# 22nd National Information Systems Security Conference

## Conference Committee

1999 National Computer Systems Security Award

## Papers

<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find and Fix Y2K Embedded Equipment Risks</td>
<td>Dick Lefkon, <em>New York University</em></td>
</tr>
<tr>
<td>Active Networks and Security</td>
<td>Vijay Varadharajan, Rajan Shankaran, Michael Hitchens, <em>University of W. Sydney</em></td>
</tr>
<tr>
<td>Security of High-Performance Messaging Layers on Programmable Network Interface Architectures</td>
<td>Srigurunath Chakravarthi, <em>Mississippi State University</em></td>
</tr>
<tr>
<td>Attitude Adjustment: Trojans and Malware on the Internet: an Update</td>
<td>Sarah Gordon, David Chess, <em>IBM Thomas J. Watson Research Center</em></td>
</tr>
<tr>
<td>The Network Vulnerability Tool (NVT) – A System Vulnerability Visualization Architecture</td>
<td>Ronda Henning, Ph.D., Kevin L. Fox, Ph.D., <em>Harris Corporation</em></td>
</tr>
<tr>
<td>Implementation of Multiple Access Control Policies within a CORBASEC Framework</td>
<td>Ramaswamy Chandramouli, <em>National Institute for Standards and Technology</em></td>
</tr>
<tr>
<td>Immunity-Based Intrusion Detection System: A General Framework</td>
<td>Dipankar Dasgupta, <em>University of Memphis</em></td>
</tr>
<tr>
<td>From AntiVirus to AntiMalware Software and Beyond: Another Approach to the Protection of Customers from Dysfunctional System Behaviour</td>
<td>Dr. Klaus Brunnstein, <em>University of Hamburg, Germany</em></td>
</tr>
</tbody>
</table>
Validating A High Performance, Programmable Secure Coprocessor
Sean Smith, Ron Perez, Steve Weingart, Vernon Austel, IBM T.J. Watson Research Center

Status of the Advanced Encryption Standard (AES) Development Effort
James Foti, National Institute of Standards and Technology

Assessing Network Infrastructure Vulnerabilities to Physical Layer Attacks
T. H. Shake, B. Hazzard, D. Marquis, Massachusetts Institute of Technology

Using Composition & Refinement to Support Security Architecture Trade-off Analysis
C.N. Payne, Jr., Secure Computing Corporation

Abstracting Security Specifications in Building Survivable Systems
J. Jenny Li, Mark Segal, Telcordia Technologies

An Avenue for High Confidence Applications in the 21st Century
Timothy W. Kremann, William B. Martin, Frank Seaton Taylor, National Security Agency

A Comparison of CDSA to Cryptoki
Ruth Taylor, National Security Agency

Application Support Architecture for A High-Performance, Programmable Secure Coprocessor
Joan Dyer, Ron Perez, Sean Smith, Mark Lindemann, IBM T.J. Watson Research Center

Statistical Testing of Random Number Generators
Juan Soto, National Institute of Standards and Technology

Provably Insecure Mutual Authentication Protocols: The Two-Party Symmetric-Encryption Case
Jim Alves-Foss, University of Idaho

Automatically Detecting Authentication Limitations in Commercial Security Protocols
Stephen H. Brackin, Arca Systems, Inc.

Smart Certificates: Extending X.509 for Secure Attribute Services on the Web
Joon S. Park, Ravi Sandhu, George Mason University

A Method for Quantitative Risk Analysis
James W. Meritt, CISSP, Wang Global

Using Security Metrics to Assess Risk Management Capabilities
Natalie Givans, Nadya Bartol, Booz-Allen & Hamilton, Inc.
Lisa A. Gallagher, Arca Systems, Inc.
Christina Kormos, National Security Agency

Network Security Framework: Robustness Strategy
Steve Hirsch, Teri Arber, Deb Cooley, Martha Mahan, Jim Osterritter, National Security Agency

Interdependency Analysis
Richard K. McAllister, SPARTA Incorporated
James L. Coyle, Averstar Incorporated

Towards Security of Integrated Enterprise Systems Management
Alexander D. Korzyk, Sr., Virginia Commonwealth University

Understanding the World of Your Enemy with I-CAT (Internet-Categorization of Attacks Toolkit)
Peter Mell, National Institute of Standards and Technology
Infrastructure Monitoring Challenges
J. L. Bayuk, Bear Stearns & Co., Inc.

