IFIP

SECURE INFORMATION NETWORKS
Communications and Multimedia Security

Preneel

SECURE INFORMATION NETWORKS

Communications and Multimedia Security

Edited by
Bart Preneel

IFIP

KLUWER
ACADEMIC
PUBLISHERS

SECURE INFORMATION NETWORKS

Communications and Multimedia Security

IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS'99) September 20-21, 1999, Leuven, Belgium

Edited by

Bart Preneel
Katholieke Universiteit Leuven
Belgium

KLUWER ACADEMIC PUBLISHERS
BOSTON / DORDRECHT / LONDON

Distributors for North, Central and South America:
Kluwer Academic Publishers
101 Philip Drive
Assinippi Park
Norwell, Massachusetts 02061 USA
Telephone (781) 871-6600
Fax (781) 871-6528
E-Mail <kluwer@wkap.com>

Distributors for all other countries:
Kluwer Academic Publishers Group
Distribution Centre
Post Office Box 322
3300 AH Dordrecht, THE NETHERLANDS
Telephone 31 78 6392 392
Fax 31 78 6546 474
E-Mail <services@wkap.nl>

Electronic Services <http://www.wkap.nl>

Library of Congress Cataloging-in-Publication Data

IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (1999 : Louvain, Belgium)
Secure information networks : communications and multimedia security : IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS'99), September 20-21, 1999, Leuven, Belgium / edited by Bart Preneel.
p. cm. — (International Federation for Information Processing ; 23)
Includes bibliographical references.
ISBN 0-7923-8600-0
1. Computer networks—Security measures Congresses. 2. Multimedia systems—Security measures Congresses. 3. Computer security Congresses. 4. Cryptography Congresses. 5. Computer network protocols Congresses. I. Preneel, Bart, 1963- . II. Title. III. Series: International Federation for Information Processing (Series) ; 23.
TK5105.59.I35 1999
005.8—dc21 99-37131
CIP

Printed on acid-free paper.

Printed in the United States of America.

SECURE INFORMATION NETWORKS
Communications and Multimedia Security

IFIP - The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the First World Computer Congress held in Paris the previous year. An umbrella organization for societies working in information processing, IFIP's aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

IFIP's mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.

IFIP is a non-profitmaking organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP's events range from an international congress to local seminars, but the most important are:

- The IFIP World Computer Congress, held every second year;
- open conferences;
- working conferences.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is small and by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is less rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

Any national society whose primary activity is-in information may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly, National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.

Preface

This volume contains papers presented at the fourth working conference on Communications and Multimedia Security (CMS'99), held in Leuven, Belgium from September 20-21, 1999. The Conference, arranged jointly by Technical Committees 11 and 6 of the International Federation of Information Processing (IFIP), was organized by the Department of Electrical Engineering of the Katholieke Universiteit Leuven.

The name "Communications and Multimedia Security'' was used for the first time in 1995, when Reinhard Posch organized the first in this series of conferences in Graz, Austria, following up on the previously national (Austrian) IT Sicherheit conferences held in Klagenfurt (1993) and Vienna (1994). In 1996, CMS took place in Essen, Germany; in 1997 the conference moved to Athens, Greece.

The Conference aims to provide an international forum for presentations and discussions on protocols and techniques for providing secure information networks. The contributions in this volume review the state-of-the-art in communications and multimedia security, and discuss practical experiences and new developments. They cover a wide spectrum of topics including network security, web security, protocols for entity authentication and key agreement, protocols for mobile environments, applied cryptology, watermarking, smart cards, and legal aspects of digital signatures.

The Program Committee, consisting of 23 members and 1 advisory member, considered 30 papers and selected 21 for presentation. The selection process was a difficult and challenging task, and I wish hereby to thank the members of the program committee for their hard work. Each submission was refereed by at least three reviewers. Reviews were anonymous and, whenever possible, constructive comments were provided to the authors resulting in improved versions of the submitted papers. I also gratefully acknowledge the assistance of several colleagues who reviewed submissions in their area of expertise: Johan Borst, Michael Bungert, Joris Claessens, Stefanos Gritzalis, Markus Jakobsson, Herbert Leitold, Keith Martin, Udo Payer, Vincent Rijmen, Peter Schartner, Diomidis Spinellis, Mark Vandenwauver, and Jean-Jacques Vandewalle.

I wish to thank especially Joris Claessens for providing assistance with processing the papers during submission, review and editing. I would also like to thank Vincent Rijmen for assistance with the editing process. Special thanks go to Reinhard Posch for support and advice during all the phases of the organization, and to Joos Vandewalle and his organizing committee for their assistance. Finally, I wish to thank all the authors who submitted papers; without their efforts this conference would not have been possible.

I hope that this volume presents a further step forward towards a more secure information society, and that it stimulates further research and applications.

