



2001 NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM (NDSS'01)

8-9 February 2001 • Catamaran Resort Hotel • San Diego, California

HOSTED BY THE INTERNET SOCIETY
<http://www.isoc.org/ndss01>

The 8th Annual Symposium brings together researchers, implementers, and users of network and distributed system security technologies to *discuss today's important security issues and challenges*. The Symposium provides a mix of technical papers and panel presentations that describe *promising new approaches to security problems* that are practical, and to the extent possible, have been implemented. The Symposium also fosters the exchange of technical information and encourages the Internet community to deploy available security technologies and *develop new solutions to unsolved problems*.

THURSDAY, 8 FEBRUARY 2001

PACKET FLOWS (9:00–10:30)

- *An Algebraic Approach to IP Traceback*, D. Dean, M. Franklin and A. Stubblefield
- *Authenticating Streamed Data in the Presence of Random Packet Loss*, P. Golle and N. Modadugu
- *Practical Experiences with ATM Encryption*, G. Byrd, N. Hillery and J. Symon

SECURITY PROTOCOLS (11:00–12:00)

- *Efficient and Secure Source Authentication for Multicast*, A. Perrig, R. Canetti, D. Song and D. Tygar
- *TRICERT: A Distributed Certified E-Mail Scheme*, G. Ateniese, B. de Medeiros and M.T. Goodrich

PANEL: WIRELESS SECURITY – IS IT REAL? (14:00–15:30)

MISCELLANEOUS (16:00–17:00)

- *An Architecture for Flexible, High Assurance, Multi-Security Domain Networks*, T.J. Gibson
- *Authentication and Key Agreement Via Memorable Passwords*, T. Kwon

FRIDAY, 9 FEBRUARY 2001

POLICY (8:30–10:00)

- *SPL: An Access Control Language for Security Policies with Complex Constraints*, C. Ribeiro, A. Zuquete, P. Ferreira and P. Guedes
- *Limiting the Disclosure of Access Control Policies during Automated Trust Negotiation*, K. E. Seamons, M. Winslett and T. Yu
- *Principles of Policy in Secure Groups*, P. McDaniel, H. Harney and A. Colgrove

TRUST MANAGEMENT (10:30–12:00)

- *Trust Management for IPsec*, A.D. Keromytis, M. Blaze and J. Ioannidis
- *Building Certification Paths: Forward vs. Reverse*, Y. Elley, A. Anderson, S. Hanna, S. Mullan, R. Perlman, S. Proctor
- *Decentralized Jini Security*, P. Eronen, P. Nikander

IMPLEMENTATION ISSUES (14:00–15:30)

- *Termination in Language-based Systems*, A. Rudys, J. Clements, D.S. Wallach
- *Cryptography As a Network Service*, D. Dean, T. Berson, M. Franklin, D. Smetters, M. Spreitzer
- *Implementation of Crossrealm Referral Handling in the MIT Kerberos Client*, J. Trostle, I. Kosinovsky

INVITED TALK: SECURITY RISKS OF PEER-TO-PEER NETWORKING, S. Bellovin (16:00–17:00)

PRE-CONFERENCE TECHNICAL TUTORIALS • WEDNESDAY, 7 FEBRUARY 2001

Full-Day (8:30–17:00)

- #1 *Network Security Protocol Standards*, Stephen T. Kent
- #2 *Deployed and Emerging Security Systems for the Internet*, Charlie Kaufman

Morning (8:30–12:00)

- #3 *Building Secure Software*, Gary McGraw

- #4 *Intrusion Detection*, Dan Nadir

- #5 *Biometrics*, Jim Wayman

Afternoon (13:30–17:00)

- #6 *Secure Electronic Commerce*, Amir Herzberg

- #7 *Group Security*, Thomas Hardjono & Hugh Harney

CATAMARAN RESORT HOTEL: The Internet Society has reserved a special block of sleeping rooms at the Catamaran Resort Hotel at the following rates: Single - \$139; Double - \$139; Extra person - \$20. Current room tax is 10.5%. Parking is available at \$6/day for hotel guests. Government rate rooms are limited. Directly contact the Catamaran Resort Hotel at +1 800 288 0770 or FAX to +1 619 488 1387. (Outside the U.S., call +1 619 539 8700.) To receive special group rates, *reservations must be made no later than Jan. 15, 2001*. Registration includes attendance, proceedings (hardcopy and CD-ROM), reception, two continental breakfasts and luncheons, Casino Night and Dinner, and coffee breaks. Early registration postmarked on/before Jan. 11, 2001. Non-member fee includes one-year Internet Society membership. Refunds (less \$50 processing fee) will be issued for cancellations received on/before January 25, 2001.

PROGRAM COMMITTEE: David Aucsmith, Intel Corporation; Tom Berson, Anagram Laboratories; Matt Bishop, UC Davis; Bill Cheswick, Bell Labs; James Ellis, Sun Microsystems; Edward W. Felten, Princeton University; Virgil D. Gligor, University of Maryland; Peter Gutmann, University of Auckland, New Zealand; Dave Kormann, AT&T Labs – Research; David P. Maher, Intertrust; Gary McGraw, Reliable Software Technologies; Kevin McCurley, IBM Almaden Research Center; Fabian Monrose, Bell Labs, Mudge, L0pht Heavy Industries, Inc.; Sandra Murphy, Network Associates; Radia Perlman, Sun Microsystems; David Wagner, UC Berkeley; Bennet Yee, University of California San Diego

GENERAL CHAIR: Stephen R. Welke, Trusted Computer Solutions

PROGRAM CHAIRS: Avi Rubin, AT&T Labs – Research and Paul Van Oorschot, Entrust Technologies

TUTORIALS CHAIR: Eric Harder, National Security Agency

LOCAL ARRANGEMENTS CHAIR: Thomas Hutton, SDSC

PUBLICITY CHAIR: David M. Balenson, NAI Labs, Network Associates

PUBLICATIONS CHAIR: Mahesh Tripunitara, Purdue University

LOGISTICS CHAIR: Torryn Brazell, Internet Society

