Monday, October 16
10:30 am–12:00 noon
Opening Plenary

Lieutenant General Michael V. Hayden, United States Air Force, Director, National Security Agency/Central Security Service (NSA/CSS), Fort George G. Meade, MD. As the Director of NSA/CSS, he is responsible for a combat support agency of the Department of Defense with military and civilian personnel stationed worldwide.

Dr. David J. Farber is the Alfred Fitler Moore Professor of Telecommunication Systems at the University of Pennsylvania, holding appointments in the Computer Science and Electrical Engineering Departments. He was a principal in the creation and implementation of CSNet, NSFNet, BITNET II, and CREN, and was instrumental in the creation of the NSF/DARPA funded Gigabit Network Testbed Initiative.

Dr. Eugene H. Spafford is a Professor of Computer Science at Purdue University. Spafford is director of the Purdue CERIAS (Center for Education and Research in Information Assurance and Security). He has authored several books and many publications dealing with Internet-related computer security. He is respected worldwide for his work in computer ethics and vulnerability analysis.

Wednesday, October 18
7:00 pm
Conference Banquet

Mr. Mark Rasch is Vice President of Global Integrity Corporation in Reston, Virginia. In this capacity, he advises banks, insurance companies, entertainment companies, and other Fortune 100 companies on legal and policy issues relating to doing business in Cyberspace. He has written and lectured extensively on computer crime, privacy, trademark and trade secret issues on the Internet, and has been featured in the New York Times, ABC’s Nightline, PBS’ Technopolitics, CNBC, and NPR as an expert on computer law and policy.

Thursday, October 19
10:30 am–12:00 noon
Closing Plenary

Mr. Michael Jacobs, Deputy Director for Information Systems Security, National Security Agency

Mr. Simon Gauthier, Deputy Chief, Information Technology Security, CSE, Canada

Dr. William Mehruron, Director, Information Technology Laboratory, NIST

The Closing Plenary will be a North American Panel Discussion on issues relevant to Information Assurance, Technology, and Security. The speakers will discuss common goals and needs for the future of their respective countries.
**Schedule**

*Please Note: Presentations have been graded as to their degree of technical difficulty—with 1 being the least difficult and 5 being the most difficult.*

**Monday, October 16, 2000**

**Earlybird Sessions**

8:30am—10:30am

**Rooms 301—303**

**Killer Apps—and You’re Dead Meat**

*The Code That Shagged Me*

(p. 475)

G. Mark Hardy, Guardent, Inc.

As our computing model shifts from a well-controlled client/server model to that of the active desktop, a flood of dangerous and malicious code is now coursing through enterprise networks. From Melissa to ILOVEYOU to the next attack, our traditional means of screening out malicious code seem to be letting a lot through. We'll take a look at the most significant attacks of this past year, see how well (or poorly) the security infrastructure responded, and provide recommendations as to how you can better protect yourself in the future.

Technical Degree of Difficulty = 2

**Room 324**

**Conference Overview—Welcome Newcomers**

Mark Wilson, NIST

The NIST Program Chair for this year’s Conference will welcome newcomers to the 22nd NISSC and help them navigate their way through their many choices during the next 3.5 days.

**Room 330**

**Paper Session: Student Papers**

Session Chair: (TBD)

**The Competitive Intelligence and National Security Threat From Website Job Listings**

Jay Kranow, Georgetown University

**The Case for Beneficial Computer Viruses and Worms—A Student’s Perspective**

Greg Moorer, Mississippi State University

**Subliminal Traceroute in TCP/IP**

Thomas E. Daniels, Purdue University

**10:30am—12:00noon**

**Rooms 307—310**

**Opening Plenary**

Opening Plenary Keynote Speakers:

Lieutenant General Michael V. Hayden, USAF, Director, National Security Agency/Central Security Service (NSA/CS)

Dr. David J. Fischer, Alfred P. Sloan Professor of Telecommunication Systems at the University of Pennsylvania

**National Computer Systems Security Award Winner:**

The NIST Information Technology Laboratory and the NSA National Computer Security Center present the 2000 National Computer Systems Security Award to Dr. Eugene H. Spafford, Professor of Computer Science at Purdue University.

---

**Don't miss the Awards Ceremony**

Ceremony: 5:30 p.m., Room 310

Reception: 6:15 p.m., Pratt Street Lobby
Room 308

AES and Beyond (p. 490)
Chair: Elaine Barker, NSA
Jim Foti, NIST
(ToD)—Submitter of the selected AES algorithm
Bill Burr, NIST
Marcus Leech, Nortel Networks

The end of the AES development process is now in sight. The algorithm has been selected, and the draft standard is ready for public comment. After nearly four years of intensive effort, what has been accomplished? What has been learned? What would we do differently? What are the next steps in making AES the international standard that was intended? And—what lies beyond AES? NIST is in the process of initiating a number of other cryptographic activities, including a standard specifying modes of operation for symmetric key block ciphers (e.g., AES), an HMAC standard, a key management standard, a new and enlarged hash function that is consistent with the AES key sizes, and an increase in key sizes for the Digital Signature Algorithm (DSA).

