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.

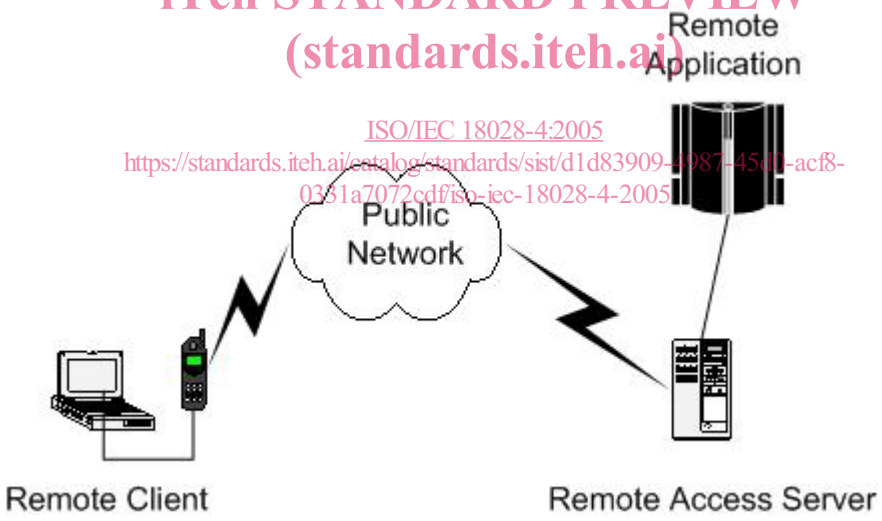

Figure 1 — Remote Access to Resources

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.

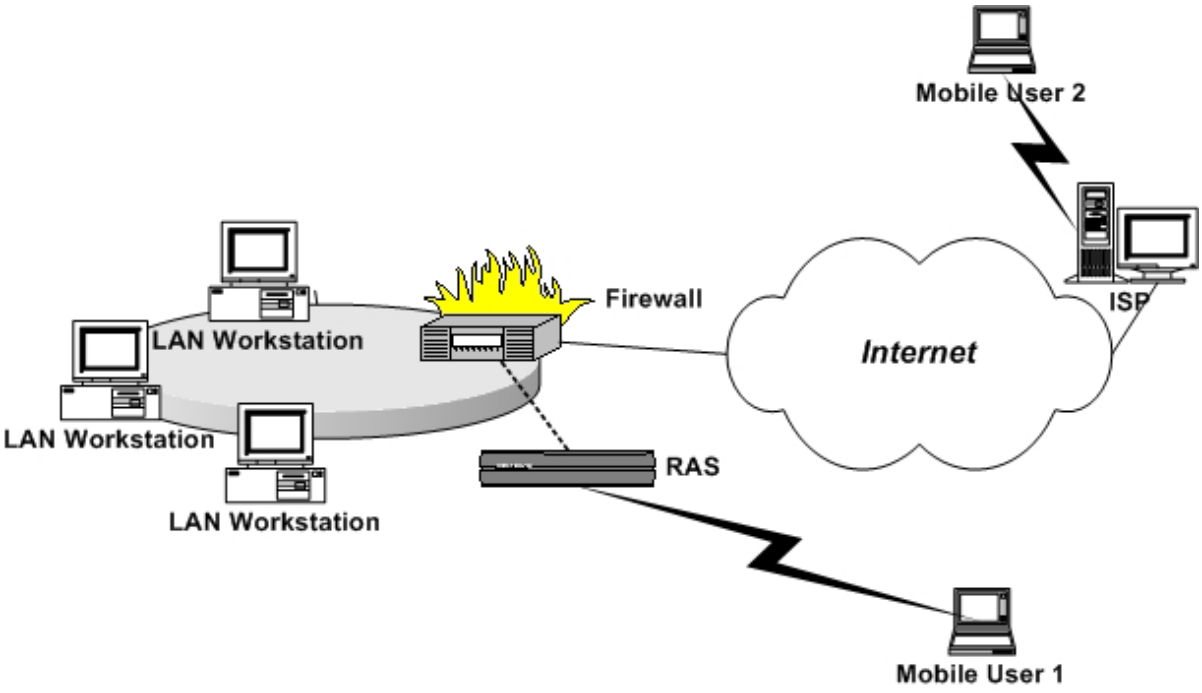

Figure 2 — Types of Remote Access

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").