INTERNATIONAL STANDARD

ISO/IEC 18028-4

First edition
2005-04-01

Information technology — Security techniques — IT network security —

Part 4: Securing remote access

Technologies de l'information — Techniques de sécurité — Sécurité de réseaux TI —

Partie 4: Téléaccès de la sécurité

Reference number
ISO/IEC 18028-4:2005(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18028-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 18028 consists of the following parts, under the general title *Information technology — Security techniques — IT network security:*

— *Part 2: Network security architecture*

— *Part 3: Securing communications between networks using security gateways*

— *Part 4: Securing remote access*

Network security management and securing communications between networks using Virtual Private Networks will form the subjects of the future Parts 1 and 5, respectively.

Introduction

In Information Technology there is an ever increasing need to use networks within organizations and between organizations. Requirements have to be met to use networks securely.

The area of remote access to a network requires specific measures when IT security should be in place. This part of ISO/IEC 18028 provides guidance for accessing networks remotely – either for using email, file transfer or simply working remotely.

Information technology — Security techniques — IT network security —

Part 4: Securing remote access

1 Scope

This part of ISO/IEC 18028 provides guidance for securely using remote access – a method to remotely connect a computer either to another computer or to a network using public networks and its implication for IT security. In this it introduces the different types of remote access including the protocols in use, discusses the authentication issues related to remote access and provides support when setting up remote access securely. It is intended to help network administrators and technicians who plan to make use of this kind of connection or who already have it in use and need advice on how to set it up securely and operate it securely.

2 Terms, definitions and abbreviated terms

For the purposes of this document, the following terms, definitions and abbreviated terms apply.

2.1
Access Point
AP
the system providing access from a wireless network to a terrestrial network

2.2
Advanced Encryption Standard
AES
a symmetric encryption mechanism providing variable key length and allowing an efficient implementation specified as Federal Information Processing Standard (FIPS) 197

2.3
authentication
the provision of assurance of the claimed identity of an entity. In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication).

2.4
call-back
a mechanism to place a call to a pre-defined or proposed location (and address) after receiving valid ID parameters

2.5
Challenge-Handshake Authentication Protocol
CHAP
a three-way authentication protocol defined in RFC 1994

2.6
Data Encryption Standard
DES
a well-known symmetric encryption mechanism using a 56 bit key. Due to its short key length DES was replaced by the AES, but is still used in multiple encryption mode, e.g., 3DES or Triple DES (FIPS 46-3).

2.7
de-militarised zone
DMZ
a separated area of a local or site network whose access is controlled by a specific policy using firewalls. A DMZ is not part of the internal network and is considered less secure.

2.8
Denial of Service
DoS
an attack against a system to deter its availability

2.9
Digital Subscriber Line
DSL
a technology providing fast access to networks over local telecommunications loops

2.10
Dynamic Host Control Protocol
DHCP
an Internet protocol that dynamically provides IP addresses at start up (RFC 2131)

2.11
Encapsulating Security Payload
ESP
an IP-based protocol providing confidentiality services for data. Specifically, ESP provides encryption as a security service to protect the data content of the IP packet. ESP is an Internet standard (RFC 2406).

2.12
Extensible Authentication Protocol
EAP
an authentication protocol supported by RADIUS and standardised by the IETF in RFC 2284

2.13
File Transfer Protocol
FTP
an Internet standard (RFC 959) for transferring files between a client and a server

2.14
Internet Engineering Task Force
IETF
the group responsible for proposing and developing technical Internet standards

2.15
Internet Message Access Protocol v4
IMAP4
an email protocol which allows accessing and administering emails and mailboxes located on a remote email server (defined in RFC 2060)

2.16
Local Area Network
LAN
a local network, usually within a building

2.17
modem
hardware or software that modulates digital signals into analogue ones and vice versa (demodulation) for the purpose of using telephone protocols as a computer protocol

2.18
Multipurpose Internet Mail Extensions
MIME
a method allowing the transfer of multimedia and binary data via email; it is specified in RFC 2045 to RFC 2049

2.19
Network Access Server
NAS
a system, normally a computer, which provides access to an infrastructure for remote clients

2.20
one-time password
OTP
a password only used once thus countering replay attacks

2.21
Passive mode
PASV mode
an FTP connection establishment mode

2.22
Password Authentication Protocol
PAP
an authentication protocol provided for PPP (RFC 1334)

2.23
Personal Digital Assistant
PDA
usually a handheld computer (palmtop computer)

2.24
Point-to-Point Protocol
PPP
a standard method for encapsulating network layer protocol information over point-to-point links (RFC 1334)

2.25
Post Office Protocol v3
POP3
an email protocol defined in RFC 1939 which allows a mail client to retrieve email stored on the email server

2.26
Pretty Good Privacy
PGP
a publicly available encryption software program based on public key cryptography. The message formats are specified in RFC 1991 and RFC 2440.

2.27
Private Branch Exchange
PBX
usually a computer-based digital telephone switch for an enterprise

2.28
Remote Access Dial-in User Service
RADIUS
an Internet Security protocol (RFC 2138 and RFC 2139) for authenticating remote users

2.29
Remote Access Service
RAS
usually hardware and software to provide remote access

2.30
remote access
authorized access to a system from outside of a security domain

2.31
Request for Comment
RFC
the title for Internet standards proposed by the IETF

2.32
Secure Shell
SSH
a protocol that provides secure remote login utilising an insecure network. SSH is proprietary but will become an IETF standard in the near future. SSH was originally developed by SSH Communications Security.

2.33
Secure Sockets Layer
SSL
a protocol located between the network layer and the application layer provides authentication of clients and server and integrity and confidentiality services. SSL was developed by Netscape and builds the basis for TLS.

2.34
Security/Multipurpose Internet Mail Extensions
S/MIME
a protocol providing secure multipurpose mail exchange. Its current version 3 consists of five parts: RFC 3369 and RFC 3370 define the message syntax, RFC 2631 to RFC 2633 define message specification, certificate handling and key agreement method.

2.35
Serial Line Internet Protocol
SLIP
a packet framing protocol specified in RFC 1055 for transferring data using telephone lines (serial lines)

2.36
Service Set Identifier
SSID
an identifier for wireless access points, usually in the form of a name

2.37
Simple Mail Transfer Protocol
SMTP
an Internet protocol (RFC 821 and extensions) for sending mail to mail servers (outgoing)

2.38
Transport Layer Security Protocol
TLS
the successor of SSL is an official Internet Protocol (RFC 2246)

2.39
Uniform Resource Locator
URL
the address scheme for web services

2.40
Uninterruptible Power Supply
UPS
usually a battery-based system to protect devices against power outages, sags and surges

2.41
User Datagram Protocol
UDP
an Internet networking protocol for connectionless communications (RFC 768)

2.42
Virtual Private Network
VPN
a private network utilising shared networks. E.g., A network based on a cryptographic tunnelling protocol operating over another network infrastructure.

2.43
WiFi Protected Access
WPA
a specification for a security enhancement to provide confidentiality and integrity for wireless communications; it includes the temporal key implementation protocol (TKIP). WPA is the successor of WEP.

2.44
Wired Equivalent Privacy
WEP
a cryptographic protocol offering stream cipher encryption with a key length of 128 bits; it is defined within the IEEE 802.11 Wireless LAN specifications

2.45
Wireless Fidelity
WiFi
a trademark provided by the WiFi Alliance promoting the use of wireless LAN equipment

2.46
Wireless LAN
WLAN
a network using radio frequencies. The most common standards in use are IEEE 802.11b and 802.11g with up to 11 Mbps respectively 54 Mbps transfer rate utilising the 2,4 GHz frequency band.

3 Aim

This part of ISO/IEC 18028 is intended to guide network administrators and IT security officers when confronted with the problems of securing remote access. It provides information on the various types and techniques for remote access and helps the intended audience to identify adequate measures to protect remote access against identified threats.

It may also provide help to users who intend to access their office remotely from their home office or when travelling.

4 Overview

Remote access enables a user to log on from a local computer to a remote computer or computer network and use its resources as if a direct LAN link existed. The services used here are known as Remote Access Service (RAS). RAS ensures that remote users can access the network resources.

In general, RAS is used in the following situations:

- to link individual stationary workstations (e.g., so that individual staff can work from home as telecommuters),
- to link mobile computers (e.g., to support staff working in the field or on business trips),
- to link entire LANs (e.g., to connect local networks of remote locations or branch offices to a corporate headquarter LAN),
- to provide management access to remote computers (e.g., for remote maintenance).

RAS offers a simple way to connect remote users in such scenarios: the remote user establishes a connection with the main network e.g., over the telephone network using a modem. This direct connection may exist for as long as is necessary and can be viewed as a leased line, which is only active on demand. It may also be permanent when DSL or other adequate technology is used.

