20th National Information Systems Security Conference

Referred Papers
Early Bird Session

Information Security is Information Security 1
Ira S. Winkler, *National Computer Security Association*

Secrets, Lies, and IT Security 7
Guy King, *Computer Sciences Corporation*

The NPS CISR Graduate Program in INFOSEC: Six Years of Experience 22
Cynthia E. Irvine, Daniel F. Warren, Paul C. Clark *Naval Postgraduate School*

Cellular Technology and Security 31
Ryan Jones, *University of Maryland*

The Security of Electronic Banking 41
Yi-Jen Yang, *University of Maryland* slides

Extranet Security: A Technical Overview from a Business Perspective 53
Jennifer Jordan, *University of Maryland*

Digital Coins based on Hash Chain 72
Khanh Quoc Nguyen, Yi Mu, Vijay Varadharajan, *University of Western Sydney, Nepean, Australia*

Internet — Track A

Go Ahead, Visit Those Web Sites, You Can't Get Hurt … Can You? 80
James S. Rothfuss, *Lawrence Livermore National Laboratory* slides
Jeffrey W. Parrett*, PeopleSoft*

Web Spoofing: An Internet Con Game 95
Edward W. Felton, Dirk Balfanz, Drew Dean, Dan S. Wallach *Princeton University*

When JAVA Was One: Threats from Hostile Byte Code 104
Mark D. Ladue, *Georgia Institute of Technology*

Stupid JavaScript Security Tricks 116
Walter Cooke, *CISSP, W. J. Cooke & Associates Ltd., Canada*

Information Infrastructure — Track C

Cryptographic Algorithm Metrics 128
Landgrave T. Smith, Jr., *Institute for Defense Analyses* slides

Using Datatype-Preserving Encryption to Enhance Data Warehouse Security.....141
Harry E. Smith, *Quest Database Consulting, Inc.* slides
Michael Brightwell*, FM Software, Inc.*

Multistage Algorithm for Limited One-Way Functions.....150
William T. Jennings, *Raytheon E-Systems & Southern Methodist University*

Practical Defenses Against Storage Jamming.....162
J. McDermott, J. Froscher, *Naval Research Laboratory*

What is Wild?.....177
Sarah Gordon, *IBM* slides

Secure Software Distribution System.....191
Lauri Dobbs, Tony Bartoletti, Marcey Kelley, *Lawrence Livermore National Laboratory* slides

A Methodology for Mechanically Verifying Protocols Using an Authentication Logic.....202
J. Alves-Foss, *University of Idaho*
Munna*, Tata Institute of Fundamental Research, India*

A Practical Approach to Design and Management of Secure ATM Networks.....213
Vijay Varadharajan, Rajan Shankaran, University of West Sydney, Nepean, Australia;
Michael Hitchens, *University of Sydney, Australia*

Distributed Network Management Security.....233
Paul Meyer, *Secure Computing Corporation* slides

Assurance/Criteria/Testing — Track E

A New Strategy for COTS in Classified Systems.....250
Simon Wiseman, *Defence Evaluation and Research Agency, UK*
Lt. Col. Colin J. Whittaker*, UK Ministry of Defence, UK*

Outsourcing-A Certification & Accreditation Dilemma.....265
Harold Gillespie, *CISSP,* Mike O'Neill*, CISSP, CTA Incorporated*

The Department of Defense Information Assurance Support Environment.....276
Barry C. Stauffer, *CORBETT Technologies*
Jack Eller, Penny Klein*, DISA, IPMO*
Joel Sachs*, The Sachs Group*
Dennis Winchell*, Logicon, Inc.*

CYBERTERRORISM - Fact or Fancy?.....285
Mark Pollitt, *Federal Bureau of Investigation Laboratory*

Protecting American Assets -- Who is Responsible?.....290
Anthony C. Crescenzi, *Defense Investigative Service*

Who Should Really Manage Information Security in the Federal Government.....295
Alexander D. Korzyk, Sr., A. James Wynne, *Virginia Commonwealth University* slides

Application of the IT Baseline Protection Manual 305
Dr. Angelika Plate, *BSI, Germany*

The Use of Information Technology Security Assessment Criteria to Protect Specialized Computer Systems 319
Ronald Melton, David Devaney, *Pacific Northwest National Laboratory*
V.A. Lykov, A.V. Shein, A.S Piskarev*, Russia*
William J. Hunteman, Joan M. Prommel*, Los Alamos National Laboratory*
James S. Rothfuss*, Lawrence Livermore National Laboratory*

R & D — Track F

Role Based Access Control for the World Wide Web 331
D. Richard Kuhn, John F. Barkley, Anthony V. Cincotta, David Ferraiolo, Serban Gavrila, National Institute of Standards and Technology slides