Technical Degree of Difficulty = 2 to 3

Room 309

NIAP/Common Criteria Scheme Presentations
Chair: Tom Anderson, NSA

Room 310

Effective Risk Analysis (p. 494)
Thomas Pelletier, Symantec Corporation

The dictionary defines RISK as someone or something that creates or suggests a hazard. In today’s environment, it is one of the many costs of doing business or providing a service. Information security professionals must understand that nothing ever runs smoothly for very long. Any manner of internal or external hazard or risk can cause a well run organization to lose competitive advantage, miss a deadline, or suffer embarrassment. This session will review the current practical application of cost-effective risk analysis.

Technical Degree of Difficulty = 3

Rooms 327–329

The Secret and Below Interoperability (SABI) Process—Continuing the Discovery of Community Risk (p. 492)
Chair: Mark Loepker, NSA
Curtis Dukes, NSA
Charles Schreiner, NSA
Willard Unkenholz, NSA
Corky Parks, NSA
Dallas Pearson, NSA
Warner Brake, NSA

Secret and Below Interoperability (SABI) is an Information Assurance initiative mandated by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I). SABI improves the security posture of all secret and below DoD systems by using a community-based risk acceptance approach. During the discussion about the current status of the SABI program, the panel will focus on the progress and impact of the National Information Assurance Certification and Accreditation Process (NIACAP), NSTISSI 1000.

Technical Degree of Difficulty = 3

Room 330

Paper Session: Intrusion Detection Session Chair: Becky Bace

Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection (p. 13)
Susan M. Bridges, Mississippi State University

Next Generation Intrusion Detection: Autonomous Reinforcement Learning of Network Attacks (p. 1)
James Cannady, Georgia Institute of Technology

Multiple Self-Organizing Maps for Intrusion Detection (p. 32)
Brandon Craig Rhodes, Georgia Institute of Technology

Rooms 331–332

Themes and Highlights of the New Security Paradigms Workshop 2000 (p. 515)
Chair: Steven J. Greenwald, INFOSEC Consultant
Simon N. Foley, University College, Cork, Ireland
Cynthia Irvine, Naval Postgraduate School
Kai Rannenberg, Microsoft Research Cambridge, UK
Emilia Rosti, Università degli Studi di Milano, Italy

This panel will highlight a selection of some of the most interesting and provocative papers from the 2000 New Security Paradigms Workshop (NSPW), held September 19–21 in Ballycotton, County Cork, Ireland. In keeping with the NSPW philosophy, this panel will challenge many of the dominant paradigms in information security. It will be highly interactive; we expect lively exchanges between the panelists and the audience. Come prepared with an open mind and a willingness to question and comment on what our panelists present and be sure to strap on your seat belt! The panel will consist of four authors selected with great pain and difficulty from the great papers presented at the last NSPW.

Technical Degree of Difficulty = 3
Room 308

State of Key Recovery: Government and Industry
Chair: Santosh Chokhani, CygnusCom Solutions/an
Entrust Technologies Company
Donna Dodson, SSA
Diane Dunsee, NSA
Santosh Chokhani, CygnusCom
Cragin Shelton, The Mitre Corporation
David Gross, Microsoft

As government agencies use PKI technology for confidentiality (i.e., encryption of communicated messages), key recovery will play an increasingly important role. The well designed key recovery system ensures that the authorized managers within the organization can decrypt the communication while the employee is not available. The purpose of this session is to provide a status of the various key recovery initiatives in the Government and to provide a description of the capabilities in the commercial products.

Technical Degree of Difficulty = 3

Room 309

National Information Assurance Partnership—2001
Chair: Ron Ross, NIST
L. Arnold Johnson, NIST
Gene Troy, NIST
Peter Mell, NIST

The National Information Assurance Partnership (NIAP) is a U.S. Government initiative originated to meet the security testing needs of both information technology (IT) consumers and producers. This session will provide updates on several high visibility NIAP projects to include smart card security specification, security in healthcare systems, automated security testing, development of security specifications for critical information technologies, specification tool kits, and the Common Criteria evaluation and validation program.

Room 310

Network-Based Contingency Plans
Thomas Pelletier, Nexity Corporation

Attempting to complete an organization-wide or even a data center disaster recovery plan can be a daunting task. However, by using some tested project management techniques, the process can be divided into a manageable undertaking. In this session we will review the process used by successful DRP developers and how they break down the processes and then prioritize the tasks. By identifying what needs to be done first, the efforts of the DRP team can be concentrated on those elements that will provide the organization with the quickest return on its investment.