IMPORTANT: Remote access to an enterprise should always be directed through a remote access server; direct dial-in into computers implies many risks and should therefore be omitted. Modems in enterprises should only be used at defined locations.

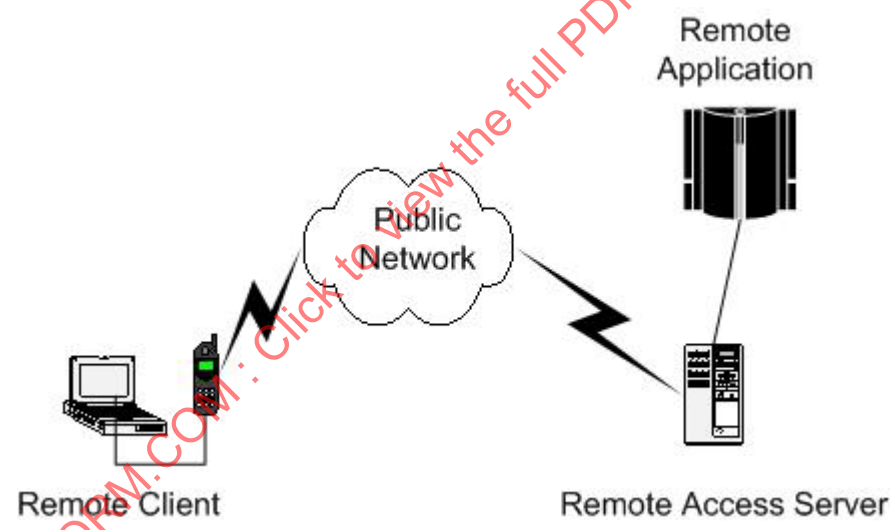

Figure 1 — Remote Access to Resources

Establishment of a RAS connection generally requires three components as follows:

1. A local network component within the corporate network, which provides the RAS (i.e. RAS software has been installed) and which is ready to accept RAS connections. This is known as the *RAS server* or *access server*.
2. A remote computer on which RAS software has been installed and which initiates the RAS connection. This is known as the RAS client. Remote clients may be workstations or mobile computers.
3. The communication medium over which the RAS connection is established. In most scenarios the RAS client uses a telecommunications network to establish the connection. The very minimum that is required, therefore, is a telephone line and a modem to go with it. Depending on the RAS architecture, different connection technologies can be used server-side.

RAS is implemented as a client/server architecture: a RAS client may be configured so that it automatically establishes the RAS connection when corporate network resources are required by dialling the phone number of the computer on which the RAS server software is installed.

Alternatively, the user can initiate the RAS connection manually. Some operating systems also allow the RAS to be activated immediately following system logon. Have in mind that a client system may be any kind of computer (e.g., laptop, PDA, smart phone).

After connection establishment, a client system may use various applications; some of these may have security implications.

5 Security requirements

From a security standpoint the RAS server and the RAS client are considered to be under control of a given security policy while the communication medium is considered out of control and possibly in a hostile environment. Security mechanisms concentrate on the risks that unauthorized entities (e.g. individuals or processes) may

- gain access to the RAS client,
- gain access to the RAS server,
- block access to the RAS server (Denial of Service),
- eavesdrop on the information exchanged between the RAS client and the RAS server, and
- modify information in exchange.

The security services to counter these risks are confidentiality services, authentication services and access control. Therefore, the following security objectives apply to RAS access:

Authentication: The remote user must be uniquely identified by the RAS system. The identity of the user must be established through an authentication mechanism every time that a connection is established to the local network. In the context of system access, additional control mechanisms must be employed to ensure that system access by remote users is properly controlled (e.g., restricting access to certain times or to permitted remote connection points only).

There are various methods of authenticating users and processes differing in quality and technology. The most common, but also the most vulnerable, method is the use of passwords.

Access control: Once the remote user has been authenticated, the remote access server must be able to restrict the interactions of the user with the network. This requires that the authorisations and restrictions, which have been specified for local network resources by authorised administrators, be also enforced for remote users in addition to any specific restrictions for remote users (e.g., specific daytime period, one connection per user).

Security of communications: Where local resources are accessed remotely, user data have also to be transmitted over the established RAS connection. In general the security requirements, which apply in the local network with regard to protection of communications (***confidentiality, integrity, authenticity***) must also be implementable for data transmitted over RAS connections.

However, protection of RAS communications is especially critical since communications can be transmitted using a number of communications media and protocols, which cannot generally be assumed to be under the control of the operator of the local network.

Availability: Where remote access is used for mainstream business activities, the availability of RAS access is particularly important. The smooth flow of business processes may be impaired in the event of total failure of RAS access or if connections have insufficient bandwidth. This risk can be reduced to a certain extent

through the use of alternative or redundant RAS connections. This applies especially where the Internet is used as the communications medium, as here there are generally no guarantees of either connection or bandwidth.

The client/server architecture of RAS systems means that both the RAS client and the RAS server are exposed to specific risks due to the type of operational environment and the manner of use.

RAS clients do not have to be stationary (e.g., home PC), but may also be mobile devices (e.g., laptops). However, the client location will normally not be under the control of the LAN operator so that, especially where the client is mobile, it must be assumed that the environment is insecure and is exposed to specific threats. In particular, the threats, which have to be considered here, include physical threats, such as theft or damage.

RAS servers are generally part of the LAN to which remote users wish to log on. They are under the control of the LAN operator and can therefore be covered by the security provisions, which apply locally. As the main task of the RAS server is to ensure that only authorised users can access the connected LAN, the threats to which the RAS server is exposed should be viewed as falling within the area of attacks where the objective is unauthorised access to the LAN.

6 Types of remote access connection

There are various ways of establishing a connection between a client and computers in the remote LAN:

- Direct dial-up to the access server;
- Dial-up to an access server of an Internet Service Provider (ISP) and access to the remote LAN over the Internet;
- Non-dial-up access by means of permanent connections to another network.

The following figure (Figure-2) shows these types of remote connections; mobile user 2 accesses the LAN via an ISP and the Internet and is filtered by a firewall which controls access between the Internet and the local network. Mobile user 1 could also be a WLAN user; then the RAS is called Access Point (AP). This access server is also controlled by the firewall (dotted line).

NOTE Mobile users may be using dial-up, leased line, broadband or wireless connections.

The situation with so-called “WLAN hot spot” is described through mobile user 2 accessing a WLAN access point instead of using a local modem. This means, that general Internet access is provided via the WLAN AP and an ISP.

There are a variety of methods that a client may use to connect to an ISP. The client may use wired and/or wireless technologies. Depending on the methods used, additional risks may occur, e.g., a WLAN requires that specific security measures be applied in order to keep confidentiality.

These methods offer specific pros and cons which have to be taken into account. For example, direct dial-up is intended to ensure that only authorised users who know the dial-up number may access the network remotely. However, tools scanning for accessible dial-up numbers (war dialers) help hackers to identify existing modems actively waiting for incoming calls. Internet dial-up provides a per-call advantage for the remote user. The user may access local ISPs to connect to the remote LAN. However, this connection method may require more complex and expensive server set-up and configuration.

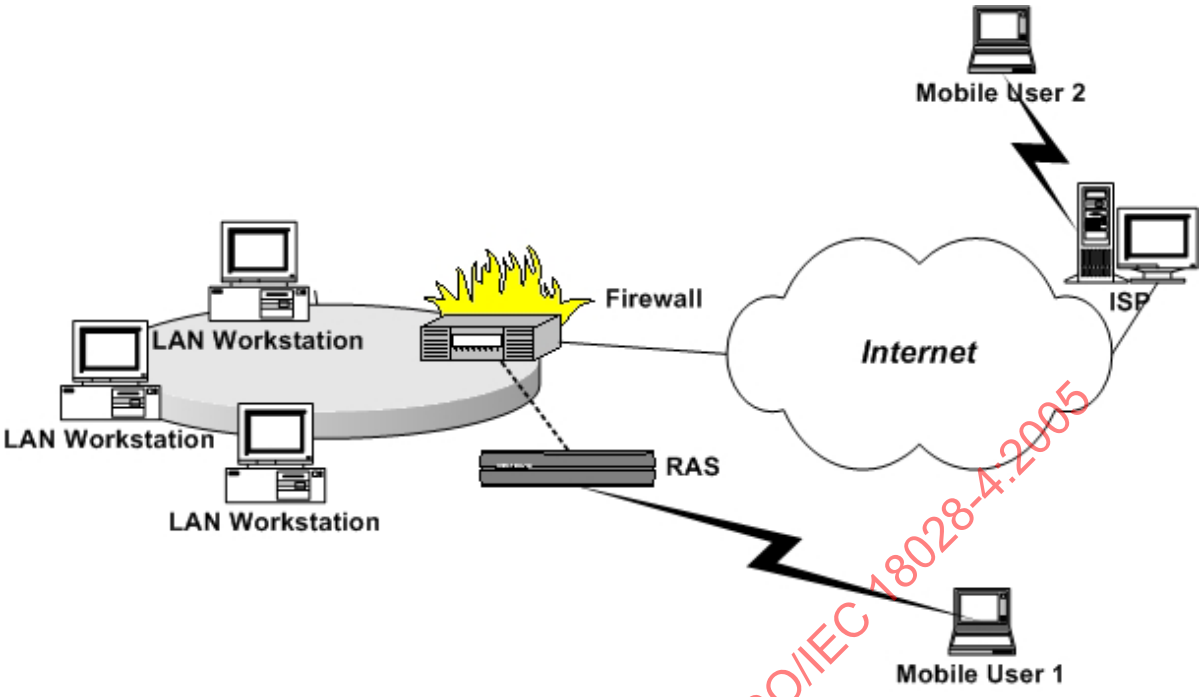

Figure 2 — Types of Remote Access

7 Techniques of remote access connection

7.1 General

Remote access should only be provided following a need-to-know principle. Therefore, an enterprise has to determine, which systems and which applications shall be accessible from the outside world by which user. The type of remote access should be defined by the service used remotely.

