

SHERATON WAIKIKI HOTEL, HONOLULU, HAWAII, USA



CALL FOR PAPERS

We solicit papers offering novel contributions in computer and application security. Papers should present technique or application with practical experience. Papers are encouraged on technologies and methods that have been demonstrated to improve information systems security and that address lessons from actual application. We are especially interested in papers that address the application of security technology, the implementation of systems, and lessons learned. See example topics on the right.

Submitted papers must differ substantially from papers published previously or papers submitted to a journal or conference proceedings, may be at most 15 pages including bibliography and appendices, and must be formatted in a single column using 11-point font and reasonable margins on letter-sized paper.

Committee members are not required to read the appendices, so the paper should be intelligible without them. All submissions must be anonymized (i.e., no author names, affiliations or obvious citations). Submissions not meeting these guidelines risk rejection without consideration of merit.

Submissions must be received in PDF or Postscript by **June 1, 2009** at <http://www.acsac.org> (follow the link for Submission & Review). Authors will be notified by **August 17, 2009**. Authors of accepted papers must present their paper at the conference.

Suggested topics:

- access control
- applied cryptography
- audit and audit reduction
- biometrics
- boundary control devices
- certification and accreditation
- cyber security
- database security
- denial of service protection
- distributed systems security
- electronic commerce security
- enterprise security management
- forensics
- identification & authentication
- identify management
- incident response planning
- insider threat protection
- integrity
- intellectual property rights
- intrusion detection
- malware
- mobile and wireless security
- multimedia security
- network resiliency
- operating systems security
- peer-to-peer security
- privacy and data protection
- privilege management
- product evaluation/compliance
- risk/vulnerability assessment
- secure cloud infrastructures
- security engineering/mgmt
- security in IT outsourcing
- service oriented architectures
- software assurance
- trust management
- virtualization security
- VOIP security
- Web 2.0/3.0 security

PROGRAM COMMITTEE

Charles Payne, Adventium Labs (Chair)
 Michael Franz, UC Irvine (Co-Chair)
 Anas Abou El Kalam, IRIT/ENSEEIH
 Claudio Ardagna, U. of Milan
 Vijay Atluri, Rutgers U.
 Tuomas Aura, Microsoft Research
 Lee Badger, NIST
 Kosta Beznosov, U. of British Columbia
 Marco Casassa Mont, HP Labs
 Marc Dacier, Symantec Corporation
 Robert Deng, Singapore Mgmt U.
 Mary Denz, Air Force Research Lab
 Philip Fong, U. of Regina
 Sara Foresti, U. of Milan
 Vinod Ganapathy, Rutgers U.
 Carrie Gates, CA Labs
 Dieter Gollman, Hamburg U. of Tech.
 Steven Greenwald, Info. Security Adv.
 Dimitris Gritzalis, Athens U.
 Tom Haigh, Adventium Labs
 Wesley Higaki, Symantec Corporation
 Cynthia Irvine, Naval Postgraduate School
 Hongxia Jin, IBM Almaden
 Ulf Lindqvist, SRI International
 Peng Liu, Penn State U.
 Javier Lopez, U. of Malaga
 John McDermott, Naval Research Lab
 Peng Ning, North Carolina State U.
 Stefano Paraboschi, U. of Bergamo
 Guenther Pernul, U. of Regensburg
 Marco Pistoia, IBM T.J. Watson
 Lillian Røstad, NTNU
 Reiner Sailer, IBM
 Andre dos Santos, U. of Puerto Rico
 Christoph Schuba, Sun Microsystems, Inc.
 Kent Seamons, Brigham Young U.
 Randall Smith, Boeing Corporation
 Angelos Stavrou, George Mason U.
 Vipin Swarup, MITRE Corporation
 Dan Thomsen, Cyber Defense Agency
 Patrick Traynor, Georgia Inst. of Tech.
 Venkat Venkatakrishnan, UI at Chicago
 David Whyte, CSE
 Alec Yasinac, U. of South Alabama