A Common Weak Link in the Security Chain
Gregory B. White, Ph.D., SecureLogix Corporation

Tutorials

Database Security
Dr. William Wilson, Arca Systems, Inc.

Security Engineering Best Practices
Karen Ferraiolo, Arca Systems, Inc.

Specifying System Security Requirements
Paula A. Moore, Federal Aviation Administration

Surviving the FIPS 140-1 Validation Process
Brenda Kallighan, Tom Caddy, Patricia Lareau, InfoGard Laboratories, Inc.

Managing Your Return on Investment (ROI) for PKI Security in the Digital Future
Peter Butziger, Booz-Allen & Hamilton

“Holistic” Security: Circles, Pies, or Crystals?
Jim Litchko, IMSI

Total BS Security: Business-Based Systems Security
Jim Litchko, IMSI

INFOSEC Update 1999: Computer Crime Review
M.E. Kabay, Ph.D., CISSP, ICSA

A Survey of Mobile Code Security Techniques
Dr. Roshan Thomas, NAI Labs at Network Associates

Developing Security Plans for Information Technology Systems
Marianne Swanson, National Institute of Standards and Technology

Role Based Access Control
Professor Ravi Sandhu, George Mason University

The Computer Security Professional’s Role in Trade Secret Protection
Christopher Marquart, J.D., Wyeth-Ayerst Global Pharmaceuticals

Trust No One - Successfully Defending Your Network
Scott Blake, Netect, Ltd.

Authentication: “I Know You”
Michael J. Corby, CCP, CISSP, M Corby & Associates, Inc.

Biometrics: Installing and Integrating Biometric Systems into your Existing Systems
William Saito, I/O Software, Inc.

The Bind Activity: A Case Study in Incident and Vulnerability Handling
Kathy Fithen, Jeffrey J. Carpenter, Shawn Hernan, Carnegie Mellon

Computer Forensics in a LAN Environment
Michael J. Corby, CCP, CISSP, M Corby & Associates, Inc.

Usage of Certificate Policies in a PKI to Model Real-World Trust Relationships
Dr. Sarbari Gupta, CygnaCom Solutions
Panels and Other Presentations

The Future of Networking – Can Security Keep Up?
Chair: Jeff Ingle, National Security Agency
Panelists:
- Stan Hanks, Enron
- Chris Kubic, National Security Agency
- Tom Shake, MIT Lincoln Laboratory

The Current State of the CORBA Security Market
Chair: Edward Feustel, Institute for Defense Analyses
Viewpoints:
- Edward Feustel, Institute for Defense Analyses
- Bob Blakley, DASCOM, Inc.
What, Exactly is CORBAsec?
- David Chizmadia, Computer Science Corporation
The Status of OMG CORBA Security Implementations
- Bret Hartman, Concept Five Technologies
Toward an Interoperable *and* Portable CORBA Security Specifications
- Polar Humenn, Adiron

Security Requirement for PKIs
Chair: Alfred W. Arsenault, Jr., National Security Agency
Viewpoints:
- Marc LaRoche, Entrust
- Kathy L. Lyons-Burke, National Institute of Standards and Technology
- Eric S. Rosenfeld, Spyrus

PKI – The Gap Between Products and Standards
Chair: Santosh Chokani, CygnaCom Solutions
Panelists:
- Sharon Boeyen, Entrust
- Patrick Cain, BBN Technologies
- Warwick Ford, Verisign
- W. Timothy Polk, National Institute of Standards and Technologies

Comparative Approaches to Critical Infrastructure Protection
Chair: Dr. Andrew Rathmell, King’s College London
Panelists:
- Edna Chivers, UK Cabinet Office
- Suzanne Jantsch, IABG, Germany
- Lars Nicander, Swedish National Defence College