Bart Preneel
Katholieke Universiteit Leuven
Department Electrical Engineering-ESAT
Kardinaal Mercierlaan 94
B-3001 Heverlee, BELGIUM
Email: bart.preneel@esat.kuleuven.ac.be

Conference Committees

CMS Conference Steering Committee

Chairman R. Posch, TU Graz, Austria

Members P. Horster, University of Klagenfurt, Austria
S. Katsikas, University of the Aegean, Greece
P. Kraaibeek, ConSecur, Germany
G. Pernul, University of Essen, Germany
R. Posch, TU Graz, Austria

Program Committee

Chairman B. Preneel, Katholieke Universiteit Leuven, Belgium

Members P. Ashley, Queensland University of Technology, Australia
A. Casaca, Inesc, Portugal
S. Fischer-Huebner, Hamburg University, Germany
W. Fumy, Siemens Corporate Technology - Security Technologies, Germany
D. Gollmann, Microsoft Research, UK
D. Gritzalis, Athens University of Economics and Business, Greece
P. Horster, University of Klagenfurt, Austria
S. Katsikas, University of the Aegean, Greece
L.R. Knudsen, University of Bergen, Norway
P. Kraaibeek, ConSecur, Germany
C.J. Mitchell, Royal Holloway, University of London, UK
D. Naccache, Gemplus, France
R. Oppliger, BFI, Switzerland
G. Pernul, University of Essen, Germany
R. Posch, TU Graz, Austria
G. Quirchmayr, University of Vienna, Austria
J.-J. Quisquater, Université Catholique de Louvain, Belgium
M. Reiter, Bell Labs, USA
D. Tygar, University of California at Berkeley, USA
P.C. van Oorschot, Entrust Technologies, Canada
S.H. von Solms, Rand Afrikaans University, South Africa
L. Yngstrøm, Stockholm University and Royal Institute of Technology, Sweden
Adv. Memb. L. Strous, De Nederlandsche Bank NV, The Netherlands

Organizing Committee

Chairman J. Vandewalle, Katholieke Universiteit Leuven

Members J. Claessens, Katholieke Universiteit Leuven
J. Nakahara Jr., Katholieke Universiteit Leuven
P. Noë, Katholieke Universiteit Leuven
V. Rijmen, Katholieke Universiteit Leuven
M. Vandenwauver, Katholieke Universiteit Leuven

Contents

Network Security: ATM and ISDN

Applied Cryptology I

Entity Authentication and Key Agreement Protocols

Applications

Network Security: IP

Protocols for Mobile Applications

Applied Cryptology II

Web Security

NETWORK SECURITY: ATM AND ISDN

SECURITY ON ATM NETWORKS

Stelios Karanastasis and Ahmed Patel
Department of Computer Science, University College Dublin,
Belfield Campus, Dublin 4, Ireland,
Tel: ++353 1 7062488,
stkara@aegean.gr, apatel@net-cs.ucd.ie

Abstract: This paper discusses the ATM security problems, requirements, implementation issues and challenges. It also presents a survey of the existing solutions aiming to secure the data transferred over an ATM network. Different solutions are presented analysed and compared. Details are given about the security services offered their placement within the ATM Reference Model and the techniques to provide synchronisation and dynamic key change during user data exchange.

1. INTRODUCTION

In recent years, security has been more and more significant in network environment with the emergence of the internetworking technology. The internetworking technology can provide the communication channels across networks so that, machines in different networks can talk to each other. However, the internetworking communication will be exposed to all kinds of attacks in such an open environment. Most of the network technologies, without integrating with security mechanism originally, have to be redesigned to provide some security services. ATM is one of those technologies.

The Asynchronous Transfer Mode (ATM) forms the basics for many broadband networks, and it forms part of the foundation for B-ISDN networks. ATM uses multiplexing, switching and segmentation/reassemble operations to support a high-speed transport network. It was designed to make Broadband-ISDN a reality. B-ISDN was created conceptually as just an extension of ISDN so it functions as a communication network that can provide integrated broadband services such as high speed data services, video phone, video conferencing, CATV services along with traditional ISDN services such as phone an telex. In order to have these services, an interface between the ATM layer and higher layers was necessary. The ATM adaptation layer provides this service. Its main purpose is to resolve any disparity between a service required by the user and services available at the ATM layer. It lies between the ATM layer and the higher layers of B-ISDN protocol reference model, as can be seen in *Figure 1* [I.321]. The user plane is responsible for users data exchange; the control plane monitors signalling information; and the management plane maintains the network operational.

