The 1996
Symposium on Network and Distributed Systems Security
(SNDSS'96)

Hypermedia Proceedings, Slides, and Summary Report

Table of Contents

Session 3: Distributed System Security
Chair: Michael Roe - University of Cambridge

1. A Flexible Distributed Authorization Protocol
   J.T. Trostle and B.C. Neuman (abstract)
2. Preserving Integrity in Remote File Location and Retrieval
   T. Jaeger and A.D. Rubin (abstract)
3. C-HTTP - The Development of a Secure, Closed HTTP-Based Network on the Internet
   T. Kiuchi and S. Kaihara (abstract, slides)

Session 4: Panel - Intellectual Property Protection
Moderator: Peter Neumann - SRI International (abstract)

- Olin Sibert - Electronic Publishing Resources
- Russell D. Housley - Spyrus (slides)
- Dan Boneh - Princeton University (slides)

Session 5: Network Security
Chair: Matt Bishop - University of California at Davis

1. Designing an Academic Firewall: Policy, Practice, and Experience with SURF
   M. Greenwald, S.K. Singhal, J.R. Stone, and D.R. Cheriton (abstract, slides)
2. Digital Signature Protection of the OSPF Routing Protocol
   S.L. Murphy and M.R. Badger (abstract, slides)
3. A Case Study of Secure ATM Switch Booting
   S-C. Chuang and M. Roe (abstract)

Session 6: Key Management
Chair: Burton S. Kaliski, Jr. - RSA Laboratories

1. SKEME: A Versatile Secure Key Exchange Mechanism for Internet
   H. Krawczyk (abstract, slides)
2. IDUP and SPKM: Developing Public-Key-Based APIs and Mechanisms for Communication Security Services
   C. Adams (abstract, slides)

Session 7: Encryption
Chair: Aviel D. Rubin - Bellcore

1. An Empirical Study of Secure MPEG Video Transmissions
   I. Agi and L. Gong (abstract, slides)
2. Parallelized Network Security Protocols
   E. Nahum, D.J. Yates, S. O'Malley, H. Orman, and R. Schroeppel (abstract, slides)
3. A "Bump in the Stack" Encryptor for MS-DOS Systems
   D.A. Wagner and S.M. Bellovin (abstract, slides)

Session 8: Panel - Public-Key Infrastructure
Moderator: Warwick Ford - Bell-Northern Research (abstract)

- John Wankmueller - MasterCard International
- Taher ElGamal - Netscape Communications (slides)
- Michael Baum - Verisign

General Chair's Message

Welcome to the third annual ISOC Symposium on Network and Distributed System Security! Each year we seek to bring together researchers, implementors, and users of network and distributed system security facilities. This year our Program Committee has again done an outstanding job of selecting a mix of technical presentations and panel sessions to discuss and debate the issues we face today.

As we are all aware, the need for usable distributed system security mechanisms is growing rapidly, tracking the growth and utilization of the world-wide Internet. For a welcome change, the general awareness of and interest in security is growing significantly as well _ by commercial organizations, the media, and private citizens. More than ever before, organizations will be looking to you, the participants of this symposium, for both technical solutions to specific problems and advice for the emerging public policy debates.

I encourage you to take advantage of this Symposium to not only listen to the presentations but also share your own experiences and ideas with other attendees during the breaks and evening activities.

Many thanks are in order for the behind-the-scenes effort that has culminated in this symposium: Tom Hutton "secured" our new location at the Princess Resort; Donna Leggett has done a superb job in handling the increased registration activities; and Stephen Welke has brought our Proceedings into the electronic age! I also want to commend the Program Co-Chairs, David Balenson and Clifford Neuman, for their excellent work with the Program Committee for pulling together the excellent program in which you are about to participate. Without the hard work by all these folks, this symposium would not have been possible.

As always, I want to thank all the authors who submitted papers and the panelists who are participating by sharing their knowledge and experiences with us.

Enjoy!

James T. Ellis
Carnegie Mellon University
jte@cert.org

Program Chairs' Message

In the past year, the public has increasingly been urged to enter cyberspace and to use the Internet to obtain information from vendors, order products, and even bank from home. At the same time, businesses are being compelled to have a presence on the Internet, making information available to customers and other businesses. As a result, the need for network and distributed system security has grown dramatically.

