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.

Communications and Multimedia Security

Proceedings of the IFIP TC6, TC11 and Austrian Computer Society joint working conference on communications and multimedia security, 1995

Edited by

Reinhard Posch
Institute for Applied Information Processing and Communications
Technical University of Graz
Graz, Austria

SPRINGER INTERNATIONAL PUBLISHING, CHAM

First edition 1995

© 1995 IFIP International Federation for Information Processing
Originally published by Chapman & Hall in 1995
Softcover reprint of the hardcover 1st edition 1995
ISBN 978-1-5041-2908-4 ISBN 978-0-387-34943-5 (eBook)
DOI 10.1007/978-0-387-34943-5

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the UK Copyright Designs and Patents Act, 1988, this publication may not be reproduced, stored, or transmitted, in any form or by any means, without the prior permission in writing of the publishers, or in the case of reprographic reproduction only in accordance with the terms of the licences issued by the Copyright Licensing Agency in the UK, or in accordance with the terms of licences issued by the appropriate Reproduction Rights Organization outside the UK. Enquiries concerning reproduction outside the terms stated here should be sent to the publishers at the London address printed on this page.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

A catalogue record for this book is available from the British Library

Printed on permanent acid-free text paper, manufactured in accordance with ANSI/NISO Z39.48-1992 and ANSI/NISO Z39.48-1984 (Permanence of Paper).

CONTENTS

Preface

In October 1994 the German newspaper *Die Zeit* published an article about the Washington museum on cryptography. Next to this article was placed the future of CD-ROM. From this it may be seen that public opinion is already beginning to make some connection between multimedia and security. In fact, these two areas have a close connection and start to show their social impact -- and thus the need of awareness. Doing an event about these two items should be an effort to bring these twofold views into an even closer relation. It is also a contribution to building social awareness for security needs when deploying multimedia applications. In this context, networks and multimedia security is one way of treating the social impact of electronic communication.

The term multimedia is placed right in the middle of technical communication, media and entertainment. It will need a lot of effort to build up ethics and rules, so that after a first phase of enthusiasm, multimedia will not be abused and drop into the twilight -- and thus earn a reputation it would not deserve.

The first associations in the public opinion with information security still are military, espionage, red telephone, etc. The museum of cryptology mentioned earlier contributed its share by exhibiting famous species like the ENIGMA. Placing activities in the area between multimedia and communication security shall also be an effort to gradually influence public opinion concerning this point.

IT security has moved and still is moving fast from the intelligence area to the commercial field. With smart cards and electronic payment, with electronic shopping and all the commercial applications around the internet, IT security will soon be omnipresent. Just to give one example of a step towards this end: Austria will experience the switch of all bank cards to a smart card system within a two month's time. Credit cards will follow in a few years.

Besides this fact that information security is moving towards commercial applications, we may as well observe two further trends:

First, in most cases we are not protecting life or military secrets but a limited amount of commercial risk. There is a temptation to delude security and to implement some obscurity and some guruism instead. But if we treat it the right way, it is the challenge to build a light weight security.

Second, unlike the military case, people will not really feel the need for security before they experience a damage. We cannot expect the general public to take the responsibility. The second demand therefore will be the integration of security. As it can be seen in examples like electronic mail systems and in program downloading like FTP, security without integration just does not happen.

There are already some efforts to integrate IT security. A very controversial example for this development is the famous CLIPPER technology. With its law enforcement features CLIPPER is a perfect example that IT security has tremendous social impact. All users should be taught the security goals and the side effects. Solutions like CLIPPER, putting most of its features in the confidentiality area, do not aim at this goal. They might even hinder or disfavor advanced

methods like escrow technologies. At what end? Asking this question one could come up with the idea that at the best such an effort as CLIPPER is to assure a forerunner position for strong national commercial interests.

Besides awareness, light weight security, and other goals mentioned, multimedia security also needs to work on the national and international protection policies. ITAR is one of the best examples how such regulations gain on influence. Since solutions as SSL and SHTTP as well as others are available, these solutions may only be efficiently exploited in some part of the world for legal reasons; it is open to judge on the effect but it definitely will lead to a diversification.

Unlike intelligence, commercial use demands for a maximum of knowledge about mechanisms, their effect and their capabilities. This conference shall contribute in the mentioned context to the technical understanding, and thus to setup means and regulations for using open networks with a maximum range of applications, still giving the confidence that the design goals of the network are not violated.

Reinhard Posch

Institute for Applied Information Processing and Communications Technology,
Graz University of Technology,
Klosterwiesgasse 32/I,A-8010 Graz
email: rposch@iaik.tu-graz.ac.at