7.2 Access to communications servers

7.2.1 General communications protection

The most common access provided is the access to the communications services within an enterprise, i.e. access to a user's email account, to an FTP server or to a web server. Annex D provides checklists on the implementation and operation of a secure mail server and Annex E helps in setting up and administering a web server securely.

There are various ways to protect the communication between a server and a client, thus providing authenticity, confidentiality and integrity services, such as:

a) Secure Sockets Layer (SSL) provides a method of authenticating the communicating parties (client and server authentication) and encrypting the information exchange between those parties. SSL is supported by any Internet Browser and web server as well as by almost all operating systems. The Internet Engineering Task Force (IETF) has developed the Transport Layer Security Protocol (TLS), which is based on SSL, as an Internet Standard (RFC 2246) for protecting client/server communications.

b) IPsec (Internet Protocol Security) provides ways of authenticating the communicating partners as well as protecting the transferred information. IPsec also offers functions to deal with key management issues (see also RFC 2401, “Security Architecture for the Internet Protocol”).

c) Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an insecure network. It establishes a secure communications link after a successful authentication of the remote user and provides a set of commands and services (e.g., secure file transfer).

These methods provide secure authentication and confidentiality and integrity services and should be used in addition to the communications software. Due to the fact that SSL is part of commonly available Internet browsers, web mail access may be easily protected by establishing an SSL connection prior to accessing a user's email account.

A major difference between these methods lies in the fact that SSL/TLS and IPsec are usually provided as underlying communications functionalities thus being a security network service and SSH being a security application.

These techniques are also applicable for connecting an FTP client to an FTP server thus allowing access to data stored on that server.

Note: Many Internet protocols, e.g., telnet providing terminal access capabilities or FTP allowing file transfer, do only implement weak authentication mechanisms, and do typically send password information in clear text.. Tunnelling such protocols through secure protocols such as SSH, SSL/TLS or IPsec provides not only confidentiality but also provides substantial improvement for the authentication process.

Note that many web servers make use of SSL/TLS in only providing server authentication for the user but not vice versa, which requires the user to verify the server certificate.

7.2.2 Protecting electronic mail

Although email is a service whose messaging in general does not provide confidentiality, specific prerequisites have to be met to allow access to mail servers from outside. A common way to provide access to an email server is to offer a web interface to the mail accounts, which allows users on the road to access their emails. This method only requires a computer with a browser; i.e. it may be used on any computer available. On the other hand, this method is not intended to let users download their mail and answer it off-line.

Other approaches allow users to make use of their standard email clients but still do not provide sufficient confidentiality and privacy due to the concepts of email protocols. In general, an email client accesses a post office (i.e. the common program administering all incoming email accounts) by authenticating itself and the user behind in clear text. The two mail access protocols in use (POP3 and IMAP4) primarily differ in the way they treat received email:

- POP3 downloads all new email available and a user can work with it locally,
- IMAP4 allows a user to download only the mail headers and decide afterwards which mail to download to the local machine.

Due to the fact that these protocols alone do not provide sufficient security mechanisms, strong authentication and transmission confidentiality have to be provided additionally (e.g., SSL, SSH).

Note: You may also protect email contents (this excludes sender address, recipient address and subject line). The two main specifications are PGP (Pretty Good Privacy) and S/MIME (Secure Multi-Purpose Information Message Exchange), which both provide services for confidentiality, integrity, authenticity and non-repudiation of origin. Both can be integrated appropriately into many email client programs. Neither protects against traffic analysis because sender and recipient addresses are transferred in clear text.

An email server accessible by remote users should be located in the de-militarised zone (DMZ) of a network. The task of the DMZ is to separate the external network from the internal one by isolating those computers that are directly accessed from each of the networks. Placing the email server into a DMZ means that this machine is accessible from the external network and also accessible from the internal network. To avoid that this generates a risk for the internal network, certain measures have to be met:

In general, it should be avoided that an online connection between a computer of the external network and a computer of the internal network via the DMZ can be established. This can be achieved either by configuring

the respective gateways and the interim computer accordingly or by using computer constellations which provide this kind of separation.

The appropriate configuration needs to take care of the following issues:

- The mail server shall only host the specific application and a minimal operating system in order to avoid that it may be misused as a interim machine for attacks.
- The access from the outside network shall be restricted to precisely defined applications (identified by IP address and port number).
- Access from the internal network shall also be restricted by defined addresses and ports for source addresses (those computers in the internal net that are allowed to access) as well as for the destination address. Also, the direction of the information flow shall be restricted. This can be achieved by routers or firewalls.

Other communications servers such as web servers may also be situated within a DMZ and be protected accordingly. The following table (Table-1) provides the port numbers and protocols that may be considered when placing an email server in a DMZ.

Table 1 — E-Mail and related Port Numbers

Number	Name	Description
22	ssh	Secure shell login
25	smtp	conventional SMTP port with TLS/SSL capability
465	smtps	SMTP over TLS/SSL
143	imap	conventional IMAP port
993	imaps	IMAP over TLS/SSL
110	pop3	conventional POP3 port
995	pop3s	POP3 over TLS/SSL

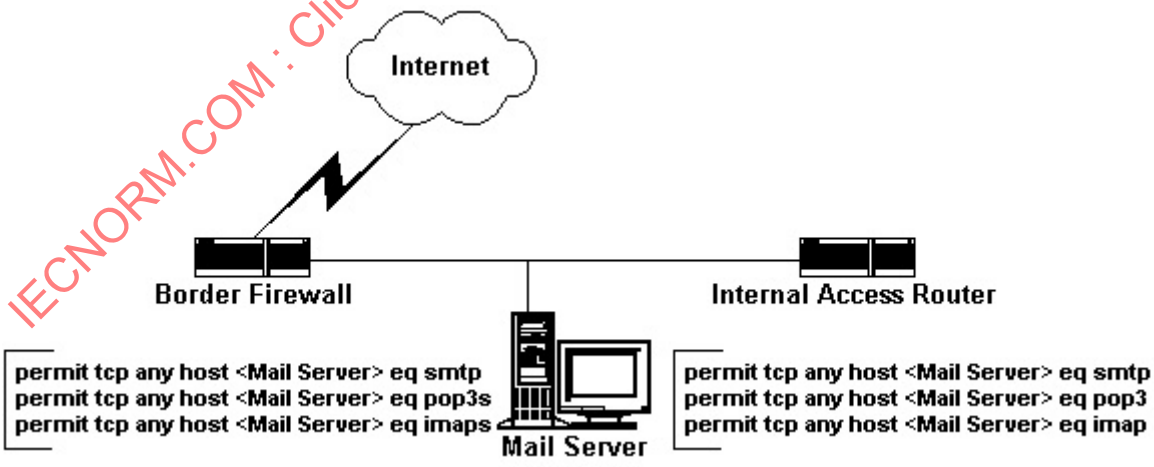

Figure 3 — Access to a Mail Server within a DMZ

Figure-3 shows the different configurations required on routers located to the Internet and to the internal network. In this case, access from the outside to the mail server is only permitted via IMAP over TLS/SSL and POP over TLS/SSL while sending emails may be done using normal SMTP. From the inside network, access is allowed using IMAP or POP without the additional protection by TLS/SSL. The commands are a pseudo command language describing the required access list commands for border firewall and internal router. By definition, any other port is prohibited to avoid weaknesses related to other ports and protocols.

Additional safeguards may be applied to avoid misuse of the SMTP Mail Server (e.g., restricted SMTP connections to avoid unsolicited email).