Technical Degree of Difficulty = 3

Room 327–329

Department of Defense (DoD) Wide Information Assurance Program (DIAP): Current Initiatives (p. 525)
Chair: Captain J. Katharine Burton, USN, DoD
Terry Bartlett, DIAP
George Bieler, DIAP
Jim Christy, DIAP

This panel will begin with an overview of where the DIAP stands today and what activities/initiatives have been accomplished in the past year. Following that will be presentations on three areas where significant effort is currently being spent: IA Metrics, IT/IA Professionalization and Law Enforcement. Each presenter will discuss where their initiative currently stands, what activities are ongoing within DoD and the various services/agencies, and what the activity will contribute to the improvement of the IA posture of the Department.

Technical Degree of Difficulty = 3–4

Room 330

Paper Session:
Practices, Curses, and Risks
Session Chair: (TBD)

Best Security Practices:
An Overview (p. 56)
Guy King, Computer Sciences Corporation

The Curse of Service: Civil Liability for Computer Security Professionals (p. 43)
Arthur J. Wylie, New College of California School of Law

Visualizing Risks: Icons for Information Attack Scenarios (p. 71)
Hilary H. Hsosier, Data Security, Inc.

Room 331–332

Security and Source-Available Systems:
Risks and Opportunities (p. 531)
Chair: Peter G. Neumann, SRI International
Jay Beale, Bastille Linux
Crispin Conson, WinX Communications, Inc.
Eric Raymond, Open Source Initiative

Today’s mass-market proprietary closed-source software seriously impedes efforts to improve installed systems in response to recognition of new vulnerabilities and risks. Source-available software provides a potential alternative, enabling open collaborative efforts, widespread review of source code, rapid generation and acquisition of fixes, and widespread community collaboration. Additional benefits also accrue from well-defined open requirements and open specifications. This panel will explore the source-available alternatives and how they might best contribute to the development and operation of meaningfully robust secure systems.

Technical Degree of Difficulty = 2 to 4
**Room 303—303**

**Aspects of InfoSec: The UK View** (p. 562)

**Chair:** John Doody, SESG, UK

Roger Griffin, Civil Service College, UK

Terry Wells, Department of the Environment, UK

John Laskey, Home Office, UK

John Peters, Ministry of Defence, UK

In 1997, the UK Government launched a programme called "Modernising Government." The aim was to have government departments connected electronically and allow the UK citizen to access government departments. Part of the Modernising Government initiative was the launch of the Government Secure Intranet (GSI).

The challenge facing the security authorities was how to implement a secure architecture that would allow the safe handling of both classified and unclassified information. This presentation will highlight the development of the GSI, case studies associated with the rules in place to join the GSI and the impact and relevance of BS7799 in setting security standards.

**Technical Degree of Difficulty = 3**

**Room 307**

**Certified vs Secure** (p. 533)

**Chair:** Jon David, Lehmann Brothers

Sarah Gordon, IBM

Tim Polk, NIST

Dan Woolley, Global Integrity Corporation

Fred Kolbrenner, Vacta Corporation

Proper products and processes are necessary to secure systems and operations, but this implies the ability to accurately differentiate between alternatives. Few of us have either the ability or time to attempt formal comparative evaluations. We look to outside certifiers, but how good are they, how honest are they, how do their results apply to specific requirements? This session examines the implications of various types of certification, and suggests ways to best use what's available.

**Room 309**

**Achieving Global Trust in an e-World** (p. 536)

**Chair:** Richard G. Wilsher, the Zyngue partnership, GII

**Panelists:**

Michael S. Baum, VeriSign inc., US

Caelen King, Baltimore Technologies plc., IE

Helmut Kurnth, atsec GMBH, IE

The ISSC has a long and respected heritage as an important event in the field of information security. However, in recent years the influence of "nfosec" has spread pervasively into the commercial domain; in that time its scope has also become fundamentally international. This panel has come about because its members believe that it is appropriate for the ISSC to now adopt a broader approach and to reach out to a much wider international audience. This session will bring to a largely US audience some specific European perspectives and awareness of ongoing work. It is intended to be interactive, even provocative: members of the audience will be invited to respond and debate the issues in terms of the relevance of this work to the US business environment and exploring ways in which joint cooperation could be fostered. Technical Degree of Difficulty = 3.5

(Business-focused; not for pure techies)

**Room 309**

**Common Criteria Tools: A Status and Demonstration** (p. 588)

**Chair:** Kris Britton, NSA

Gary Guinauer, Mitretek Systems

Jim Williams, Independent Consultant

This panel will provide a demonstration of the Common Criteria Toolset (i.e., CC Toolbox™, CC Profile Knowledge Base™) developed by the National Information Assurance Partnership for information security professionals responsible for writing and justifying security requirements. It will include an explanation of the latest updates as well as a plan for its continued development in 2001.

