Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

396

T.A. Berson T. Beth (Eds.)

Local Area Network Security

Workshop LANSEC '89
European Institute for System Security (E.I.S.S.)
Karlsruhe, FRG, April 3–6, 1989
Proceedings

Springer-Verlag
Berlin Heidelberg New York London Paris Tokyo Hong Kong

Editors

Thomas A. Berson
Anagram Laboratories
P.O. Box 791, Palo Alto, CA 94301, USA

Thomas Beth
Universität Karlsruhe, Fakultät für Informatik
Technologie-Fabrik Karlsruhe
Haid-und-Neu-Straße 7, D-7500 Karlsruhe 1, FRG

CR Subject Classification (1987): C.2.0, D.4.6, E.3

ISBN 3-540-51754-5 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-51754-5 Springer-Verlag New York Berlin Heidelberg

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
2145/3140-543210 – Printed on acid-free paper

Preface

An Invitational Workshop on Local Area Network Security (LANSEC) was held April 3-6, 1989 in Karlsruhe, Federal Republic of Germany. The purpose of the workshop was to assemble knowledge about technical issues of LAN security and to make this knowledge public. This volume is an edited collection of the papers presented at LANSEC, as modified by the authors based upon workshop discussions.

LANSEC was sponsored and funded by the European Institute for System Security (E.I.S.S.), an institute located at the University of Karlsruhe. E.I.S.S. was established in 1988 by the State Government of Baden-Württemberg to support the successful development of information technology in Europe by specialising in the key area of system security.

The director of E.I.S.S. is Professor Thomas Beth. He is a member of the Faculty of Computer Science in the University of Karlsruhe and of its Institute for Algorithms and Cognitive Systems.

LANSEC was organized and led by Dr. Thomas Berson of Anagram Laboratories in Palo Alto, California. He has worked in computer security since 1967. As early as 1982, at Sytek, Inc., he brought to market a LAN secured by end-to-end cryptography at the session layer. He is the current president of the International Association for Cryptologic Research.

LANSEC's invited participants were:

L. Kirk Barker (*Datotek*)
Steven Bruniges (*Retix Systems Ltd.*)
Morrie Gasser (*Digital Equipment Corporation*)
Russell Housley (*Xerox Special Information Systems*)
Kimberly E. Kirkpatrick (*MITRE Corporation*)
Paul Lambert (*Motorola*)
Brian P. Schanning (*Ungermann-Bass*)
Richard Ward (*British Telecom*)
Steve Wilbur (*University College London*)

We are grateful to the Land Baden-Württemberg, especially to the Ministerium für Wissenschaft und Kunst and the Staatsministerium Baden-Württemberg for sponsoring E.I.S.S., and, in turn, LANSEC. The workshop would not have been possible without the personal efforts of the participants and, in most cases, the understanding approval and support of their companies. Our warm thanks go also to the faculty, students, and staff of E.I.S.S. who not only were active LANSEC observers but who also provided logistic support, pastries and pizza. In this regard we especially thank Dieter Gollmann, Michael Vielhaber and Frau Renate Leppich. Hans Peter Riess took our group photograph. Lastly, we are grateful to the Editors of the Springer-Verlag Lecture Notes in Computer Science for helping us achieve our objective of publishing this information about the technical issues of local area network security.

Thomas A. Berson
Thomas Beth

July, 1989

LANSEC '89: (*Front Row, left to right*) Paul Lambert, Kimberly Kirkpatrick, Thomas Berson, Victoria Barnett, Brian Schanning, Richard Ward, Dieter Gollmann. (*Second Row*) Steven Wilbur, Morrie Gasser, Thomas Beth, Michael Vielhaber, Volker Hatz, Hans Peter Riess. (*Back Row*) Russell Housley, L. Kirk Barker, Steven Bruniges.