Observations on the Real-World Implementation of Role-Based Access Control 341
Burkhard Hilchenbach, *Schumann Security Software, Inc.*

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances 353
Phillip Porras, Peter Neumann, *SRI International*

An Application of Machine Learning to Anomaly Detection 366
Terran Lane, Carla E. Brodley, *Purdue University*

A Process of Data Reduction in the Examination of Computer Related Evidence 381
Mary F. Horvath, *Federal Bureau of Investigation Laboratory*

Automated Information System (AIS) Alarm System 394
William Hunteman, University of California, *Los Alamos National Laboratory*

The Use of Belief Logics in the Presence of Casual Consistency Attacks 406
J. Alves-Foss, *University of Idaho*

Achieving Interoperability Through Use of the Government of Canada Public Key Infrastructure 418
Capt. John H. Weigelt, *Department of National Defence (Canada)*

Implementation of Key Escrow with Key Vectors to Minimize Potential Misuse of Key 431
William J. Caelli, D. Longley, *Queensland University of Technology, Australia*

Security Tools - A “Try Before You Buy” Web-Based Approach 443
Sheila Frankel, *National Institute of Standards and Technologies*

Internet Protocol Next Generation: Saving the Internet in the New Millennium 452
Robert A. Kondilas, *MCI* slides

Vulnerability of “Secure” Web Browsers 476
Richard Kemmerer, Flavio De Paoli, Andre L. Dos Santos, *University of California, Santa Barbara*

Policy/Administration/Management — Track G

A Multi-Level Secure Object-Oriented Database Model 488
George Durham, Konstantinos Kalpakis, *University of Maryland Baltimore County*

Use of SSH on a Compartmented Mode Workstation 498
Johnny S. Tolliver, *Oak Ridge National Laboratory*
David Dillow, *Lockheed Martin Energy Systems*

Multilevel Architectures for Electronic Document Retrieval 505
James A. Rome, Johnny S. Tolliver, *Oak Ridge National Laboratory*

Security Modeling for Public Safety Communication Specifications 514
Daniel Gambel, *Mitretek Systems, Inc.*

Towards a Framework for Security Measurements 522
Chenxi Wang, William Wulf, *University of Virginia*

Connecting Classified Nets to the Outside World: Costs and Benefits 534
Christopher P. Kocher, *L-3 Corporation*

Software Encryption in the DoD 543
Russell Davis, *Boeing Information Services, Inc.*
Al Kondi, *PMO RCAS*

TRANSMAT Trusted Operations for Untrusted Database Applications 555
Dan Thomsen, *Secure Computing Corporation* slides

A New Paradigm for Performing Risk Assessment 565
Judith L. Bramlage, *Computer Associates International, Inc.* slides

INFOSEC Risk Management: Focused, Integrated & Sensible 577
Donald R. Peeples, *National Security Agency*

Role-Based Risk Analysis 587
Capt Amit Yoran, *USAF*
Lance C. Hoffman, *George Washington University*

Professional Development — Track I

A Risk Minimisation Framework For Electronic Commerce 603
Denis Tr ek, *Jozef Stefan Insititute, Slovenia*

Threats And Vulnerabilities For C4I In Commercial Telecommunications: A Paradigm for Mitigation 612
Joan Fowler, Robert C. Seate III, *Data Systems Analysts, Inc*.

Surviving Denial of Service on the Internet 619

Winn Schwartau, *COO, Security Experts, Inc.*

The Extended Commercially Oriented Functionality Class for Network-based IT Systems.....641
Alexander Herrigel, *r3 Security Engineering, Switzerland*
Roger French, *Digital Equipment Corporation, U.S.*
Herrmann Siebert, *EDP Consulting, Germany*
Helmut Stiegler, *STI Consulting, Germany*
Haruki Tabuchi, *Fujitsu Ltd., Japan*

Panels

Internet — Track A

Critical Elements of Security Frameworks.....654
Chair: Judith Furlong, *MITRE Corporation*
Panelists:
Michael Willett, *IBM Corporation*
David Aucsmith, *Intel Architecture Labs*
Keith Klemba, *Hewlett Packard Company*

Security and Trust on the World Wide Web.....656
Chair: Jim Miller, *World Wide Web Consortium*
Panelists:
Philip DesAutels, *World Wide Web Consortium*
Win Treese, *Open Market, Inc.*
Brian O'Higgins, *Entrust Technologies*
John Wankmueller, *MasterCard*

Critical Components of Intrustion Detection Systems.....657
Chair: Jill Oliver, *Citibank*
Panelists:
Dan Esbensen, *Touch Technologies*
Lee Sutterfield, *WheelGroup*
Mark Crosbie*, Hewlett-Packard*
Christopher Klaus*, Internet Security Systems, Inc.*