**Technical Degree of Difficulty = 3**

**Room 310**

**Preparing for Intrusion Detection** (p. 553)

Thomas Pellett, Netivy Corporation

Systems and networks are subject to attacks both internally and externally. The increasingly frequent attacks on Internet-visible systems could be attempts to steal your company's jewels, personal employee and customer information, or use of your computer resources. Intrusion detection systems collect information from a variety of vantage points within the operating systems and networks. This session will examine intrusion-detection and vulnerability-assessment technologies that will allow your organization to protect the enterprise from losses associated with network security problems. We will review how intrusion detection and vulnerability assessment products fit into the overall security architecture, case histories, and product features.

**Technical Degree of Difficulty = 3**

**Room 327—329**

**Progress of the Best Security Practices Subcommittee** (p. 550)

**Chair:** James P. Craft, United States Agency for International Development (USAID)

Marianne Swanson, NIIT

Mary Schanken, NSA

Marty Poch, EPA

Michael T. Howey, Computer Sciences Corporation

The CID Council's Best Security Practice (BSP) project fills the security knowledge gap between episodic professional classroom training and disorganized electronic bulletin board discussion threads by providing a structured capability for all Federal IT professionals to share first-hand information regarding their security implementation experiences. Upon accessing the BSP website (http://bep.cio.gov) users can easily obtain information most relevant to their unique needs.

**Technical Degree of Difficulty = 2**

**Room 330**

**Paper Session: Access Control**

Session Chair: David Ferruolo, NIST

**Push Architectures for User Role Assignment** (p. 89)

Venkata Bhimindipati, George Mason University

**A Role-Based Delegation Model and Some Extensions** (p. 101)

Ezedin Baka, George Mason University

**Generalized Role-Based Access Control for Securing Future Applications** (p. 115)

Michael J. Konston, Georgia Institute of Technology

**Rooms 331—332**

**Security and Quality of Service Interactions** (p. 583)

**Chair:** Susan Hinrichs, Cisco Systems, Inc.

Klara Nahrstedt, University of Illinois

John McHugh, CERT Coordination Center

Partha Bhattacharja, Cisco Systems, Inc.

Security and quality of service (QoS) are two critical network services in today's inter-networked world. Security mechanisms are used to provide proof of identity, preserve protected information, and ensure that information received has not been tampered with. Quality of service enables multimedia and other real-time services to use public data networks instead of more expensive dedicated networks. This panel session will be geared for attendees interested in network management and design. In particular, this session will be of interest to attendees responsible for the security and quality of service aspects of network design and management.

**Technical Degree of Difficulty = 4**
Room 308
Guideline for Implementing Cryptography in the Federal Government (p. 594)
Annabelle Lee, NIST
The purpose of the Guideline for Implementing Cryptography in the Federal Government (SP 800-21) is to provide guidance to Federal agencies on how to select cryptographic controls for protecting Sensitive Unclassified information. The Guideline focuses on Federal standards documented in Federal Information Processing Standards Publications (FIPS PUBs) and the cryptographic modules and algorithms that are validated against these standards. This guideline was written for Federal employees who are responsible for designing systems, and procuring, installing, and operating security products to meet identified security requirements. The purpose of the presentation is to provide an overview of this guideline.
Technical Degree of Difficulty = 3

Room 309
Innovative Uses of the Common Criteria (p. 613)
Chair: Terry Losonsky, NSA; Jack Sherwood, USN, DoD; John Wildner, USN, DoD; Peter Sargent, COACT Inc.
The session introduces the audience to innovative ways the Common Criteria is used to solve Information Assurance (IA) challenges.
Technical Degree of Difficulty = 3

Room 310
Privacy in the Information Age (p. 597)
Chair: Blaine W. Barnham, University of Nebraska at Omaha; Jeffrey Husker, National Security Council; John Hale, University of Tulsa; David L. Sobel, EFFC; Simson Garfinkel, Information Security Specialist
One of the most potentially disruptive consequences of the Information Age is the impact on personal privacy. The ability for so many to know so much about everyone is growing at an unprecedented rate. Historically, this accumulation of individual personal information has been perceived by the public as sort of a necessary evil, particularly in the case of the credit reporting services. The extent of the accuracy of that information, the case or circumstance under which it was gathered, and the extent to which that information was shared or sold was thought to be more-or-less understood by the public and the sense of personal invasion was limited. Now all bets are off. In Cyberspace, technology enables the recording and reporting of actions without any personal knowledge or awareness. The practice of collecting, consolidating, interpreting, and reselling personal information is for all intents unregulated and, possibly more importantly, not available to the individuals. There is a growing concern for the potential abuses of personal information. This panel attempts to illuminate the many sides to the discussion. What is the government role? What is actually going on—how bad is it out there? What is the commercial sector trying to accomplish?
Technical Degree of Difficulty = 4