7.2.3 Protecting an FTP connection

The File Transfer Protocol (FTP) is another service, where the server may be located within a DMZ. FTP specifies two operational modes:

- PORT mode (also known as Normal or Active mode)
- PASV mode (also known as Passive mode)

These modes differ in the establishment of the data channel: in the PASV mode the command channel and the data channel are established by the FTP client accessing the FTP server; in the PORT mode the FTP client opens a command channel and the FTP server opens the data channel back when accepting the client's request. FTP is specified to use port 21 to build up the command channel; the data channel port is dynamically assigned out of a range typically beginning at port 1024 up to port 5000.

Principally the PORT mode allows a more secure setup of a packet filtering firewall when providing FTP capabilities to remote clients. Only TCP port 21 needs to be opened inbound to set up of the client-initiated command channel. The following establishment of the data channel is then opened outbound. Figure-4 shows the adequate filtering for the DMZ containing an FTP server.

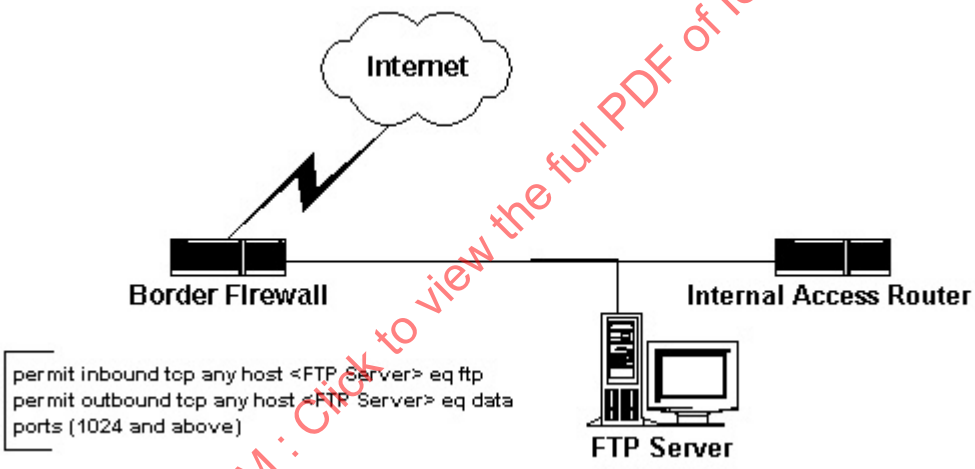

Figure 4 — Access to an FTP server within a DMZ

In contrast, implementing an FTP server using PASV mode connections requires for simple firewalls the opening of a wide port range starting at port 1024 for incoming connections. Such a setup would imply major risks to the firewall itself.

Unfortunately, PORT mode cannot be used in combination with network address translation at the firewall due to the separated establishment of the data channel. PASV mode overcomes this limitation because all channels are initiated by the client system. The implied risks in opening this wide range of ports can be solved by implementing more sophisticated firewall techniques: Firewalls providing state-full inspection techniques do allow the temporarily on-demand opening of incoming ports, allowing to provide PASV mode FTP services without requiring a wide range of open inbound ports. The same result can also be achieved by using a dedicated ftp proxy component in the firewall.

When considering providing FTP capabilities to remote clients it is important to be aware that the FTP protocol itself provides only very basic security measures. Confidentiality is not supported and the authentication services provided are on a very basic level. As an example, passwords are transmitted in clear text which does allow replay attacks.

Therefore, FTP services should whenever possible be implemented in combination with underlying security layer tunnelling protocols (e.g., TLS/SLS), or improved file transfer applications like Secure FTP or scp (secure copy), both based on the SSH protocol. Both variants allow the implementation of strong authentication as well as providing for confidentiality services.

7.3 Access to LAN resources

This access requires a set-up of machines and specific system configuration. Due to the fact that a remote user accessing resources within a network poses a high risk to this network, remote access has to satisfy the requirements as follows.

Authentication: a strong authentication mechanism or two-factor authentication have to ensure that the identity of a remote user is verified.

Authorisation: after successful authentication a remote user gets those rights granted which allow him to conduct his work as defined. This way a user performs a specific remote-user role.

Access control: prior to accessing resources or data, a remote user's access is checked against his granted rights.

Confidentiality, authenticity and integrity: depending on the resources and data used, communications security has to be established by providing confidentiality, authenticity and integrity services.

These requirements will be fulfilled by secure tunnelling protocols as used for Virtual Private Networks including appropriate authentication mechanisms. More details are discussed in ISO/IEC 18028-5 (Virtual Private Networks).

Appropriate authentication mechanisms for remote users are for example one-time password (OTP) tokens which provide a unique password every time accessed by a user who enters his Personal Identification Number (PIN). Tokens like this provide a two-factor authentication where a user has to both possess a token and know the appropriate PIN.

Authorisation may be installed by specific roles which may be assigned to groups of remote users. A group shall get those rights granted which are required to fulfil the tasks they are conducting remotely. This way restricted access for remote users can easily be implemented.

Access control may be implemented with a policy supported by the mechanisms provided from the respective operating systems in use. For example, the user account policy may define the required rights and restrictions. Operating systems may also provide group policies specifically developed for remote users.

The most commonly used set of protocols is provided with the Remote Authentication Dial-In User Service (RADIUS). These protocols, originally developed only for dial-up remote access, enable centralised authentication, authorisation and accounting for network access and are supported by VPN and strong authentication mechanisms. The protocols work as follows:

A RADIUS client (typically an access server such as a dial-up server, VPN server, or wireless access point) sends user credentials and connection parameter information in the form of a RADIUS message to a RADIUS server. The RADIUS server authenticates and authorises the RADIUS client request, and sends back a RADIUS message response. RADIUS clients also send RADIUS accounting messages to RADIUS servers. Additionally, the RADIUS standards support the use of RADIUS proxies. A RADIUS proxy is a computer that forwards RADIUS messages between RADIUS clients and RADIUS servers, possibly via other RADIUS proxies. RADIUS messages are never sent between the access client and the access server.

RADIUS messages are sent as User Datagram Protocol (UDP) messages; UDP port 1812 is used for RADIUS authentication messages and UDP port 1813 is used for RADIUS accounting messages. Only one RADIUS message is included in the UDP payload of a RADIUS package.

RFC 2865 defines the following RADIUS message types:

- **Access-Request.** Sent by a RADIUS client to request authentication and authorisation for a network access connection attempt.
- **Access-Accept.** Sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt is authenticated and authorised.
- **Access-Reject.** Sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt is rejected. A RADIUS server sends this message if either the credentials are not authentic or the connection attempt is not authorised.
- **Access-Challenge.** Sent by a RADIUS server in response to an Access-Request message. This message is a challenge to the RADIUS client that requires a response.

Annex B provides support for the implementation and deployment of RADIUS within a Microsoft Windows 2000 environment.

7.4 Access for maintenance

This type of remote access is provided to system administrators who connect when required to administer systems remotely. Due to the fact that this group of users has usually the highest access rights at the system, access has to be set up in the most secure way. Also, any activity conducted remotely has to be logged and audited afterwards, especially when system administration is outsourced to a service provider.

Therefore, access should only be provided to the specific computer which is to be administered remotely. The following measures are required:

- Access shall only be provided to a specific account on the defined machine;
- The communications between the remote user and the machine to be administered shall be protected using tools like SSH;
- The user has to be authenticated using strong authentication mechanisms;
- Every user allowed for remotely administering a system has to be trained in the appropriate mechanisms and procedures;
- Any action shall be logged;
- The logs should be audited immediately after a remote administration was conducted, or at the first opportunity in the case of an out-of-hours maintenance activity.

A call-back mechanism (requires additional safeguards, see also 8.2) is an option. Following these requirements restricts the risks implied with this type of remote access.

8 Guidelines for selection and configuration

8.1 General

The following clause will discuss the measures required to counter the threats identified. Each measure proposed will be explained in detail and the pros and cons will be introduced. The structure is so that the areas RAS client, RAS server and RAS communications will be introduced separately. Joint measures will be discussed in the end.

At this point we advise against considering the threats to the client and server completely separately since, for example, if a RAS client were to be compromised, the RAS server would automatically be endangered.

Moreover it should be borne in mind that, for example in the Windows environment, every RAS client can also be operated as a RAS server, so that the threats which apply to RAS servers may apply equally to a RAS client.

8.2 Protecting the RAS client

8.2.1 Stationary RAS client

A stationary client may first be protected physically, i.e. it may be kept in a room where only authorised people have access. This may be an appropriate approach for telecommuters who make use of a home office.

A stationary RAS client may be connected to the RAS server using a telephone modem, a cable modem or a DSL connection. The second and the third type of connection require additional measures for the broadband connection providing a permanent connection to the Internet. A simple approach is the installation and correct configuration of a so-called “personal firewall” which restricts access from the outside to the connected computer.