Contents

Section III: Management

Introduction

This introduction to LANSEC is adopted from an interview with Thomas A. Berson entitled **LAN Security Workshop Held in Germany**. It first appeared in *Data Security Letter* (DSL)[1].

DSL: *How did LANSEC come to be organized?*
BERSON: Prof. Beth and I are both directors of the International Association for Cryptologic Research (IACR). I visited the University of Karlsruhe two years ago to give a lecture on cryptography. He told me about E.I.S.S., which was still being formed, and asked me if I would organize a workshop on LAN security. That was very farsighted of him. The topic has become important to LAN designers and to the increasing number of LAN users.

DSL: *How many people attended LANSEC?*
BERSON: We were a small group. There were nine invited participants (besides myself). The United States, the United Kingdom, and the Federal Republic of Germany were represented. We were joined by some of the students doing work in the Institute. They study data privacy, data security, security mechanisms for open networks, and security mechanisms for information in computer systems. I was very impressed by the students there. They are talented, motivated, and hard-working.

DSL: *What was the purpose of the workshop?*
BERSON: The purpose of LANSEC was to assemble knowledge about technical issues of LAN security and to make this knowledge public.

DSL: *What were the themes of the workshop?*
BERSON: Our discussion focussed on several themes, including:

> What is a LAN?

> How is LAN security different from other network security?

> Integration of security mechanisms with existing standards, and the complication brought by framework models (such as OSI and IEEE).

> Layering principles (and layering of protocols in general).

> Layer 2 (data link) security issues.

> Security solutions are multi-layered. Authentication, key distribution, and traffic encryption all may happen at different layers of protocol.

> Network management of secure LANs.

> Interaction of security with existing network support tools.

> Migration from unsecure LANs to secure LANs.

> National security criteria, and evaluation of LANs against these criteria.

DSL: *What was the workshop's definition of a LAN?*
BERSON: A lot of the participants (all of the Americans, in fact) are involved in formulating the IEEE 802.10 Standard for Interoperable LAN Security (SILS). Kimberly Kirkpatrick of MITRE is the chair of that committee. IEEE 802.10 is a subcommittee of IEEE 802. They are

1. *DSL* 9 (April, 1989) pp. 4-6. Copyright 1989 *Data Security Letter*. Used by permission. Data Security Letter, P.O. Box 1593, Palo Alto, CA 94302, USA.

constrained by the IEEE 802 definition of a LAN to consider only layers 1 and 2 (the physical and data link layers). So basically what we mean by LAN is layer 1 and layer 2 of the OSI model. We can talk about layer 2 entity names and end-to-end associations at layer 2.

One of the things we discussed, and which Kirkpatrick wrote up for us, was what are the differences between a LAN and a wide area network (WAN). One is that LANs tend to be characterized by undirected (for example, broadcast) communication. Another is that in a LAN there is no control over who listens. A third is that there are end-to-end associations at layer 2. There are others.

DSL: *How is security of a LAN different from that of a WAN?*
BERSON: A LAN node has a layer 2 address. You cannot achieve finer granularity of access control than a layer 2 address will support -- for example, you can't have per-process or per-user security. So you can't do access control on a user basis if there are going to be shared nodes. You have the same or similar problems with layer 3 approaches.

DSL: *What kind of security are we talking about?*
BERSON: The security we addressed was primarily LAN transmission security. This means encrypting the traffic to provide confidentiality, integrity, and possibly sender non-repudiation. We did *not* talk about passwords for file servers, file transfer protocols, email security, and security of other LAN applications. LANSEC did not address the security of LAN applications; perhaps that's the topic for a later workshop.

DSL: *What level of threat were you concerned with?*
BERSON: Two papers from universities confirmed that universities are extremely hostile environments for LANS. The experience there is that students are motivated, informed, and equipped to perform highly sophisticated attacks against traffic on the university LAN. For universities, then, authentication and encryption of the highest quality are required.