Critical Infrastructure Assurance
Chair: John Tritak, Critical Infrastructure Assurance Office
Viewpoints:
- Stevan Mitchell, Department of Justice
- Nancy Wong, Pacific Gas and Electric
- Thomas Burke, General Services Administration
- John Davis, National Security Agency
<table>
<thead>
<tr>
<th>Event</th>
<th>Chair</th>
<th>Panelists</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security</td>
<td><em>Information Security Center (GTISC)</em></td>
<td>Todd Inskeep, <em>Bank of America</em></td>
</tr>
<tr>
<td>Achieving Assurance: What will we do?</td>
<td></td>
<td>Peter Neumann, <em>SRI International</em></td>
</tr>
<tr>
<td>Viewpoints</td>
<td></td>
<td>Clark Weissman</td>
</tr>
<tr>
<td>Panelists</td>
<td></td>
<td>Roger Schell</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LtCol Fred W. Peters, <em>United States Air Force OASD and TMA</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>David J. Wilson, <em>Telos Corporation</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Virgil Gligor, <em>University of Maryland, College Park</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sami Saydjari, <em>DARPA</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brian Snow, <em>National Security Agency</em></td>
</tr>
<tr>
<td></td>
<td><em>University/Software Engineering Institute</em></td>
<td>Ken Fong, <em>IBM Security and Privacy Services</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lawrence R. Rogers, *Carnegie Mellon University/Software Engineering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Institute*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ronald B. Knode, <em>Computer Sciences Corporation</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Paul Livingston, <em>Intellink Management Office</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Jim Williams, <em>Booz-Allen &amp; Hamilton Corporation</em></td>
</tr>
</tbody>
</table>
University Approaches to Information Security Education—Challenges, Issues, Successes, and Opportunities  
Chair: Dr. Rayford Vaughn, *Mississippi State University*

Viewpoints:
Remote Learning for Information Security Professionals  
Professor Allan Berg, *James Madison University*

What Do We Mean by “Computer Security Education”?  
Dr. Matt Bishop, *University of California, Davis*

The NPS CISR Approach to Information System Security Education  
Dr. Cynthia Irvine, *Naval Postgraduate School*

Computer Security Training and Emerging Software Engineering Degree Programs  
Dr. Rayford Vaugh, Jr., *Mississippi State University*

Panelists:  
Dr. Virgil Gligor, University of Maryland

Teaching Information Warfare – Lessons Learned  
Chair: Professor Lance J. Hoffman, *George Washington University*

Viewpoints:
Teaching Information Warfare at The George Washington University  
Professor Lance J. Hoffman, *George Washington University*

Teaching Information Warfare at Georgetown University  
Dorothy E. Denning, *Georgetown University*

Frameworks and End States in the Teaching of the Strategic and Ethical Dimensions of Strategic Information Warfare  
Roger C. Molander, *Rand Corporation*

Teaching Information Warfare and Information Operations at National Defense University  
Dan Kuehl, *National Defense University*

Themes and Highlights of the New Security Paradigms Workshop 1999  
Chair: Mary Ellen Zurko, *Iris Associates*

Viewpoints:
Strike Back: Offensive Actions in Information Warfare  
Nathan A. Buchheit, Anthony Ruocco, Donald J. Welch, *United States Military Academy, West Point*

Security Architecture Development and its Role in the Seat Management and Total Cost of Ownership Environments  
Ronda R. Henning, *Harris Corporation*

Optimistic Security: A New Access Control Paradigm  
Dean Povey, *DSTC*

Securing Information Transmission by Redundancy  
Professor Peter Reiher, Jun Li, Gerald Popek, *University of California, Los Angeles*

Unfinished Business: What's Next for IPsec?  
Chair: Dr. Stephen Kent, *BBN Technologies*

Panelists:  
Roy Pereria, *TimeStep Corporation*

Dr. Steven Bellovin, *AT&T Research*

Luis Sanchez, *BBN Technologies*
Career Development and Hiring Trends into the 21st Century
Chair: Marla Collier, Internet Resources
Panelists:
  Todd Inskeep, Bank of America
  Mark Mercer, Ernst & Young, LLP
  G. Mark Hardy, Secure Computing Corporation
  Ira Winkler, Internet Security Advisors Group
  Dr. Rayford Vaughn, Mississippi State University
  Jeremy Epstein, Network Associates Laboratory

How can the Security Community Share Detailed Attack and Vulnerability Information?
Chair: Peter Mell, National Institute of Standards and Technology
Viewpoints:
Why Share AV Information?
  Peter Mell, National Institute of Standards and Technology
The Case for Corporate Sharing of AV Information
  Kevin Ziese, Cisco
A Model for Sharing
  Gene Spafford, CERIAS
Alternate Sharing Models
  Matt Bishop, University of California, Davis

Secure Electronic Mail: It’s Ready for Prime Time
Chair: Russell Housley, SPYRUS
Panelists:
  John Pawling, J.G. Van Dyke & Associates
  Michael Elkins, Network Associates, Inc.