Public Key Infrastructure - Issues and Challenges.....660
Chair: Warwick Ford, *VeriSign, Inc.*
Panelists:
Taher ElGamal, *Netscape Communications Corporation*
Donna Dodson, *National Institute of Standards and Technology*
Tom Manessis*, Visa*
Ted Humphreys*, XiSEC Consultants Ltd.*

Developing a PKI Solution for Web Transactions: Lessons Learned 662
Chair: Judith A. Spencer, *General Services Administration*
Viewpoints:
Implementation Lessons Learned 665

Stanley Choffrey, *General Services Administration*
Public Key Infrastructure Philosophy 670
Phillip Mellinger, *First Data Corporation*
How it Works 672
Monette Respress*, Mitretek Systems*
Where Do We Go From Here 678
Isadore Schoen, *Cygnacom Solutions*

Firewalls Are More Than Just Bandages 679
Chair: Peter Tasker, *The MITRE Corporation*
Panelists:
Tom Haigh, *Secure Computing Corporation*
John Pescatore, *Trusted Information Systems*
Tony Vincent, *Raptor Systems*, Inc.

Practical Experience WithVirtual Private Networks (VPNs) 681
Chair: Steve Kent, *BBN*
Panelists:
Paul Lambert, *Oracle*
Naganand Doraswamy, *Bay Networks, Inc.*
Roy Pereira, *Timestep*
Dan McDonald, *Sun Microsystems, UK*

Network Security - From a User & Vendor Perspective 682
Chair: Ken Heist, *National Security Agency*
Panelists:
Frank Hecker, *Netscape Communications Corporation*
Gregory Gilbert, *National Security Agency*
James S. Prohaska, *Litronic, Inc.*
Richard Parker, *NATO Consultation, Command, and Control Agency*

Electronic Commerce — Track B

Security Architectures for Electronic Commerce 684
Chair: Clinton Brooks, *National Security Agency*
Panelists:
Bruce Schneier, *Counterpane Systems*
Tony Lewis, *VISA International*
Jerome Solinas, *National Security Agency*

Legislative Issues Associated with Digital Signatures and Supporting Technologies 685
Chair: Steve Ross, *Deloitte and Touche*
Viewpoints:
Certification Authorizes and Digital Signature A UK Perspective 685
Nigel Hickson, *Department of Trade and Industry*

Information Infrastructure — Track C

Infrastructure Vulnerabilities 686

Chair: John P. L. Woodward, *MITRE Corporation*
Panelists:
John C. Davis, *NCSC; Commissioner, Presidential's Commission on Critical Infrastructure Protection*

Technologies/Procedures Needed to Enhance the Assurance of the Telecommunications Infrastructure 687
Chair: Dick Brackney, *National Security Agency*
Viewpoints:
Internet Routing Infrastructure....688
Steve Kent, *BBN*
Intrusion Detection: Technology Gaps and Research Investments....688
Teresa Lunt, *Defense Advanced Research Projects Agency*
Securing The Evolving Public Telecommunications Networks 689
John Kimmins, *BELLCORE*
GII Security - Research, Technical Developments and Standards....690
Ted Humphreys, *XiSEC, UK*
Technology Research....690
Nancy Wong, *President's Commission on Critical Infrastructure Protection*

The InterTrust Commerce Architecture 692
Chair: Willis Ware, RAND Corporation
Viewpoints:
The InterTrust Approach to Electronic Commerce 692
David Van Wie, *Inter Trust Technologies Corporation*
The InterTrust Security Architecture....694
Olin Sibert, *Inter Trust Technologies Corporation*
InterTrust's Research Directions for Electronic Commerce....696
James Horning, *InterTrust Star Laboratory*

Debate — Track D

Legal and Liability Issues for Use of Cryptography 698
Chair: Joan Winston, *Trusted Information Systems, Inc.*
Panelists:
Michael Scott Baum, *VeriSign, Inc*.
Hoyt L. Kesterson II, *Bull HN Information Systems Inc.*
Robert L. Meuser, *Attorney at Law*

Copyright: Should Media Matter? (How Much?)....700
Chair: Joan Winston, *Trusted Information Systems, Inc.*
Panelists:
Prue Adler, *Association of Research Libraries*
Jonathan Band, *Morrison & Foerster LLP*

Technology Around The Next Corner: The Future of INFOSEC....702
Chair: Hilary Hosmer, *Data Security Inc.*
Panelists:
Emmet Paige, *OAO*

Kathy Kincaid, *IBM*
John Graff, *KPMG, Peat, Marwick, LLP*
Ruth Nelson*, Information Systems Security*

