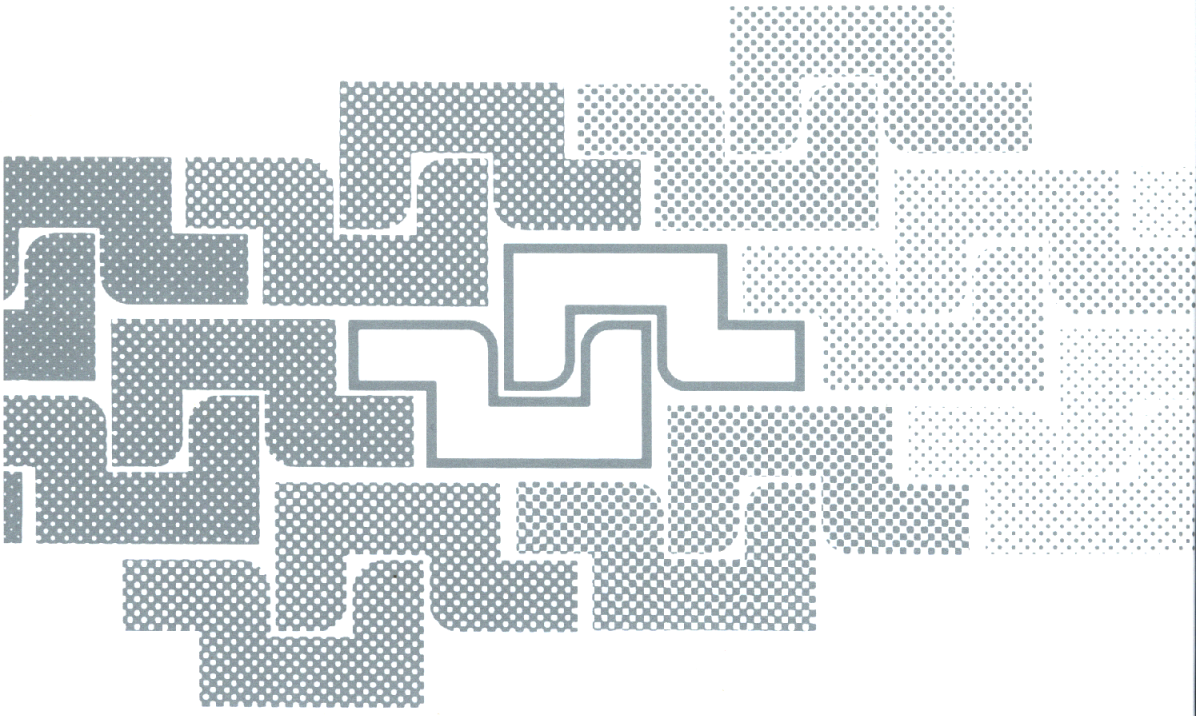


Advanced Security Technologies in Networking

Edited by
Borka Jerman-Blažič
Wolfgang S. Schneider
Tomaž Klobučar

IOS Press
Ohmsha

NATO Science Series

Series III: Computer and Systems Sciences - Vol. 178

ADVANCED SECURITY TECHNOLOGIES IN NETWORKING

NATO Science Series

A series presenting the results of scientific meetings supported under the NATO Science Programme.

The series is published by IOS Press and Kluwer Academic Publishers in conjunction with the NATO Scientific Affairs Division.

Sub-Series

I.	Life and Behavioural Sciences	IOS Press
II	Mathematics, Physics and Chemistry	Kluwer Academic Publishers
III.	Computer and Systems Sciences	IOS Press
IV.	Earth and Environmental Sciences	Kluwer Academic Publishers

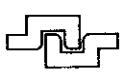
The NATO Science Series continues the series of books published formerly as the NATO ASI Series.

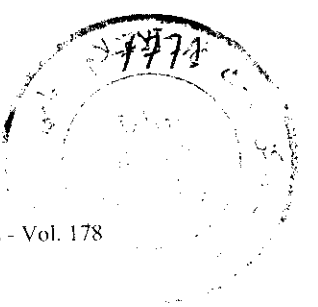
The NATO Science Programme offers support for collaboration in civil science between scientists of countries of the Euro-Atlantic Partnership Council. The types of scientific meeting generally supported are "Advanced Study Institutes" and "Advanced Research Workshops", and the NATO Science Series collects together the results of these meetings. The meetings are co-organized by scientists from NATO countries and scientists from NATO's Partner countries - countries of the CIS and Central and Eastern Europe.

Advanced Study Institutes are high-level tutorial courses offering in-depth study of latest advances in a field.
Advanced Research Workshops are expert meetings aimed at critical assessment of a field, and identification of directions for future action.