8.2.2 All RAS clients

For all RAS clients there are several levels of security applicable to avoid misuse of the computer and to secure the remote connection.

The first barrier to be established is the computer hardware itself. An easy approach to protect the computer and to avoid misuse is the installation of a boot password, which enforces the user’s identification prior to booting the system. This barrier is a first obstacle for potential attackers but it does not provide a sufficient protection.

A second obstacle is the operating system. For portable computers and workstations an operating system should be used which provides user identification and authentication. Most operating systems provide this feature. The account to be used should be a normal user account, not an administrator account because these accounts provide more privileges and therefore should only be used to administer a computer. Also bear in mind, that adequate password quality[1)] should be enforced.

If information considered of value for a company is stored on a computer then additional measures should be in place.

The operating system should be hardened providing better security than the off-the-shelf configuration. This implies that all unnecessary components of the operating system should be removed and only those applications installed that are needed. Also, features like network configuration are restricted in a way that only those services required for the specific system are allowed.

Strong authentication can be achieved using smart cards, token cards or biometric[2)] mechanisms. Strong authentication, also known as multi or two-factor authentication requires a user to fulfil at least two ways of identification[3)].

Hard disk encryption provides protection against disclosure of information stored. This confidentiality service has to make use of strong algorithms (see also ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*[4)]).

---

1) More information on password management can be found in ISO/IEC 17799.

2) Biometrics refers to the authentication of people based on physical or behavioral characteristics.

3) Authentication usually requires users to provide something they know (a password), something they possess (a token or smart card), something they are (a biometric characteristic), or sometimes a combination thereof, in order to provide evidence of their identity.

4) To be published.

Another important configuration issue is the modem configuration. The client modem has to be set up in a way that it generally does not accept incoming calls. This way a connection has to be initiated by the client user.

In many circumstances a personal firewall may improve security, if configured correctly.

Finally, to avoid and restrict damages caused by malicious code, an anti-virus program has to be installed and regularly updated.

8.3 Protecting the RAS server

8.3.1 Physical and logical set-up

For the RAS server physical security is a necessity. Usually, the RAS server is part of the server infrastructure of an enterprise and should have the same physical security as the other servers. Like any other services to the outside, a RAS server should be located within a DMZ. This includes protection against unauthorised physical access by keeping it locked away in a server room and against power failure in using a UPS. Other measures required are the secure set-up and configuration of the RAS server, the secure administration and the back-up and recovery procedures.

Although the most common type of RAS server is still a server providing modem access either using telephone line or ISDN, there are meanwhile solutions available where the dial-in takes place at a local service provider RAS outside the control of an enterprise. Further access is then provided by the Internet and is controlled and restricted by its perimeter, the firewall system.

The advantage of this approach is that costs are kept low (the dial in is usually a local call), the disadvantage is that the client has to be identified twice: at the ISP first and then again at the remote location.

8.3.2 RAS server and modem

For a RAS server providing modem access several measures should be in place to ensure that the modem provision does not introduce additional risks to the infrastructure.

The computer should be configured to fulfil the task of providing RAS services and all other services should be omitted. This implies that the operating system is hardened and all relevant upgrades and patches are applied. Only administrators and maintenance staff are allowed to physically access the server. Normal user accounts should not be installed.

If the RAS server also provides other services then it has to be tested and verified that the combination of services does not introduce new risks. Explicit configuration support for RAS may be provided by the vendor of the software.

Other important issues to be taken into account are the backup of data, the log information to be collected, the transfer of logs to a management station (including its daily evaluation) and the development of emergency plans.

Prior to actively providing remote access services the server shall be tested against known vulnerabilities. The tests shall include local configuration and network penetration testing.

A modem shall be configured to passively work in one direction, in this case, allowing incoming calls. If possible, the configuration shall allow the authentication at the modem and then initiate a call-back (also known as dial-back) to a pre-stored number. This call-back only works with stationary clients or laptops connected via mobile phones. This ensures that only known addresses (phone numbers) are connected and allows to restrict the costs for the calling entity.

Modern telephone equipment (e.g., PBX) provides features like re-routing of calls which may direct the call to a number other than intended. Therefore, call-back mechanisms need to be supplemented by additional safeguards.

As proposed for the client set-up, an anti-virus program has to be installed and regularly updated.

8.3.3 Network access server

If remote access is set up so that the dial-in takes place at a local Internet service provider (ISP) access to the network has to be controlled by a Network access server (NAS). Access to the ISP will then be out of direct control of the enterprise and the result of any authentication there will not be known to the enterprise.

A NAS has to be protected like any other network device, i.e. it has to be kept locked away that only authorised administrators get physical access. The management of the device should comply with the local policy: if a network management system is supervising its activities then the traffic between the management system and the NAS has to be either kept within the local network or tunnelled to hide its information type.

A NAS is a kind of gateway between the local enterprise network and the outside world; therefore the mechanisms proposed in ISO/IEC 18028-3 should be applied.

8.3.4 Wireless access points

Although Access Points (AP) for Wireless LAN are not a typical remote access scenario they may be used to provide access to a network. Therefore, such an AP, as access points for other wireless techniques, should be located in a DMZ and thus be protected. Additional information on wireless security is provided in 8.5.

8.4 Protecting the connection

8.4.1 General

The connection between RAS client and RAS server moves through a number of phases. In the beginning the connection will be established, then it will be operated and after use it will be terminated. All these communication phases require protection.

The following section will concentrate on the various steps to secure the connection respectively the communication between the RAS client and the RAS server.

8.4.2 Connection establishment

The establishment of a secure connection requires authentication of the remote user. This takes place when the protocol[5)] used for the remote access has been set up.

There are different ways of authenticating a user, which also differ in terms of security. The first two protocols are in use between a client (called the peer) and a server (the authenticator), the third protocol makes use of an authentication server which allows the inclusion of additional authentication schemes.

The most common authentication scheme makes use of the Password Authentication Protocol (PAP). PAP is a two-way handshake protocol where an authenticator - the server - receives the credentials of a peer – the client – and allows or refuses access based on these credentials. The credentials are sent in clear text and consist normally of a user ID and a password. Therefore this protocol does not provide protection against replay attacks.

A better authentication scheme is offered by the Challenge-Handshake Authentication Protocol (CHAP). CHAP is a three-way handshake protocol, where the authenticator sends a “challenge” to the peer. This challenge is unique and must be changed each time a challenge is sent. The peer responds with a hash value calculated on his ID parameters (the so-called “secret”) and the “challenge”. The authenticator compares the result with his calculations and either allows or refuses access. The credentials transferred are encrypted using a hash algorithm (most commonly used is MD5). CHAP protects against replay attacks for the challenge is not predictable.

---

5) For modem access the old protocol was the Serial Line Internet Protocol (SLIP) which only allowed simple authentication; now the Point-to-Point Protocol (PPP) offers a more reliable protocol and better authentication.

A more general approach is provided with the Remote Authentication Dial-in User Service (RADIUS) as introduced in 7.3.

The RADIUS server usually stores ID parameters of users centrally, i.e. it keeps the shared secrets for remote users. If a user wants to access a system in a network, he sends an “Access Request” to the RADIUS server containing the user ID, the password, the system ID and the system port the user is accessing. When a password is present it is masked using cryptographic means. The Radius server may either answer the request or forward it to another RADIUS server. If the RADIUS server answers the request, it will first verify that the data transmitted are valid. A valid identification must at least consist of user ID and password but may also include the system address and the port provided. If a request is forwarded to another RADIUS server then the originally addressed RADIUS server acts as a client. This way additional authentication may be enforced. Examples are UNIX authentication, Windows 2000 authentication or NOVELL authentication. A RADIUS server may also use the authentication schemes PAP and CHAP.

Other strong authentication to be used may be authentication using Digital Certificates or using tokens. This way the authentication not only relies on the knowledge of the user but also on the possession of a token or certificate; therefore it is called two-factor authentication. Biometric authentication may also be included.

Note: The older network service Terminal Access Controller Access Control System (TACACS) and its derivates XTACACS and TACACS+ are still existent but do not play a role as important as RADIUS.

8.4.3 Communications encryption

The threat of eavesdropping can only be countered using cryptography. Link encryption restricts communications to those facilities where the adequate encryption equipment is provided. Content encryption provides more flexibility and allows also connections to servers, which do not provide encryption. It also provides confidentiality only between the respective encryption end-points.

An example for content encryption is the use of software like Pretty Good Privacy (PGP), a software package that provides encryption based on public key cryptography thus also allowing services like non-repudiation and authenticity.

IMPORTANT: When using an encryption program, make sure that the key length in use is sufficient. Also, define procedures to verify the authenticity and validity of public key certificates received via email prior to importing and using them.