Rooms 327–329
Critical Infrastructure Protection for Chief Information Officers or CIOs (p. 596)
Chair: John C. Davis, Mitretek; John M. Gilligan, Department of Energy; Col John E. Whiteford, USAF, NSA
Linda Burek, Department of Justice
Since the signing of the Presidential Decision Directive on Critical Infrastructure Protection (CID) and the publication of the National Plan for Information System Protection, CIOs have new responsibilities. They must protect the infrastructures of their departments and agencies; help to make the government a model for the private sector; and transition the lessons learned from the successful PDD effort to CIP. The panel will explore how CIP responsibilities will be accomplished in their organization.
Technical Degree of Difficulty = 2

Room 330
Paper Session: Malicious Code
Session Chair: (TBD)
The Evolving Virus Threat (p. 141)
Carey Nachenberg, Symantec Corporation
Crispin Cowan, WinX Communications, Inc.
Antivirus Software Testing for the New Millennium (p. 125)
Sarah Gordon, IBM Research

Rooms 331–332
RSA Digital Signature Standards (p. 775)
Burt Kaliski, RSA Laboratories
Standards, theory and practice have resulted in a variety of digital signature schemes based on the RSA public-key cryptosystem, including PKC’s #1, ANSI X9.31, and the Bellare-Rogaway Probabilistic Signature Scheme (PSS). This presentation describes these schemes and gives a strategy for improving long-term security as well as interoperability of digital signature standards based on the RSA algorithm.
Technical Degree of Difficulty = 4
Tuesday, October 17, 2000

1:30 p.m. – 3:00 p.m

Rooms 301—303
Protection of B2B Exchanges and Vendor Operations (p. 638)
Chair
Charlie Baggett, Risk Management Associates, Inc.

Panels
Tim Ehrsam, Oracle Corporation
Nick Pizzola, Verseign
Gary Secret, Johnson & Johnson

This panel will address the risks and remedies associated with the security of operating business-to-business (B2B) exchanges and vendor websites. Every new technology and paradigm being hit new risks, and B2B Internet business is no exception. This panel will discuss the risks associated with this new business area and the remedies which can be applied to reduce those risks. Panelists will come from the commercial sector, defense/commercial industry, and government.

Room 307
Federal Bridge Certification Authority (FBCA) Demonstration and Panel—Part I (p. 614)
Chair
Richard A. Guilia, FederalIST Steering Committee
Panels
Tim Polk, NIST
Stanley Cholstrey, GSA
Dave Ellingham, NRC

This panel will discuss efforts to establish and operate a Federal Bridge Certification Authority (FBCA) to support peer-to-peer, non-hierarchical interoperability among disparate agency PKI domains. The discussion will cover (a) how interoperability among Federal agency PKI domains may be affected on a policy and technical level; (b) why the FBCA concept has emerged as the most attractive solution; (c) how the FBCA has been implemented and tested in prototype form; (d) how the production FBCA is being developed; (e) what the principal challenges are on a policy and technical level; and (f) how the FBCA activities will be managed pursuant to a Federal IST Policy Authority. Part II of this session will follow immediately at 3:00 p.m.

Technical Degree of Difficulty = 3 to 4

Room 308
Incident Response—Stopping Them Dead in Their Tracks (p. 624)
Chair
Joel David, Lockheed Martin
Robert Stone, UNABET Technologies
Jim Duncan, Cisco
Bill Hancock, Examsa Communications
Richard Reynolds, Merrill Lynch

When security fails, as it always has done and will always continue to do, the reaction to breaches is of prime importance. This panel addresses data breaches, their causes, and defenses against them. Panelists will agree that incidents happen to even the most secure organizations. They will discuss how they react to breaches, the tools available to them, and the remediation actions they take. The panel will discuss how the remediation process is applied against breaches.

Room 309
Chair
Lewis Lorton, Fornum Privacy & Security in Healthcare
Lisa A. Gallagher, Comito Security Services
Paul Zaychuk, EWA-Canada Ltd.
Craig Timmons, USA Medical Network
Ahm Brown, McKesson & Company

This panel will provide an accurate general understanding of how the Common Criteria can order the healthcare industry. Panelists will provide a related discussion of different segments of the community. Topics covered in this panel include: viewpoints of the various industry segments; benefits to various industry segments; drivers for the use of the Common Criteria; obstacles to completion; relationship to regulatory requirements; and risks to the healthcare industry from an unregulated security process.