Healthcare Protection Profile Initiative
Chair: Diann A. Carpeneter, ARCA Systems
Panelists:
  Dr. Ross Anderson, Cambridge University, UK
  Lewis Lorton, DDS, MSD, Forum on Privacy and Security in Healthcare
  Arnold Johnson, National Institute of Standards and Technology

End-to-End Encryption
Chair: David Kennedy, CISSP, ICSA, Inc.
Panelists:
  Michael Miora, InfoSec Labs, Inc.
  Russ Cooper, R.C. Consulting, Inc.
  Pirkka Palomaki, Datafellows, Inc.
  Robert Moskowitz, ICSA, Inc.

Non-Technical Issues Influencing Information Assurance
Chair: Paul B. Pattak, The Byron Group, Ltd.
Panelists:
  William Bruck, Ph.D, Author
  Addison Slayton, Jr., Virginia Department of Emergency Services
  Steven D. Mitchell, US Department of Justice
  Donald M. Le Vine, Ph.D., TRW
Rapid Risk Analysis for Information Security
Chair: Hilary Hosmer, *Data Security, Inc.*
Viewpoints:
Rapid Risk Assessment
Walter Cooke, *Canada*
Panelists:
Caroline Hamilton, *RiskWatch*

Common Criteria Project: Implementing the Mutual Recognition Arrangement
Chair: Gene Troy, *National Institute of Standards and Technology*
Panelists:
Murray Donaldson, *Communications-Electronics Security Group, UK*
Robert Harland, *Communications Security Establishment, Canada*
Ron Ross, *National Institute of Standards and Technology*

ISO/IEC JTC 1/SC 27 “IT Security Techniques” or Why Bother About ISO Security Standards?
Chair: Walter Fumy Ph.D., *Siemens AG, Germany*
Panelists:
Ted Humphreys, *XISEC Consultants Ltd., UK*
Marijke De Soete Ph.D., *Europay International, Belgium*
Eugene Troy, *National Institute of Standards and Technology*
Jerry A. Rainville, JD, *National Security Agency*

TPEP to NIAP CCEVS: Completing the Transition
Chair: Tom E. Anderson, *National Security Agency*
Panelists:
L. Arnold Johnson, *National Institute of Standards and Technology*
Jeffrey Horlick, *National Voluntary Laboratory Accreditation Program*
Keith F. Brewster, *National Security Agency*
Suzanne S. O’Connor, *National Security Agency*

Cryptographic Module Validation Program: The Next Generation (FIPS 140-2)
Chair: Annabelle Lee, *National Institute of Standards and Technology*
Panelists:
Ray Snouffer, *National Institute of Standards and Technology*
Tom Casar, *Communications Security Establishment, Canada*

U.S. Government Use of the Systems Security Engineering Capability Maturity Model (SSE-CMM)
Chair: Mary D. Schanken, *National Security Agency*
Panelists:
James P. Craft, *United States Agency for International Development*
Charles G. Menk III, *National Security Agency*

Databases of Threats and Countermeasures
Chair: Jim Williams, *MITRE Corporation*
Panelists:
Natalie Brader, *L-3 Network Security*
Kenneth Olthoff, *National Security Agency*
Adam Shostack, *BindView Development*
Pascal Meunier, *Purdue University*
Using the Common Criteria in Smart Card Security
Chair:  Stuart W. Katzke, National Security Agency
Panelists:
    Kenneth R. Ayer, Ph.D., Visa International
    Gilles Lisimaque, Gemplus
    Gene F. Troy, National Institute of Standards and Technology

International Recognition for Digital Signatures – A Need for a World Wide Common Approach?
Chair:  Klaus J. Keus, BSI/GISA, Germany
Panelists:
    Michael Hange, BSI/GISA, Germany
    Mark Bohannon, Department of Commerce, USA
    Detlef Eckert, European Commission, Belgium

The National Colloquium for Information Systems Security Education
Chair:  Dr. Vic Maconachy, National Security Agency
Panelists:
    Dr. Corey Schou, Idaho State University
    Dr. Charles Reynolds, James Madison University

Defense-wide Information Assurance Program (DIAP)
Chair:  CAPT J. Katharine Burton, United States Navy
Viewpoints:
Defense-wide Information Assurance Program
    CAPT J. Katharine Burton, United States Navy
USCINCSPACE Assumption of CND Mission
    COL Tom Muchenthaler, United States Air Force
Panelists:
    Christina McBride, DIAP
    Mark Viola, DIAP

Who is this Melissa Anyway?
    Jimmy Kuo, AntiVirus Research, Network Associates Inc.

Network Security Improvement Program (NSIP)
Phillip J. Loranger, LTC LeRoy Lundgren, Headquarters, Department of the Army