For remote access, sufficient ways to protect the contents of a communication is provided by the use of Virtual Private Networks (VPN). There are a number of products available that offer this kind of protection. Make sure that only standardised protocols will be used for the VPN. Guidance on this topic will be provided in a future International Standard (ISO/IEC 18028-5).

8.5 Wireless security

Wireless Protocols may be used in various scenarios in the area of remote access:

- Protocols such as Bluetooth are used to locally connect mobile phones, modems or broadband access components to a remote access client system.
- Wireless LAN protocols such as the protocols defined in IEEE 802.11 series of standards may be used to connect remote access client systems to public or private networks.

In most of these scenarios the organization providing remote access capabilities has no or only very limited influence on the configuration or setup of the involved wireless communications protocols:

As an example, a mobile user may connect a remote access client system by using a public wireless LAN access facility (so-called hot spot) offered at an airport. The wireless access infrastructure in this example is typically operated by an ISP and users or their organizations have no influence on configuration issues.

Even though wireless protocols provide some security services, these cannot be relied on in the context of the scenarios in the area of remote access.

Therefore if wireless protocols are to be allowed in conjunction to implement remote access capabilities, all required security services such as authentication or confidentiality need to be implemented by using the capabilities of higher level protocols as introduced in 8.3. A common approach is using tunnelling protocols such as IPsec or SSL/TLS to provide strong authentication and confidentiality.

For situations, where an organization can configure the wireless access infrastructure additional technical measures are required to secure the access point. There are currently three basic methods to secure access to an AP that are built into the IEEE 802.11 protocols:

- Service Set Identifier (SSID);
- Media Access Control (MAC) address filtering;
- Wired Equivalent Privacy (WEP) or WiFi Protected Access (WPA).

Even all three methods together may not provide adequate security for an organization.

The SSID provides a mechanism to segment a wireless network into multiple networks serviced by one or more APs. Each Access Point comes with a manufacturer's default SSID indicating the manufacturer of that AP and potentially other information related to the respective AP. Therefore, the SSID should be changed to an internal, not easily guessable SSID, which does not provide information on the organization operating the AP nor on the equipment itself. The minimal security requirement for an AP is to prohibit broadcasting its SSID; otherwise any listening device can record the SSID and try to connect to the AP in calling the correct SSID. Therefore, it is strongly recommended that APs be configured with broadcast mode disabled, although there are still ways to record an SSID which is not broadcasted.

While an SSID identifies an AP, a MAC address identifies the network interface of a computer. Each network interface card has a unique MAC address. To increase the security of the WLAN, an AP should identify the valid client computers by their MAC addresses, if possible[6)]. Although a spoofing of MAC addresses is possible, this adds some protection to the WLAN access.

WEP is known to have fundamental vulnerabilities which affect confidentiality, integrity and authenticity. However, it provides encryption for the communications using a shared key of either 40 or 104 bits. This key is concatenated with a 24-bit initialization vector, resulting in 64- or 128-bit key length. Due to the known weaknesses of the protocols, WEP keys should be changed frequently, thus increasing security. WPA – the successor of WEP – overcomes these weaknesses if configured correctly by providing temporal shared keys.

In addition to this, the use of the Dynamic Host Configuration Protocol (DHCP) provided by the AP with the “client reservation” feature (i.e. computer MAC addresses are bound to defined IP addresses) or static addresses is recommended.

In case of using non-routable IP addresses, change the internal IP subnet address (usually 192.168.0.0) to another subnet address. Also, prohibit administrative wireless access to the WAP and the wireless router to avoid modifications by attackers.

Finally, evaluate the status of your WLAN on a regular basis.

A detailed checklist on WLAN security is provided in Annex F.

8.6 Organizational measures

Organizational measures should include a Remote Access Policy, which defines the different roles of users, administrators and security personnel. Also, responsibilities of the people involved have to be defined. More information on an appropriate network policy (including remote access) will be given in ISO/IEC 18028-1. An example for a remote access policy is provided in Annex A.

---

6) Restricting access based on MAC address filtering may not be feasible in large wireless environments or certain operational situations.

For some mobile devices (e.g., PDA, smart phone) it may not be feasible to implement sufficient technical safeguards; therefore there may be a need for additional organizational measures to counter the risks.

Other topics to be covered under organizational measures are a contingency plan, backup, disaster recovery, training of personnel, user awareness and user training.

More information on these topics may be found in ISO/IEC 13335 and ISO/IEC 17799.

8.7 Legal considerations

Implementation of remote access technology should be undertaken in consideration of any applicable national legislative or regulatory constraints or requirements.

Implementers should ensure that adequate contractual and other legal aspects of remote access deployments are in place, to ensure recourse in event of unforeseen occurrences.

9 Conclusion

Remote access requires a well-planned approach starting with an adequate security policy and covers technical means as well as organizational and legal means.

Annex A
(informative)

Sample remote access security policy

A.1 Purpose

The purpose of this policy is to define standards for connecting to <Company Name>'s network from any host. These standards are designed to minimise the potential exposure to <Company Name> from damages which may result from unauthorised use of <Company Name> resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical <Company Name> internal systems, etc.

A.2 Scope

This policy applies to all <Company Name> employees, contractors, vendors and agents with a <Company Name>-owned or personally-owned computer or workstation used to connect to the <Company Name> network. This policy applies to remote access connections used to do work on behalf of <Company Name>, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

A.3 Policy

A.3.1 General

1. It is the responsibility of <Company Name> employees, contractors, vendors and agents with remote access privileges to <Company Name>'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to <Company Name>.

2. General access to the Internet for recreational use by immediate household members through the <Company Name> Network on personal computers is permitted for employees that have flat-rate services. The <Company Name> employee is responsible to ensure the family member does not violate any <Company Name> policies, does not perform illegal activities, and does not use the access for outside business interests. The <Company Name> employee bears responsibility for the consequences should the access be misused.

3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of <Company Name>'s network:

a. Acceptable Encryption Policy

b. Virtual Private Network (VPN) Policy

c. Wireless Communications Policy

d. Acceptable Use Policy

4. For additional information regarding <Company Name>'s remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

A.3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

2. At no time should any <Company Name> employee provide their login or email password to anyone, not even family members.

3. <Company Name> employees and contractors with remote access privileges must ensure that their <Company Name>-owned or personal computer or workstation, which is remotely connected to <Company Name>'s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

4. <Company Name> employees and contractors with remote access privileges to <Company Name>'s corporate network must not use non-<Company Name> email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct <Company Name> business, thereby ensuring that official business is never confused with personal business.

5. Routers for dedicated ISDN lines configured for access to the <Company Name> network must meet minimum authentication requirements of CHAP.

6. Reconfiguration of a home user's equipment for the purpose of split-tunnelling or dual homing is not permitted at any time.

7. Frame Relay must meet minimum authentication requirements of DLCI standards.

8. Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.

9. All hosts that are connected to <Company Name> internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.

10. Personal equipment that is used to connect to <Company Name>'s networks must meet the requirements of <Company Name>-owned equipment for remote access.

11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the <Company Name> production network must obtain prior approval from Remote Access Services and InfoSec.

A.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A.5 Terms and definitions

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable
TV coaxial cable	A cable modem accepts this coaxial cable and can receive data from the Internet at over 1,5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function.
DLCI	Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analogue signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialling into AOL or other Internet service provider (ISP). Being on a <Company Name>-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into <Company Name> and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavours of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signalling info.
Remote Access	Any access to <Company Name>'s corporate network through a non-<Company Name> controlled network, device, or medium.
Split-tunnelling	Simultaneous direct access to a non-<Company Name> network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into <Company Name>'s corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunnelling" through the Internet.

Annex B
(informative)

RADIUS implementation and deployment best practices

B.1 General

This annex provides advice on the use of RADIUS for Microsoft Windows 2000 environments and operating systems.

To address RADIUS security issues, you should abide by the following implementation and deployment best practices.

B.2 Implementation best practices

To address RADIUS security issues when implementing a RADIUS client, server, or proxy, use the following best practices:

- To provide data confidentiality for the entire RADIUS message, implement IPsec using ESP and an encryption algorithm such as 3DES.

  This is described in RFC 3162. By encrypting the entire RADIUS message with IPsec, sensitive RADIUS fields (such as the Request Authenticator field in the Access-Request message) and attributes (such as User-Password, Tunnel-Password, and the MPPE-Key attributes) are protected from viewing. An attacker must first decrypt the ESP-protected RADIUS message before they can analyse the RADIUS message contents. Support for certificate-based IPsec authentication is recommended to prevent an attacker from launching online attacks against a RADIUS server.

Alternately, or in conjunction with using IPsec, you should do the following:

1. Allow the configuration and use of shared secrets at least 32 hexadecimal digits long or at least 22 keyboard characters long.