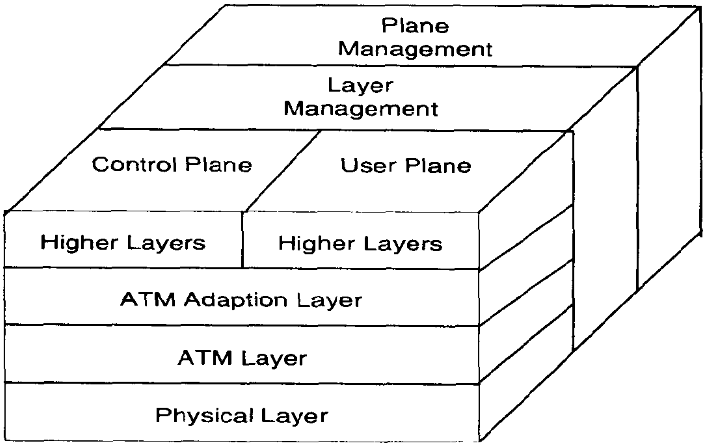

Figure 1. B-ISDN reference model and ATM

In fact, issues in ATM security have not gained enough attention until 1995, when a group within ATM Forum was established to address the security issues. Therefore, compared with other security area, ATM security is still in its beginning. Security in ATM networks is not only concerned with the user data but all the protocol control data as well. The later consists of both management and signalling information which needs to be made secure so that an attacker/intruder can't change pertinent or significant data in order to divert or destroy the proper functioning of the ATM network service (e.g. converting VCs). With no security services being currently offered in ATM specifications, communications passed over ATM networks will suffer a lot of threats. These threats are examined in section 2. Then we discuss the requirements of ATM security followed by the implementation of ATM security in the ATM architecture according to the standards proposed by the ATM Forum. In section 5, we describe, analyse and compare the different approaches of securing ATM networks. Finally in section 6 we discusses some major challenges in ATM security.

2. THREATS TO ATM NETWORKS

As other networks, ATM networks will suffer a lot of threats [Alles95], [Chuang96], [Deng95], [TayFin95], [Hanson95]. Typical ones are eavesdropping, spoofing, service denial, traffic analysis, VC stealing etc. Note that VC stealing is a new threats for networks since is only applies to ATM networks.

Eavesdropping: Eavesdropping refers to the threat that the attacker connects or taps into the transmission media and gain unauthorised access to the data. It is one of the most common attacks to the network. Although a hacker has to be familiar with the communication technology and relevant protocols operating at the tapping point, information that is widely available in academic environment. As the technology become matured, standards will be established and the technology will be well known, nothing will be protected by keeping the document secret [Hanson95].

Spoofing: Spoofing attack means that an attacker tries to impersonate another user to the third party therefore can get access to resources belonging to the victim to take advantages or just destroy them. Spoofing might need special tools to manipulate the protocol data unit and requires special access permissions. However, since a network will be connected to many untrusted networks via the Internet, it's almost impossible to prevent a hacker from getting this access permission or even trace the people with this particular access permission. ATM is being implemented in public domain. Therefore, it is subject to this kind of attack also.

Service Denial: ATM is a connection-oriented technique. A connection, which is called Virtual Circuit(VC) in ATM, is managed by a set of signals. VC is established by SETUP signals and can be disconnected by RELEASE or DROP PARTY signals. If an attacker sends RELEASE or DROP PARTY signal to any intermediate switch on the way of a VC, then the VC will be disconnected. By sending these signals frequently, the attacker can greatly disturb the communication between one user to another, therefore will disable the Quality of Service (QoS) in ATM. Combining this technique with other tricks like eavesdropping, the attacker can even completely block one user from another.

Traffic Analysis: Traffic analysis consists of an attack whereby the communication channel is tapped and statistical information about the data traffic is accumulated. Specifically, the volume, timing, source and destination addresses of communication data can be collected by the attacker. This information in conjunction with knowledge of the routing tables contained in the network switching devices (ATM switches will work with routing information which is unencrypted unless specific efforts are made to hide it) can be a very useful tool for the attacker. Thus extra provision needs to be made for protection against traffic analysis attack Another related threat is called convert channels. In this technique, the attacker can encode the information in the timing and volume of data, VCI, or even session key to release information to another people without being monitored. Normally, these two attacks aren't easy to implement. However, when ATM is used in an environment requiring stringent security, it might happen. [TayFin95]

Stealing of VCs: Switches are forwarding cells based on the VCI((Virtual Channel Identifier) or VPI(Virtual Path Identifier) in the cell header. If an attack manage to change these values at the end point switches of an ATM connection then he will be able to forward his cell via another connections that has for example better Quality of Service. The switches in the middle will not notice these changes and will switch the "faked" cells just like the authentic cells. In public packet-switching network, the attacker won't gain too much by this trick. However, in ATM network, if quality of service is guaranteed, then he can gain a lot by stealing a higher quality channel which he is not entitled to use according to the access control policy. The possibility that the end-point switches will compromise would be pretty low, if the ATM network is owned by one organisation. However, when we consider ATM internetworking, in which case cells will travel through different ATM networks, it will be very easy for two switches to compromise [Alles95].

A threat is a potential violation of a security objective. Summarising we can distinguish three kinds of threats [ATMForum98]:

- *An accidental threat*, where the origin of the threat does not involve any malicious intent
- *An administrative threat,* where the threat arises from a lack of administration of security
- *Intentional threats,* where the threat involves a malicious entity, which may attack either the communication itself or network resources.