connected console. If remote management is necessary, the management port should be on an interface to a private network that cannot be accessed from any other network or router interface. In light of the recent discovery, use of SNMP should also be avoided, and the SNMP server disabled.
23. Techniques that can be used to enhance router security are the use of access control lists and null routing. Access control lists are used to filter traffic through the router, much like a firewall’s rule set, and can be used to block traffic on particular ports from or to particular IP addresses. Null routing is a way of routing traffic to the null interface (i.e. discard the traffic) from a particular IP address, which is useful if the IP address is the source of a denial of service attack.
24. It is important to enable logging of security relevant events on all computers on your network, servers, workstations and routers. In the event of a security incident, unless the attacker can delete the logs, there will be an audit trail of the incident available.
25. In order to detect attackers using your network to launch attacks on others, the use of egress filtering is recommended. This means that your gateway checks that every outbound packet sent from your network has a valid IP address in your network. Any dropped packets should be logged and the origin of the traffic investigated.

### Securing a Wide Area Network

26. The techniques for securing a wide area network are an extension of those used for securing a local area network. The only difference between the security needs is the security of the communication bearers between the local area networks that comprise the wide area networks.

27. There are 2 different approaches to connecting local area networks, namely:

- Dedicated communications bearer
- Virtual circuits across a shared communications bearer

28. Dedicated communications links are the most secure solution if they are physically protected, but the costs associated with dedicated links are high. Virtual circuits do not in general cost as much because they reuse existing communications infrastructures.

29. There are 2 types of virtual circuit:

- Non-cryptographic virtual circuits
- Cryptographic virtual circuits

30. Non-cryptographic virtual circuits are used in the telecommunications industry to provide dedicated virtual links that are private between two parties. X.25, Frame Relay and ATM are telecommunications protocols that support virtual circuits. These links do provide privacy but traffic is sent unencrypted across the telecommunications bearers.

31. Using a cryptographic virtual private circuit has the advantage that traffic across the communications bearers will not be readily comprehensible to a third-party without knowledge of the decryption key. The UK Government has its own standards for encryption, and the commercial market is strong in this area. The de facto standard for commercial cryptographic virtual private networks is the IP Security (IPSEC) protocol suite, which encrypts traffic between local area networks across IP based networks, in particular the Internet. Using the Internet is the lowest cost option, but it is also possible to have a dedicated virtual network, which uses secret or public key cryptography over circuit based telecommunications protocols.

32. Whichever method of virtual circuit is used, it is recommended that a vulnerability analysis is performed on the communications protocols used and known vulnerabilities in the software used (if any) to maintain the virtual circuit.

### **Securing Internetworks**

33. In addition to the measures suggested in the previous sections, internetwork security has 2 further areas of interest:

- Internet Service Provider security
- Backbone Provider security

34. Common to each of the sets of providers is router security. Some security measures were suggested under "Securing a local area network", but here are some more suggestions:

- Ensure that all routing table updates from neighbouring networks are checked for authenticity and non-repudiation of origin.
- Use a dedicated authentication server to handle all remote management requests on the private network. This is particularly useful if there is remote dial-up connectivity to the management network.
- Enable network monitoring on the routers and actively monitor the traffic.
- Direct logging to another computer on the private management network.

35. Internet Service Providers have a responsibility to those to whom they provide Internet connectivity and a secondary responsibility to other network owners. As with a local area network the use of egress filtering is recommended, primarily to help combat denial of service attacks with forged source IP addresses. Where possible, the use of ingress filtering (RFC 2267) is also recommended for ISPs and backbone providers. Where an ISP connects to another ISP or backbone provider on a private link or at a peering point, the IP range of the inbound connection should be checked for validity. Ideally only egress or ingress would be needed, not both, but having both is better than having none.

36. Other proposals for dealing with denial of service attacks include Traceback (see the Internet Draft at <http://www.research.att.com/~smb/papers/draft-bellovin-itrace-00.txt>), which suggests a new type of

ICMP packet which can be sent to the attack destination with the router links between actual source and destination.

37. The focus for backbone provider security is in ensuring that none of the backbone routers is subject to a denial of service attack or is compromised by an attacker. As stated earlier, the network services offered on the router should be audited and unnecessary services removed or access blocked with an access control list. Vulnerable services should not be offered on public interfaces. SNMP should be disabled.

### **Conclusion**

38. The protecting your network section of the foregoing note has described some general measures that can be taken to secure networks of different sizes. The measures should enhance network security and minimise the risks to information assets.