Room 310
Operational Computer Forensics—The New Frontier (p. 632)
Michael J. Carby, Nixi Corporation

There can be no doubt that preventing unwanted access to systems is a good thing. But what happens if someone has already done it and how do we do it? Computer forensics is a new specialty that can analyze the proper procedures for collecting evidence in a manner suitable for use in apprehending and prosecuting security violators. The first part of this session will identify key elements in building an effective Computer Forensics program. The second part will focus on ways to configure clients and servers in a LAN to facilitate forensic data collection.

Room 330
Paper Session: Case Studies (p. 640)
Chair
James Bray, NIST

Using B Method to Formalize the Java Card Runtime Security Policy for a Common Criteria Evaluation (p. 179)
Stéphane Morel, Comito, France

Penetration Analysis of a Xerox Docucenter DC 230ST: Assessing the Security of a Multi-Purpose Office Machine (p. 167)
Benjamin A. Kuperman, Paulus University

Analysis of Terminal Server Architectures for Thin Clients in a High Assurance Network (p. 199)
Cynthia Irvine, Naval Postgraduate School

Rooms 331—332
Information Assurance Metrics: Prophecy, Process, or Pipedream? (p. 640)
Chair
Ronda K. Henning, Harris Corporation
John McGivern, Carnegie Mellon, Center for Survivable Systems
John Michael Williams, JEW Trading Company

Information Assurance has long been considered a "black art"—good security engineering knows a good security design or implementation by imitation, not by quantifiable measures.

This panel seeks to present four perspectives on information assurance measurement: 1) The perspective of information assurance metrics being attainable in the near term, if a disciplined, scientific approach is applied to the problem; 2) The perspective that service level agreements provide a near term approach to determining the information assurance capabilities of a service provider; 3) The perspective of useful assurance processes with the use of auditing to ensure process execution, with the realization these assurance processes will never replace good, basic assurance mechanisms; and 4) The perspective of the information assurance community learning from the software engineering disciplines and their repeated attempts to turn good software development practices into a quantitative measurement-based science before information assurance metrics take a similar path.
Room 307

Federal Bridge Certification Authority (FBCA) Demonstration and Panel—Part II
Chair: Richard A. Guiska, Federal PKI Steering Committee
Tim Polk, NST
Stanley Choffrey, NSA
Dare Fillingham, NSA

This panel will discuss efforts to establish and operate a Federal Bridge Certification Authority (FBCA) to support peer to peer, non-hierarchical interoperability among disparate agency PKI domains, and ultimately with FKI domains external to the Federal government. The discussion will cover: (a) how interoperability among Federal agency PKI domains may be effected on a policy and technical level; (b) why the FBCA concept has emerged as the most attractive solution; (c) how the FBCA has been implemented and tested in prototype form at the Electronic Messaging Association Challenge 2000 conference in April 2000; (d) how the production FBCA is being developed; (e) what the principal challenges are on a policy and technical level (including directories and clients); and (f) how the FBCA activities will be managed pursuant by a Federal PKI Policy Authority.

Technical Degree of Difficulty = 3 to 4

Room 308

Incident Response—Tracking Them Down—Part II
Bill Hancock and Charles Neal, Exodus Communications

Ok, you’ve found out you’ve been attacked, cracked or hacked (depending upon your definition). You may even have stopped it successfully—for now. The problem remains: what do you do about finding out where the attacker is coming from and what can you do to mitigate damage in the future or deal with the attacker in real-time when it happens again. The speakers in this session have been here and done that. Both have many years in tracking down, literally, hundreds of hackers, crackers, cyberterrorists, extortionists and other manners of cybercriminals. This session will provide insight on how to properly track incoming attacker activities, the use of technologies such as “clean” Trojan Horse programs to deceive attackers, the use of “honeypot” and other “saturator” techniques, evidence collection and preservation, chain of custody issues, what law enforcers need and want on prosecutions, and the myriad of other information needed to successfully track attackers to their fair and get law enforcement engaged to prosecute.

Room 309

The Healthcare Vertical Turns Its Eyes on Security—The Impact of HIPAA and other Legislation on Security Engineering (p. 671)
Lisa A. Gallagher, Exodus Security Services; and Lewis Lorton, Forum on Privacy and Security in Healthcare

This session will provide an accurate and general understanding of relevant healthcare legislation, and will provide specific understanding of patient rights and the requirements for use, disclosure and authorizations for patient records. Topics to be covered in this session include: a history of privacy and security regulations for healthcare, HIPAA and administrative simplification, relevant regulations that flow from HIPAA, how this affects security engineering, compliance issues, and implications of non-compliance.