2. Implement the use of the Message-Authenticator attribute for all Access-Request messages.

   For a RADIUS client, implement the use of the Message-Authenticator attribute for all Access-Request messages and allow for its configuration. For a RADIUS server or proxy, implement the required use of the Message-Authenticator attribute for all Access-Request messages and allow for its configuration.

3. Implement a cryptographic-quality random generator for the Request Authenticator.

To provide additional protection for access client authentication in your RADIUS implementation, use the following best practices:

1. Implement EAP and EAP types that use strong authentication methods.

   A good example of a strong EAP method is EAP-TLS, which requires the exchange of access client and RADIUS server certificates. All EAP messages require the Message-Authenticator attribute, which provides protection for Access-Request messages that are not protected with IPsec.

2. Implement authentication methods that use mutual authentication.

With mutual authentication, both ends of the connection authenticate their peer. If either authentication fails, the connection attempt is rejected. For example, EAP-TLS and MS-CHAP v2 are mutual authentication methods. With EAP-TLS, the RADIUS server validates the user certificate of the access client and the access client validates the computer certificate of the RADIUS server. With MS-CHAP v2, both the access client and the access server provide proof of the knowledge of the user account's password.

3. If you implement PAP authentication, disable its use by default.

   For example, OTP/Token Card uses PAP to send the authentication information. If you must implement PAP, disable its use by default and implement long shared secrets and cryptographic-quality Request Authenticators. Because IEEE 802.1X does not support PAP, this issue only applies to PPP connections.

4. If you implement CHAP authentication, use a strong CHAP challenge.

   Like the RADIUS Request Authenticators, the CHAP challenge should be random and of cryptographic quality.

5. If you implement MS-CHAP authentication, do not support LAN Manager encoding of MS-CHAP challenge responses or password changes.

B.3 Deployment best practices

To address RADIUS security issues when deploying a RADIUS solution, use the following deployment best practices:

- To provide data confidentiality for the entire RADIUS message, configure your RADIUS clients and servers to use IPsec with ESP with 3DES for all RADIUS traffic.

  The configuration of IPsec ESP with 3DES for RADIUS traffic depends on the IPsec implementation. For example, if you are using Windows 2000 Routing and Remote Access service as an access server and Windows 2000 IAS as a RADIUS server in an Active Directory™ service domain environment, you can configure the active IPsec policy for the appropriate system container with a rule that uses ESP and 3DES encryption for all traffic to and from UDP ports 1812 and 1813. For more information, see Windows 2000 Server Help.

Alternately, or in conjunction with using IPsec, you should do the following:

1. Use strong shared secrets consisting of a random sequence of hexadecimal digits at least 32 digits long or a random sequence of upper and lower case letters, numbers, and punctuation at least 22 characters long. Ideally, the shared secret should be computer- generated.

2. Use a different shared secret for each RADIUS client–RADIUS server pair.

3. Require the use of the Message-Authenticator attribute for all Access-Request messages.

   Configure each RADIUS client to send the Message-Authenticator attribute with all Access-Request messages. Configure each RADIUS server to require each RADIUS client to send the Message-Authenticator attribute with all Access-Request messages.

4. Use RADIUS clients, servers, and proxies that use cryptographically strong Request Authenticators.

To provide additional protection for access client authentication for your RADIUS deployment, use the following best practices:

1. If PAP is not required, disable its use at the access server and at the RADIUS server.

The only acceptable usage of PAP for secure connections is with OTP and Token Card authentication, where the password has high entropy and changes for each use. However, enabling PAP allows mis-configured access clients to negotiate PAP with their access servers and send unprotected user account passwords. A better solution is to use EAP and EAP types for OTP and Token Card authentication.

2. If MS-CHAP is required, disable the use of LAN Manager encoding.

   If you are using Windows 2000 IAS, set the value of the registry key **HKEY_LOCAL_MACHINE \System \CurrentControlSet\Services\RemoteAccess\Policy\Allow LM Authentication** to 0 on the IAS server.

3. Use EAP and an EAP type with a strong authentication method.

   IEEE 802.1x authentication for wireless access points requires the use of EAP, uses the Message-Authenticator attribute to protect each Access-Request message, and does not support PAP authentication.

4. Use a mutual authentication method such as EAP-TLS or MS-CHAP v2.

Annex C
(informative)

The two modes of FTP

There are two FTP modes:

- PORT mode FTP and
- PASV mode FTP.

C.1 PORT-mode FTP

PORT mode is the traditional FTP mode. The sequence of events for a PORT FTP connection would go like this:

1. **FTP client:** This opens random response ports in the high number range. (For the purposes of this example, we'll assume ports TCP 6000 and TCP 6001.)
2. **FTP client:** This sends a request to open a command channel from its TCP port 6000 to the FTP server's TCP port 21.
3. **FTP server:** This sends an OK from its TCP port 21 to the FTP client's TCP port 6000 (the command channel link). The command channel is established at this point.
4. **FTP client:** This sends a data request (PORT command) to the FTP server. The FTP client includes in the PORT command the data port number it opened to receive data. In this example, the FTP client has opened TCP port 6001 to receive the data.
5. **FTP server:** The FTP server opens a *new* inbound connection to the FTP client on the port indicated by the FTP client in the PORT command. The FTP server source port is TCP port 20. In this example, the FTP server sends data from its own TCP port 20 to the FTP client's TCP port 6001.

In this conversation, two connections were established: an outbound connection initiated by the FTP client and an inbound connection established by the FTP server. Note that the information contained in the PORT command (sent over the command channel) is stored in the data portion of the packet.

C.2 PASV-mode FTP

The most popular FTP implementation is the Passive or PASV mode. PASV-mode FTP connections are the default on most popular browsers. One of the major advantages of PASV mode is that the server does not need to create a new inbound connection to the FTP client. As we'll see later, this makes PASV-mode FTP a bit more firewall-friendly.

A PASV-mode FTP sequence of events would go like this:

1. **FTP client:** This opens random response ports in the high number range. (For the purposes of this example, we'll assume ports TCP 6000 and TCP 6001.)
2. **FTP client:** This sends a request to open a command channel from its TCP port 6000 to the FTP server's TCP port 21.
3. **FTP server:** This sends an OK from its TCP port 21 to the FTP client's TCP port 6000. The command channel is now established.

4. **FTP client:** This sends a PASV command requesting that the FTP server open a port number that the FTP client can connect to establish the data channel.

5. **FTP server:** This sends over the command channel the TCP port number that the FTP client can initiate a connection to establish the data channel. In this example, the FTP server opens port 7000.

6. **FTP client:** This opens a new connection from its own response port TCP 6001 to the FTP server's data channel 7000. Data transfer takes place through this channel.

Note that the PASV-mode FTP client initiates all connections. The FTP server never needs to create a new connection back to the FTP client.

Annex D
(informative)

Checklists for secure mail service

The following checklists help to plan, configure and operate a Mail Server, They cover topics like the operating system, Mail Security, Contents Filtering, etc.

D.1 Mail server operating system checklist

Completed	Action
	Plan the configuration and deployment of mail server
O	Identify functions of the mail server
O	Identify categories of information that will be stored, processed, and transmitted through the mail server
O	Identify security requirements of information
O	Identify a dedicated host to run the mail server
O	Identify network services that will be provided or supported by the mail server
O	Identify users and categories of users of the mail server and determine privilege for each category of user
O	Identify user authentication methods for the mail server
	Choose appropriate operating system for mail server
O	Minimal exposure to vulnerabilities
O	Ability to restrict administrative or root level activities to authorised users only
O	Ability to deny access to information on the server other than that intended to be available
O	Ability to disable unnecessary network services that may be built into the operating system or server software
O	Acceptable costs for insurance and liability (some insurers charge more for certain operating systems)
O	Available experienced staff to install, configure, secure, and maintain the operating system
	Patch and upgrade operating system
O	Identify and install all necessary patches and upgrades to the operating system
O	Identify and install all necessary patches and upgrades to applications and services included with the operating system
	Remove or disable unnecessary services and applications
O	Disable or remove unnecessary services and applications
	Configure operating system user authentication
O	Remove or disable unneeded default accounts and groups
O	Disable non-interactive accounts
O	Create the user groups for the particular computer
O	Create the user accounts for the particular computer
O	Check the organization's password policy, and set account passwords appropriately (e.g., length, complexity)
O	Configure computer to deny login after a limited number of failed attempts
O	Install and configure other security mechanisms to strengthen authentication
	Test the security of the operating system
O	Test operating system after initial install to determine vulnerabilities
O	Test operating system periodically (e.g., quarterly) to determine new vulnerabilities