The Data Encryption Standard: 20 Years Later....705
Chair: Dorothy E. Denning, *Georgetown University*
Panelists:
William J. Caelli, *Queensland University of Technology, Australia*
Stephen T. Kent, *BBN Corporation*
Viewpoint:
The Data Encryption Standard: 20 Years Later....706
William H. Murray, *Deloitte & Touche*

Can the Internet be Controlled? 709
Chair: Vin McLellan, The Privacy Guild
Panelists:
James Bidzos, *RSA Data Security, Inc.*
Thomas Black, *Smith System Engineering, Ltd.*
Patricia Edfors, *US Government's Public Key Infrastructure (PKI) Steering Committee*
David Farber, *University of Pennsylvania*
David Harper, *National Computer Security Association*

Assurance/Criteria/Testing — Track E

Alternate Assurances: Implementation of Better Ways! 712
Chair: Mary Schanken, *National Security Agency*
Viewpoints:
Trusted Capability Maturity Model (TCMM) 712
LT Renell D. Edwards, *National Security Agency*
Network Rating Methodology (NRM) 712
Todd. D. Schucker, *National Security Agency*
Systems Security Engineering Capability Maturity Model (SSE CMM)....713
Charles G. Menk, III, *National Security Agency*

Commercial Intrusion Detection & Auditing: Installation, Integration & Use from the Security Professional's Prospective....714
Chair: Jim Codespote, *National Security Agency*
Panelists:
Dan Gahafer, *CACI Inc*.
Lawrence B. Suto, *Strategic Data Command, Inc.*
Gordon Coe, *AT&T*

Information Systems Security (INFOSEC) COTS Strategy: A New Approach....715
Chair: Michael G. Fleming, *National Security Agency*
Panelists:
Thomas J. Bunt, *National Security Agency*

David E. Luddy, *National Security Agency*
Louis F. Giles, *National Security Agency*

R & D — Track F

Database Security: Browsers, Encryption, Certificates and More 717
Chair: John Campbell, *National Security Agency*
Panelists:
Tim Ehrsam, *Oracle Corporation*
Viewpoints:
Architecture and Components for Data Management Security: NRL Perspective....722
Carl Landwehr, J.N. Froscher, *Naval Research Laboratory* slides
Viewpoints:
Tom Parenty, *Sybase, Inc.* 729

Wrappers, Composition and Architecture Issues for Security and Survivability....730
Chair: Teresa Lunt, *Defense Advanced Research Projects Agency*
Panelists:
Franklin Webber, *Key Software*;
Viewpoints:
Experiments with Software Wrappers....731
Lee Badger, *Trusted Information Systems*
Survivability Architectures....733
John Knight, *University of Virginia*
Composable Replaceable Security Services....734
Rich Feiertag, *Trusted Information Systems*

Survivability Technologies....736
Chair: Teresa Lunt, *Defense Advanced Research Projects Agency*
Viewpoints:
Computational Immunology for the Defense of Distributed Large Scale Systems 736
Maureen Stillman, *ORA*
Event Monitoring Enabling Responses to Anonmalous Live Disturbances 737
Phillip Porras, *SRI International*
Automated Response to Detected Intrustions....738
Dan Schnackenberg, *Boeing*
Common Intrusion Detection Framework....739
Stuart Staniford-Chen, *University of California, Davis*

Manhattan Cyber Project....740
Chair: Mark Gembicki, *WarRoom Research*

Policy/Administration/Management — Track G

Computer Security in the Year 2000 747

Chair: Richard Lefkon, *Year 2000 Committee of AITP SIG-Mainframe*
Panelists:
Gregory Cirillo, JD; Williams, Mullen, *Christian & Dobbin*
Daniel Miekh, *Consultant, Terasys*
Sanford Feld, *President, TBI*

Public Key Certificate Policies 752
Chair: Noel Nazario, *National Institute of Standards and Technology*
Panelists:
Santosh Chokhani, *CygnaCom Solutions Inc.*
Warwick Ford, *VeriSign Inc.*
Michael Jenkins, *National Security Agency*

Cryptographic Standards for the Next Century 754
Chair: Miles Smid, *National Institute of Standards and Technology*
Panelists:
James Foti, *National Institute of Standards and Technology*
Viewpoints:
IEEE P1363: A Comprehensive Standard For Public-Key Cryptography 754
Burt Kaliski, *RSA Laboratories*
ANSI X9.F.1 Cryptographic Standards 761
Don B. Johnson, *Certicom*

Professional Development — Track I

DOCKMASTER II, A Lesson Learned: Balancing Security, Technology Advancements & The Desire To Field A System 765
Chair: Steve Kougoures, *National Security Agency*
Panelists:
Cindy Hash, *National Security Agency*
Mark Redenour, *National Security Agency*
William Dawson, *BDM*