DSL: *What sorts of architecture issues did you discuss?*
BERSON: The attendees took it as a given that there were ways to distribute keys and ways to encrypt traffic. The major architectural issues we discussed concerned the proper placements of these functions within a layered network protocol architecture.

DSL: *At which layers do these security functions belong?*
BERSON: There is no single answer to that question. The American participants put forth solutions at layer 2 and below because that's how IEEE 802 defines a LAN. The participants from the UK put forth layer 3 solutions.

DSL: *Where do the difficulties arise?*
BERSON: The supreme difficulty is to create an *open* secure network that works harmoniously in a layered model. One which, for example, won't disrupt unsecured traffic in the same network and will interconnect smoothly other, possibly unanticipated, transit networks.

Connectivity among modern networks is a minor miracle. A workstation on your network communicates easily and routinely with another halfway around the world. The difficult problem is how to provide security in an open framework such as that.

Richard Ward's paper, for example, dealt with the very interesting question of how to reconcile differences between OSI network security architecture and the network security architecture concepts in the US Red Book (*Trusted Network Interpretation (TNI) of the Trusted Computer System Evaluation Criteria (TCSEC)*. NCSC-TG-005. July 1987) to see if an alignment could be made -- what would one have to do to conform to both simultaneously. Part 2 of the Red Book acknowledges an overlap with OSI security architectures, but doesn't do the detailed work of placing security services in layers.

There was also some discussion about the German *National Catalog of Criteria for the Evaluation of Trusted IT Systems*, which will be analogous to the *TCSEC*. Apparently, the German book won't explicitly cover networks.

DSL: *Tell me something about the interaction between security services and existing network support tools.*

BERSON: L. Kirk Barker presented an interesting paper that discussed the impact of security on protocol analyzers. A protocol analyzer acts like a passive wiretap on a LAN. It is used to help the network administrator balance the workload on the LAN, to locate malfunctioning equipment, etc. But encryption at layer 2 would prevent the protocol analyzer from doing much of its job. Encryption at higher layers still partially blinds the protocol analyzer.

We also discussed the impacts of security on modem test patterns. Some modems look for certain bit patterns -- modem test patterns -- to put them into a test mode. These bit patterns may be unintentionally generated when data is encrypted. Conversely, if these bit patterns are encrypted, then they will not be recognized by the modem, which will then not go into test mode. All of these network support tools fail to operate correctly if LAN traffic is encrypted.

DSL: *What must be considered when migrating from an unsecure LAN to a secure LAN?*

BERSON: Where there are many nodes, the change to a secure LAN must be made gradually. You can't do the whole thing all at once. Can the unsecure parts continue to interoperate with the secure parts? Can the unsecure parts continue to operate with one another in the presence of encrypted traffic? The issues are similar to those associated with migration from non-OSI protocols toward OSI protocols.

DSL: *What do you have to pay for security?*

BERSON: We identified several trade-offs. Such as: (1) High performance vs. architectural simplicity. High performance leads to architectural complexity and consequent implementation complexity. (2) Flexibility of protocol definition vs. OSI fidelity. (3) Placement of security at layer *n* vs. at layer *m*. (4) Costs vs. security. Security adds cost, both of implementation and operation. (5) Security of transmission vs. ease of management and maintenance. (6) Connectivity vs. exposure.

DSL: *What about the usual trade-off between security and performance? Wasn't that an issue?*

BERSON: There are several worked examples of secure LANs, including Sytek's LocalNet and DEC's DESNC, among others. So we know that LAN security is possible to do. Our experience is that, from a user point of view, performance doesn't suffer much, if at all, as a result of security. That is, whatever performance degradation there may be is not perceived by most users.

DSL: *Would you say the workshop was successful?*

BERSON: Extremely successful. We took three and a half days to go through only 10 papers. We covered a narrow piece of ground in tremendous detail with lots of interaction and discussion. The participants, the sponsors, and the observers have all said that they derived benefits from the workshop. I expect that those who study our published papers will also benefit.