



The 15th Annual  
Network and Distributed System  
Security Symposium  
The Dana on Mission Bay  
San Diego, California  
February 10–13, 2008

*Hosted by the Internet Society*



## *Call for Papers*

### **IMPORTANT DATES:**

- **Paper and panel submissions due: 11:59 pm PDT, Friday, September 21, 2007.**
- **Author notification: Monday, November 5, 2007.**
- **Final version of papers and panels due: December 15, 2007.**

### **GOAL:**

The symposium fosters information exchange among research scientists and practitioners of network and distributed system security services. The target audience includes those interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation (rather than theory). A major goal is to encourage and enable the Internet community to apply, deploy, and advance the state of available security technology. This year's symposium continues our theme of "theory meets practice" so we encourage submission both from traditional academic researchers as well as industrial practitioners of applied security with innovative insights.

The proceedings are published by the Internet Society.

### **HOW TO SUBMIT:**

Submission instructions are available at <http://www.isoc.org/tools/conferences/NDSS08>

### **SUBMISSIONS:**

Both technical papers and panel proposals are solicited. Technical papers must not substantially overlap with papers that have been published or that are simultaneously submitted to a journal or a conference with proceedings. All papers from authors perpetrating such "double submissions" will be immediately rejected from the symposium. The Program Committee reserves the right to share information with other conference chairs and journal editors so as to detect such cases.

Technical papers should be at most 12 pages excluding the bibliography and well-marked appendices (using 11-point font, single column format, and reasonable margins on 8.5"x11" or A4 paper), and at most 20 pages total. Committee members are not required to read the appendices, so the paper should be intelligible without them. Technical papers will appear in the proceedings. Panel proposals should be one page and must describe the topic, identify the panel chair, explain the panel format, and list three to four potential panelists. A description of each panel will appear in the proceedings, and may, at the discretion of the panel chair, include written position statements from the panelists.

Submissions are solicited in, but not limited to, the following areas:

- Integrating security in Internet protocols: routing, naming, TCP/IP, multicast, network management, and the Web.
- Intrusion prevention, detection, and response: systems, experiences and architectures.
- Privacy and anonymity technologies.
- Network perimeter controls: firewalls, packet filters, application gateways.
- Virtual private networks.
- Security for emerging technologies: sensor networks, specialized testbeds, wireless/mobile (and ad hoc) networks, personal communication systems.
- ID systems, peer-to-peer and overlay network systems.
- Secure electronic commerce: e.g., payment, barter, EDI, notarization, timestamping, endorsement, and licensing.
- Supporting security mechanisms and APIs; audit trails; accountability.
- Implementation, deployment and management of network security policies.
- Intellectual property protection: protocols, implementations, metering, watermarking, digital rights management.
- Fundamental services on network and distributed systems: authentication, data integrity, confidentiality, authorization, non-repudiation, and availability.
- Integrating security services with system and application security facilities and protocols: e.g., message handling, file transport/access, directories, time synchronization, data base management, boot services, mobile computing.
- Public key infrastructure, key management, certification, and revocation.
- Special problems and case studies: e.g., tradeoffs between security and efficiency, usability, reliability and cost.
- Security for collaborative applications: teleconferencing and video-conferencing, electronic voting, groupwork, etc.
- Software hardening: e.g., detecting and defending against software bugs (overflows, etc.)
- Security for large-scale systems and critical infrastructures.
- Security of Web-based applications and services.

Each submission must be accompanied by a separate, electronically submitted Submission Overview specifying the submission type (paper or panel), the title or topic, author names with organizational affiliations, and must specify a contact author along with corresponding phone number, FAX number, postal address and email address.

Submissions must be received by 11:59pm PDT, September 21, 2007, and must be made electronically in PDF format (for example, by using pdf<sub>l</sub>atex). Each submission will be acknowledged by e-mail; if acknowledgment is not received within seven days, contact a program co-chair (see below). Authors and panelists will be notified of acceptance by November 5th, 2007, and given instructions for preparing the camera-ready copy.

#### **PROGRAM COMMITTEE:**

- Crispin Cowan, Novell (*Program co-chair*)
- Giovanni Vigna, UC Santa Barbara (*Program co-chair*)
- Lujo Bauer, Carnegie Mellon University
- Konstantin Beznosov, UBC
- John Black, University of Colorado
- David Brumley, Carnegie Mellon University
- Jon Callas, PGP
- Hao Chen, UC Davis
- Charles Clarke, University of Waterloo
- Vinod Ganapathy, University of Wisconsin
- Jonathon Giffin, Georgia Tech
- Farnam Jahanian, University of Michigan
- Angelos Keromytis, Columbia University
- Engin Kirda, Vienna University of Technology
- Christopher Kruegel, Vienna University of Technology
- Ben Laurie, Google
- Wenke Lee, Georgia Tech
- Michael Locasto, Columbia University
- Fabian Monrose, Johns Hopkins University
- Niels Provos, Google
- Len Sassaman, Katholieke Universiteit Leuven
- R. Sekar, SUNY Stonybrook
- Sean Smith, Dartmouth College
- Zhendong Su, UC Davis
- Nick Weaver, ICSI
- Others pending