
**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

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

This document is a preview generated by EVS

© ISO/IEC 2005

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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.....	v
Introduction	vi
1 Scope.....	1
2 Terms, definitions and abbreviated terms.....	1
3 Aim.....	5
4 Overview	6
5 Security requirements	7
6 Types of remote access connection	8
7 Techniques of remote access connection	9
7.1 General	9
7.2 Access to communications servers.....	9
7.3 Access to LAN resources.....	13
7.4 Access for maintenance	14
8 Guidelines for selection and configuration.....	14
8.1 General	14
8.2 Protecting the RAS client	15
8.3 Protecting the RAS server.....	16
8.4 Protecting the connection.....	17
8.5 Wireless security.....	18
8.6 Organizational measures	19
8.7 Legal considerations	20
9 Conclusion.....	20
Annex A (informative) Sample remote access security policy.....	21
A.1 Purpose	21
A.2 Scope.....	21
A.3 Policy.....	21
A.4 Enforcement	22
A.5 Terms and definitions.....	23
Annex B (informative) RADIUS implementation and deployment best practices.....	24
B.1 General	24
B.2 Implementation best practices	24
B.3 Deployment best practices	25
Annex C (informative) The two modes of FTP	27
C.1 PORT-mode FTP	27
C.2 PASV-mode FTP	27
Annex D (informative) Checklists for secure mail service	29
D.1 Mail server operating system checklist.....	29
D.2 Mail server and content security checklist.....	30
D.3 Network infrastructure checklist.....	31
D.4 Mail client security checklist.....	32
D.5 Secure administration of mail server checklist	32
Annex E (informative) Checklists for secure web services.....	34
E.1 Web server operating system checklist	34
E.2 Secure web server installation and configuration checklist	35
E.3 Web content checklist	36

E.4 Web authentication and encryption checklist..... 37
E.5 Network infrastructure checklist 37
E.6 Secure web server administration checklist 38
Annex F (informative) Wireless LAN security checklist..... 40
Bibliography..... 42

This document is a preview generated by EVS

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.

This document is a preview generated by EVS

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