Room 310

Information Systems Survivability: Protecting Critical Systems (p. 656)
Chair: Richard C. Linger, CERT Coordination Center
Robert J. Ellison, CERT Coordination Center
John McCullough, CERT Coordination Center

Increasing societal dependence on large-scale, distributed information systems amplifies the consequences of intrusions and compromises. It is vital that these critical systems survive to provide essential functions even when operating under adverse circumstances. The objective of this tutorial is to describe the practical techniques for survivability analysis and design that attendees can apply in their own environments. In particular, the tutorial introduces the Survivable Network Analysis (SNA) method developed by the SEI’s CERT/CC, as a means to assess and improve survivability and security characteristics of planned or existing information systems. The SNA method introduces concepts of mission survivability, essential services, intrusion scenarios, intrusion resistance, recognition and recovery (the three R’s), and Survivability Maps. The tutorial will present a case study of survivability analysis, and will discuss survivability research activities.

Technical Degree of Difficulty = 3

Rooms 327–339

Access Certificates for Electronic Services (ACES)—Enabling Government to Citizen Interaction via the Internet (p. 654)
Chair: Judith Spencer, GSA
David Temoshok, GSA
Stanley Choffrey, GSA

The Access Certificates for Electronic Services (ACES) program utilizes industry partners providing COTS solutions designed to facilitate secure, on-line access to Government information and services by the Public through the use of a PKI. The ACES vision is that a single member of the public or business representative would have one digital signature certificate with which he or she could do business with a variety of Federal agencies, including the electronic signing of forms prior to submission. This panel will discuss the value of public key technology and digital signatures for doing business on the Internet, present actual case studies, and provide a live demonstration of an ACES transaction.

Room 330

Paper Session: Common Criteria Issues
Session Chair: Pat Toth, NST

Thoughts and Questions on Common Criteria Evaluations (p. 203)
Kenneth G. Osthoff, NSA

Towards the Formal Modeling of a Secure Operating System (p. 408)
Dan Zhou, Florida Atlantic University

The Open Platform Protection Profile (OP3)—Taking the Common Criteria to the Outer Limits (p. 211)
Mark Kecsketh, VISA International Services Association

Rooms 331–332

Issues in High Performance Computing Security (p. 657)
Chair: Rayford B. Vaughn, Jr., Mississippi State University
Yvo Desmedt, Florida State University
Douglas Engert, Argonne National Laboratory
Jesse Pollard, DoD

This panel is composed of researchers and practitioners in the area of high performance computing (HPC) security and its purpose is to address whether or not HPC represents new security issues or whether traditional solutions apply. This topic has been addressed at the NiSSC for the past two years in the form of technical papers—but the opportunity has not yet been presented for a panel discussion on the topic. This panel seeks to close that gap and to describe not only positions associated with this interesting topic, but to also describe current research in the field.
Room 301—303

Guerrilla Security: The Martial Art of Infosecurity (p. 699)
Andrew T. Robinson, net/main InfoSecurity Solutions

While the basic principles of InfoSecurity have not changed in decades, the needs and realities of the InfoSecurity threat environment have changed radically in the past few years. Many InfoSecurity policies have failed to adapt to this reality. Such inertia means that the InfoSecurity policy does not adapt to the needs of the organization and to new threats. Guerrilla Security, also called RAPID (Rapid Policy Innovation & Deployment) is a methodology based on flexibility and rapid response. These characteristics allow an organization to practice conservative InfoSecurity practices while remaining responsive to the needs of the organization and to new InfoSecurity threats.

Room 307

Your Always-On Connection & the Telecommuter (p. 618)
Chair: Peter Ginsmore, NAI Labs, Network Associates
Michael St. Johns

Always-on Internet access to the home provided by emerging broadband technologies such as cable modems and DSL is changing the way we live and work. Reasonable bandwidth connections coupled with instant and constant access is integrating the Internet into our lives. This panel will explore the security implications of not only this new technology, but also of the changing work models. What are the risks to a home user? To a telecommuter? Where are the risks to corporations that set up virtual offices over the Internet? This panel will also explore the solutions that are available. Do I need a personal firewall? What will a VPN provide? Finally, the panel will explore what the future might hold.

Technical Degree of Difficulty = 4

Room 308

Distributed Denial of Service Attacks—Can We Survive This New Threat? (p. 682)
Chair: Jon David, Lehman Brothers
Steve Bellovin, ATEC Labs Research
Bill Cheswick, Lucent Technologies
Paul Ferguson, Cisco

DDoS attacks have recently made headlines by taking down major networks and services. The sharing of attack ‘enhancements’ and the providing of attack tools via the Web makes these attacks a growing threat. This session investigates the nature and elements of DDoS attacks, and presents things to be done by users, sys admins, ISPs, router vendors, and the like to best treat this threat. Key areas it will treat are: What is a DDoS attack? How is DDoS different from other attacks? Can they be detected in time? What security/network practices need to be in place? What user preparation is necessary for DDoS? What industry preparation is necessary for DDoS?