Today we find that the individuals trying to breach the security of computer systems are using more sophisticated attacks, and because such attacks now can yield business data or result in financial transactions, these attacks have become more lucrative. While the computer security discipline once addressed mostly hypothetical threats, the press has recently taken notice when attacks known by practitioners for years were suddenly perpetrated against widely-used and heavily marketed products including web servers and browsers and network file systems.

There is good news and bad news regarding the state of Internet security. The good news is that most of the threats we are seeing have been known for some time, and we know how to protect against them. The bad news is that the solutions must still be integrated with applications, many of the solutions require a computer security infrastructure that is not widely available, and we have yet to see widespread deployment of computer security

The organizers of this symposium hope that the symposium will encourage the Internet community to deploy the available security technology and develop new technology in areas where it is lacking. In selecting papers and panels for the symposium, the program committee sought to bring together the papers that will have the greatest impact on the field by introducing new computer security technologies whether research prototypes or actual products, demonstrating the application of computer security technologies to Internet applications, and describing components of the computer security infrastructure.

By bringing together researchers and practitioners in the field we are confident that the symposium will have a positive impact on the state of Internet security. We encourage you, as a participant in this symposium, to use this opportunity to actively participate in the dialog. Ask questions of the speakers, raise your important issues during relevant panel sessions, and let others know of your requirements, observations, and experience in this important area.

B. Clifford Neuman
Marina del Rey, California
bcn@isi.edu

David M. Balenson
Glenwood, Maryland
balenson@tis.com

Organizing Committee

General Chair
James T. Ellis
CERT Coordination Center
Carnegie Mellon University
jte@cert.org

Program Chairs

David M. Balenson
Trusted Information Systems
balenson@tis.com

B. Clifford Neuman
USC Information Sciences Institute
bcn@isi.edu

Publications Chair
Stephen R. Welke
Institute for Defense Analyses
welke@ida.org

Registrations Chair
Donna Leggett
The Internet Society
leggett@linus.isoc.org

Local Arrangements Chair
Thomas Hutton
San Diego Supercomputer Center
hutton@sdslug.org

Steering Group
Internet Research Task Force, Privacy and Security Research Group

---

Members

Thomas A. Berson - Anagram Laboratories
Matt Bishop - University of California at Davis
Doug Engert - Argonne National Laboratory
Warwick Ford - Bell-Northern Research
Burton S. Kaliski, Jr. - RSA Laboratories
Stephen T. Kent - BBN Corporation
Paul A. Lambert - Oracle
John Linn - OpenVision Technologies
Teresa Lunt - Advanced Research Projects Agency
Danny M. Nessett - Sun Microsystems
Hilarie Orman - University of Arizona
Michael Roe - University of Cambridge
Robert Rosenthal - National Institute of Standards and Technology
Aviel D. Rubin - Bellcore
Jeffrey I. Schiller - Massachusetts Institute of Technology
Robert W. Shirey - BBN Corporation
Doug Tygar - Carnegie Mellon University
Roberto Zamparo - Telia Research

External Reviewers

Carlisle Adams - Bell-Northern Research
William Burr - National Institute of Standards and Technology
Jan Carlsson - Telia Research
Trent Jaeger - University of Michigan
Stewart Kowalski - Telia Research
Tim Moses - Bell-Northern Research
Paul Van Oorschot - Bell-Northern Research
Rich Schroeppel - University of Arizona
Ola Sjögren - Telia Research
Richard Thomas - Bell-Northern Research
Jyri J. Virkki - Bellcore
Michael Wiener - Bell-Northern Research
Andrey Yeatts - University of Arizona

Privacy and Security Research Group of the Internet Research Task Force

Chair

Stephen T. Kent
BBN Corporation
kent@bbn.com

PSRG Committee Members

David M. Balenson
Trusted Information Systems
balenson@tis.com

Matt Bishop
University of California, Davis
bishop@cs.ucdavis.edu

Warwick Ford

Russell D. Housley

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.