D.2 Mail server and content security checklist

Completed	Action
	Hardening the mail server application
O	Install the server software on a dedicated host
O	Install minimal Internet services required
O	Apply any patches or upgrades to correct for known vulnerabilities
O	Remove or disable all services installed by the mail server application but not required (e.g., Web based mail, FTP, remote administration)
O	Remove all vendor documentation from server
O	Apply appropriate security template or hardening script to server
O	Reconfigure SMTP, POP and IMAP service banner (and others as required) NOT to report mail server and operating system type and version.
O	Disable dangerous or unnecessary mail commands (e.g., VRFY and EXPN)
	Configuring operating system and mail server access controls
O	Limit the access of the mail server application to a subset of computational resources
O	Limit the access of users through additional access controls enforced by the mail server, where more detailed levels of access control are required
O	Configure mail server application to execute only under a unique individual user and group identity with restrictive access controls
O	Ensure the mail server is not running as root or system/administrator
O	Configure host operating system so that mail server can write log files but not read them
O	Configure host operating system so that temporary files created by mail server application are restricted to a specified and appropriately protected subdirectory
O	Configure host operating system so that access to any temporary files created by mail server application is limited to the mail server process(es) that created these files
O	Ensure that mail server cannot save files outside of the specified files structure dedicated to the mail server
O	Configure mail server to run in chroot jail on Linux and Unix hosts
O	Install users mail boxes on a different hard drive or logical partition than the operating system and mail server application
O	Limit the size of attachments that are allowed
O	Ensure log files are stored in a location that is sized appropriately
	Coping with harmful attachment and content
O	Implement a centralised virus scanner (either on mail gateway, firewall and/or mail server)
O	Install virus scanners on all client hosts
O	Update all virus databases on all scanner or a weekly basis or when there is a particular virulent outbreak
O	Educate users on the dangers of viruses and how to minimise those dangers
O	Notify users when an outbreak occurs
O	Configure content filtering to block suspicious messages
O	Configure content filtering to block UCE messages
O	Configure lexical analysis if required
O	Create a content filtering policy
O	Add legal disclaimer to emails, if required
O	Configure mail server to block mail from open relay blacklists
O	Configure mail server to block mail from specific domains, if required
O	Configure authenticated mail rely on server
O	Configure mail server to use encrypted authentication
O	Configure mail server to support Web access only via SSL/TLS and only if such access is deemed necessary

D.3 Network infrastructure checklist

Completed	Action
	Network location
O	The mail server is located on the internal network and protected by a mail gateway and/or firewall, or The mail server is located in a DMZ
	Firewall configuration
O	Mail server is protected by a firewall
O	Mail server if it faces a higher threat or if it is more vulnerable, is protected by an application layer firewall
O	Firewall controls all traffic between the Internet and the mail server
O	Firewall blocks all inbound traffic to the mail server except TCP port 25 (SMTP), TCP port 110 (POP3), TCP port 143 (IMAP), TCP port 398 LDAP) and TCP port 636 (secure LDAP), if required
O	Firewall blocks (in conjunction with the intrusion detection system) IP addresses or subnets that the IDS reports are attacking the organizational network
O	Firewall notifies the network administrator or mail server administrator of suspicious activity through an appropriate means
O	Firewall provides content filtering (application layer firewall)
O	Firewall is configured to protect against DoS attacks
O	Firewall logs critical events
O	Firewall and firewall operating system patched to latest or most secure level
	Intrusion detection systems
O	IDS configured to monitor network traffic before any firewall or filter router (network based)
O	IDS configured to monitor traffic network traffic to and from the mail server after firewall
O	IDS configured to monitor changes to critical files on mail server (host based or file integrity checker)
O	IDS blocks (in conjunction with the firewall) IP addresses or subnets that are attacking the organizational network
O	IDS notifies the network or mail server administrator of attacks through appropriate Means
O	IDS configured to detect port scanning probes
O	IDS configured to detect DoS attacks
O	IDS configured to log events
O	IDS updated with new attack signatures frequently (weekly basis)
O	IDS configured to monitor the system resources available on the mail server host (host based)
	Network switches
O	Network switches are used on mail server network segment to protect against network eavesdropping
O	Network switches are configured in high-security mode to defeat ARP spoofing and ARP poisoning attacks
O	Network switches are configured to send all traffic on network segment to IDS host (network based)

D.4 Mail client security checklist

Completed	Action
	Patching and updating mail clients
O	Update email client to most secure version
O	Apply any necessary patches to email client
O	Apply any necessary patches to browser (for email clients that are integrated with browser (e.g., Outlook and Netscape)
	Mail client security
O	Ensure operating system is updated to most secure patch level
O	Configure operating system to allow access to locally stored messages and mail client configuration files only to appropriate user(s)
O	Secure or remove Windows Scripting Host (Windows hosts only)
O	Change the default action on files associated with the Windows Scripting Host from execute to edit (Windows hosts only)
O	Ensure that operating system is configured to show full file extensions (Windows hosts only)
O	Ensure the operating system enforces the concept of least privilege because malicious code runs in the security context on which it was launched (i.e., the user's access level)
O	Ensure that critical components of the operating system are protected from malicious code
O	Use a file encrypting system to protect the mail stored locally on the user's hard drive (especially important for laptop computers)
O	Configure client operating system to automatically lock out after a fixed period of inactivity

D.5 Secure administration of mail server checklist

Completed	Action
	Logging
O	Log IP stack setup errors
O	Log resolver configuration problem (e.g., DNS, NIS, WINS)
O	Log mail server configuration errors (e.g., mismatch with DNS, local configuration error, out-of-date alias database)
O	Log improper file and directory permissions, unsafe symlinks, and hard links
O	Log out of date alias database(s)
O	Log lack of system resources (e.g., disk space, memory, CPU)
O	Log alias database rebuilds
O	Log logons (successful and failed)
O	Log security problems (e.g., spamming)
O	Log lost communications (network problems)
O	Log protocol failures
O	Log connection timeouts
O	Log connection rejections
O	Log use of VRFY and EXPN commands
O	Log send on behalf of
O	Log send as
O	Log download
O	Log malformed addresses
O	Log message collection statistics
O	Log creation of error messages

Completed	Action
O	Log delivery failures (permanent errors)
O	Log messages being deferred (transient errors)
O	Store logs on a separate (syslog) host
O	Archive logs according to organizational requirements
O	Review logs daily
O	Review logs weekly (for more long-term trends)
O	Use automated logfile analysis tool(s)
	Mail server backups
O	Create a mail server backup policy
O	Back up mail server incrementally on a daily to weekly basis
O	Back up mail server fully on a weekly to monthly basis
O	Periodically archive backups
	Recovering from a compromise
O	Consult the organization's security policy (this should take precedence over the recommendations provided here)
O	Disconnect compromised system(s) from network or take steps to contain attack so additional evidences can be collected
O	Investigate other "similar" hosts to determine if the attacker has also compromised other systems
O	Consult with management, legal counsel, and law enforcement as appropriate (contact law enforcement immediately if prosecution is desired)
O	Analyse the intrusion
O	Restore the system
O	Reconnect system to network
O	Test system to ensure security
O	Monitor system and network for signs that the attacker is attempting to access the system or network again
O	Document lessons learned

Annex E
(informative)

Checklists for secure web services

The following checklists are intended to support in the planning, installation and operation of a secure web server.

E.1 Web server operating system checklist

Completed	Action
	Plan the configuration and deployment of Web server
O	Identify functions of the Web server
O	Identify categories of information that will be stored, processed, and transmitted through the Web server
O	Identify security requirements of information
O	Identify how information is published to the Web server
O	Identify a dedicated host to run the Web server
O	Identify network services that will be provided or supported by the Web server
O	Identify users and categories of users of the Web server and determine privilege for each category of user
O	Identify user authentication methods for the Web server
	Choose appropriate operating system for Web server
O	Minimal exposure to vulnerabilities
O	Ability to restrict administrative or root level activities to authorised users only
O	Ability to deny access to information on the server other than that intended to be available
O	Ability to disable unnecessary network services that may be built into the operating system or server software
O	Acceptable costs for insurance and liability (some insurers charge more for certain operating systems)
O	Available experienced staff to install, configure, secure, and maintain the operating system
	Patch and upgrade operating system
O	Identify and install all necessary patches and upgrades to the operating system
O	Identify and install all necessary patches and upgrades to applications and services included with the operating system
O	Remove or disable unnecessary services and applications
O	Disable or remove unnecessary services and applications
O	Configure operating system user authentication
O	Remove or disable unneeded default accounts and groups
O	Disable non-interactive accounts
O	Create the user groups for the particular computer
O	Create the user accounts for the particular computer
O	Check the organization's password policy, and set account passwords appropriately (e.g., length, complexity)
O	Configure computer to deny login after a limited number of failed attempts
O	Install and configure other security mechanisms to strengthen authentication
	Test the security of the operating system
O	Test operating system after initial install to determine vulnerabilities
O	Test operating system periodically (e.g., quarterly) to determine new vulnerabilities