As a consequence of the restructuring of the NATO Science Programme in 1999, the NATO Science Series was re-organized to the four sub-series noted above. Please consult the following web sites for information on previous volumes published in the series:

http://www.nato.int/science
http://www.wkap.nl
http://www.iospress.nl
http://www.wtv-books.de/nato_pco.htm





Series III: Computer and Systems Sciences - Vol. 178 ISSN: 1387-6694

Advanced Security Technologies in Networking

Edited by

Borka Jerman-Blažič

Laboratory for Open Systems and Networks, Institut "Jožef Stefan", Ljubljana, Slovenia
Faculty of Economics, University of Ljubljana, Ljubljana, Slovenia

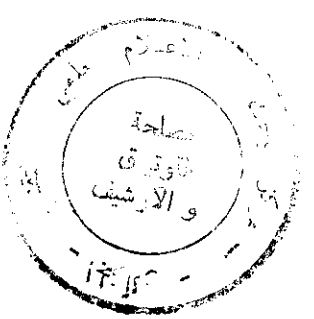
Wolfgang S. Schneider

Security and Smartcard Technology Department, GMD, Darmstadt, Germany

and

Tomaž Klobučar

Laboratory for Open Systems and Networks, Institut "Jožef Stefan", Ljubljana, Slovenia



IOS Press
Ohmsha

Amsterdam • Berlin • Oxford • Tokyo • Washington, DC

Published in cooperation with NATO Scientific Affairs Division

Proceedings of the NATO Advanced Networking Workshop on
Advanced Security Technologies in Networking
29 May–2 June 2000
Portorož, Slovenia

ISBN 1 58603 156 2 (IOS Press)
ISBN 4 274 90421 0 C3041 (Ohmsha)
Library of Congress Catalog Card Number: 00-112329

Publisher
IOS Press
Nieuwe Hemweg 6B
1013 BG Amsterdam
Netherlands
fax: +31 20 620 3419
e-mail: order@iospress.nl

Distributor in the UK and Ireland
IOS Press/Lavis Marketing
73 Lime Walk
Headington
Oxford OX3 7AD
England
fax: +44 1865 75 0079

Distributor in the USA and Canada
IOS Press, Inc.
5795-G Burke Centre Parkway
Burke, VA 22015
USA
fax: +1 703 323 3668
e-mail: iosbooks@iospress.com

Distributor in Germany, Austria and Switzerland
IOS Press/LSL.de
Gerichtsweg 28
D-04103 Leipzig
Germany
fax: +49 341 995 4255

Distributor in Japan
Ohmsha, Ltd.
3-1 Kanda Nishiki-cho
Chiyoda-ku, Tokyo 101
Japan
fax: +81 3 3233 2426

PRINTED IN THE NETHERLANDS

Foreword

Security in telecommunications and networking, especially when electronic commerce is involved, is one of the most crucial services offered in the global networks. For the most part, interconnected networks all over the world use a common set of protocols (i.e. the protocol suite TCP/IP), making up the Internet. In general, users of the computer network services are largely unaware of the potential threats to their information, or they choose to ignore such threats. However, the increasing usage of Internet services in all levels of business, education, information, entertainment and every day life has brought the importance of the protection of data, resources and identities to the fore. New applications built up within the paradigm of e-commerce are offering different level of protection and security. Recently, the Internet has started to spread "over the air" to merge with mobile communication network, thus making a new broad range of services available to the new e-conomy. Since these new services take place in a public and therefore in un-trusted networks, there are many security issues involved that are of concern to different communities e.g.:

- Commercial companies and their clients who want to do business over open networks need protection of resources and exchanged data,
- Administrations, public medical and social services, for whom it is vital that only approved groups are able to participate in their operations,
- Organisations for their external and internal network communication,
- The research community, and institutions involved in provision of digital contents related to the cultural heritage.

All these users need security services within an established infrastructure and applications, such as secured e-mail, secured Directory, secured file transfer, or secured World Wide Web applications. Lack of established security infrastructure, and the knowledge of how to set it up and use it, are the major obstacles in better proliferation of secured applications in open networks, such as tele-medicine, tele-working, business-to-business e-commerce and distance education. This book provides a broad overview of the basic aspects of technology, services and applications that enable safe and secured data exchange in un-trusted network as well as verification of identities of the participants taking part in the ubiquitous e-conomy and e-business.

The first part of the book address the basic concept of security in networking and cryptography. The second introduces the notion of security infrastructure in mobile and terrestrial networks. The next part of the book gives overview of the security provided at network levels and introduces virtual private networks (VPNs); VPN deployment has been made possible by the utilisation of security techniques. The next parts of the book deal with security provision in applications like World Wide Web, Videoconferencing, Tele-medicine and Secure Directories and Firewalls. The last parts of the book is dedicated to specific secure electronic commerce applications such as electronic payments systems and protocols, digital signature techniques and the legal aspects of secure electronic communication.

Most of the papers in this book were presented in the NATO Advanced Workshop on Security in Networking that took place in Portorož, Slovenia, from May 29 to June 2, 2000. In that context I want to express my deep appreciation to all lecturers that made this event success due to their excellent talks and papers. Special thanks go also to the Organizing Committee members and to the other two co-editors of this book.

Borka Jerman-Blažič

Co-director of NATO Advanced Workshop on Security in Networking

Contents