



**The 18th Annual
Network and Distributed System Security Symposium**
The Dana on Mission Bay
San Diego, California
6-9 February 2011

Sponsored by the Internet Society



Call for Papers

IMPORTANT DATES

- Titles and abstracts of papers due: Friday, August 6, 2010 (11:59 pm EDT)
- Full paper and panel submissions due: ~~Tuesday, August 10, 2010 (11:59 pm EDT)~~
Deadline extended to Friday, August 13, 2010 (11:59 pm EDT)
- Author notification: Monday, October 11, 2010
- Final version of papers and panels due: Wednesday, December 1, 2010

SYMPOSIUM GOALS

The Network and Distributed System Security Symposium fosters information exchange among researchers and practitioners of network and distributed system security. The target audience includes those interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation. A major goal is to encourage and enable the Internet community to apply, deploy, and advance the state of available network and distributed systems security technology. The proceedings are published by the Internet Society (ISOC).

Special emphasis will be made to accept papers in the core theme of network and distributed systems security. Consequently, papers that cover networking protocols and distributed systems algorithms are especially invited to be submitted. Moreover, practical papers in these areas are also very welcome.

WHAT TO SUBMIT

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 written in English, not exceed 20 pages (including the bibliography and well-marked appendices) using 11-point font, single column format, and 1-inch margins on 8.5"x11" or A4 paper. Reviewing is double-blind, and technical papers should thus be properly anonymized to conceal the authors' identity.

The Program 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, network management
- High-availability wired and wireless networks
- Security for Cloud Computing
- Future Internet architecture and design
- Security of Web-based applications and services
- Anti-malware techniques: detection, analysis, and prevention
- Security for future home networks, Internet of Things, body-area networks
- Intrusion prevention, detection, and response

- Combating cyber-crime: anti-phishing, anti-spam, anti-fraud techniques
- Privacy and anonymity technologies
- Security for emerging technologies: sensor networks, wireless/mobile (and ad hoc) networks, and personal communication systems
- Security for Vehicular Ad-hoc Networks (VANETs)
- Security for peer-to-peer and overlay network systems
- Security for electronic commerce: e.g., payment, barter, EDI, notarization, timestamping, endorsement, & licensing
- Implementation, deployment and management of network security policies
- Intellectual property protection: protocols, implementations, metering, watermarking, digital rights management
- Public key infrastructures, 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
- Security for large-scale systems and critical infrastructures (e.g., electronic voting, smart grid)
- Applying Trustworthy Computing mechanisms to secure network protocols and distributed systems

The deadline for full submissions, made electronically in PDF format, is 11:59 pm EDT, August 10, 2010. However, titles and abstracts of papers must be received by 11:59 pm EDT, August 6, 2010. Each submission will be acknowledged by email; if acknowledgement is not received within seven days, contact the Program Chair. Authors and panelists will be notified of acceptance by October 11, 2010, and given instructions on how to prepare the camera-ready copy.

Submission site: <http://hotcrp.cylab.cmu.edu/ndss11/>

NDSS 2011 will feature several best paper awards. There will be at least a best paper award and a best student paper award. We will seek additional opportunities to further honor authors of strong papers.

Program Committee

Adrian Perrig, PC Chair, (Carnegie Mellon University, USA)
 Giuseppe Ateniese (Johns Hopkins University, USA)
 Suman Banerjee (University of Wisconsin Madison, USA)
 Lujo Bauer (Carnegie Mellon University, USA)
 Konstantin Beznosov (University of British Columbia, Canada)
 Levente Buttyan (Budapest University of Technology and Economics, Hungary)
 Hao Chen (University of California, Davis, USA)
 Yan Chen (Northwestern University, USA)
 Mihai Christodorescu (IBM Watson, USA)
 Weidong Cui (Microsoft Research, USA)
 David Evans (University of Virginia, USA)
 Thorsten Holz (Ruhr-University Bochum, Germany)
 Yih-Chun Hu (University of Illinois at Urbana Champaign, USA)
 Collin Jackson (Carnegie Mellon University, USA)
 Christian Kreibich (International Computer Science Institute, USA)
 Yongdae Kim (University of Minnesota, USA)
 Tadayoshi Kohno (University of Washington, USA)
 Aravind Iyer (GM India Sciences Laboratory, India)
 Heejo Lee (Korea University, South Korea)
 Peng Ning (NC State University, USA)
 Cristina Nita-Rotaru (Purdue University, USA)
 Bryan Parno (Microsoft Research, USA)
 Radha Poovendran (University of Washington, USA)
 Phil Porras (SRI International, USA)
 Michael Roe (Microsoft Research, UK)
 Nitesh Saxena (Polytechnic Institute of New York University, USA)
 Ehab Al-Shaer (UNCC, USA)
 Sean Smith (Dartmouth College, USA)
 Radu Sion (Stony Brook University, USA)
 Jesse Walker (Intel, USA)
 Nick Weaver (International Computer Science Institute, USA)
 Brian Weis (Cisco, USA)
 Yinglian Xie (Microsoft Research, USA)
 Sencun Zhu (Penn State University, USA)