Room 309

Understanding FIPS 140-2 Validation (p. 712)
John Morris, Core Security

Hear a former FIPS 140-1 lab manager explain what these cryptographic module security certifications truly mean, how they affect government purchasers and commercial vendors, and how future validations will change. The session will include an interaction with the audience and candid discussion on FIPS 140-2 and other government security validations. Explore whether current US and Canadian security standards effectively enhance COTS cryptography products designed by international companies.

Technical Degree of Difficulty = 3

Room 310

Single Sign-on: Myth or Reality (p. 685)
Thomas Pelletier, Netegrity Corporation

As enterprise computing becomes more and more complex, with business systems installed across multiple platforms, form mainframe to client-server to PC, the need for a secure way to provide users with a single authentication point becomes more and more important. There are a number of methods and products on the market today with which we will examine what you will need to do to be prepared for secure single sign-on. We will also identify a set of functional requirements for a secure single sign-on methodology, so that attendees will be better able to compare the products available.

Technical Degree of Difficulty = 3

Room 324—325

Strong Authentication
Chair: Fred Tompkins, KTSI (TBD)

Strong authentication is characterized by the use of at least two kinds of (or more) evidence, at least one of which is resistant to replay. While there is a consensus for this kind of solution among security people, it has been resisted by management as expensive and by users as awkward or burdensome. This panel will demonstrate several desktop-based commercial solutions to this problem. These solutions will be used to demonstrate that the cost is measured in pennies per user per day and that by basing the solution on the desktop, the solutions can be made easy for the user.

Room 327—329

“Hands-On” Approach of Building a Security Program (p. 684)
Bill Hadesty, USDA

One of the Federal Government’s largest civilian departments has hired you to put a new IT security program in place quickly with limited funding. Where do you start when the goal is to have the Department of Agriculture become a model for computer security in three years? Where do you start when your boss was one of the authors of the Computer Security Act of 1987? This is the challenge faced by Bill Hadesty as the Associate CIO for Cyber Security at USDA. Drawing on experience gained while developing and implementing a similar program at the IRS, Mr. Hadesty will outline strategies for providing leadership and direction, ensuring compliance with laws and regulations, establishing and enforcing standards and policies, and providing security expertise and oversight.

Technical Degree of Difficulty = 1

Room 330

Paper Session: Architectures

Session Chair: (TBD)

Chair of Trust in a Digital Signature System Based on a Smart Card (p. 267)
Jean-Luc Gisquet, Compiègne, France

An Efficient Secure Authenticated Group Key Exchange Algorithm for Large and Dynamic Groups (p. 254)
Jim Alves-Foss, University of Hahn

Business Process Driven Framework for Defining an Access Control Service Based on Roles and Rules (p. 234)
Ramaswamy Chandramouli, NIST

Rooms 331—332

Information Security Research and Development in Academia (p. 706)
Chair: Susan M. Bridges, Michigan State University
Blaine W. Burnham, University of Nebraska
Dipankar Dasgupta, University of Memphis
James A. Davis, Iowa State University
Cynthia Irvine, Naval Postgraduate School

Research and development activities in information security within academia have been largely limited to a small number of institutions and research centers. This panel will present a sampling of the types of research in the area of information security that are being conducted at universities.

Technical Degree of Difficulty = 5
## Conference at a Glance
### Monday, October 16, 2000

<table>
<thead>
<tr>
<th>Room</th>
<th>8:30-10:00</th>
<th>10:30-12:00</th>
<th>1:30-3:00</th>
<th>3:30-5:00</th>
</tr>
</thead>
<tbody>
<tr>
<td>307</td>
<td>Opening Plenary Keynote Speakers: Lieutenant General Michael V. Hayden Dr. Dave Farber</td>
<td>Future of Information Security</td>
<td>Evaluation Scope: Does One Size Fit All?</td>
<td></td>
</tr>
<tr>
<td>308</td>
<td></td>
<td>Advanced Encryption Standard and Beyond</td>
<td>State of Key Recovery for the Government and Industry</td>
<td></td>
</tr>
<tr>
<td>309</td>
<td>Systems Security Award: Dr. Eugene Spafford, Purdue University</td>
<td>NIAP/CC Scheme Presentations</td>
<td>NIAP Projects—2001</td>
<td></td>
</tr>
<tr>
<td>310</td>
<td></td>
<td>Effective Risk Analysis</td>
<td>Network-Based Contingency Plans</td>
<td></td>
</tr>
</tbody>
</table>

**Solutions**

<table>
<thead>
<tr>
<th>Room</th>
<th>324–326 Solutions</th>
<th>327–329 An Overview to the Conference</th>
<th>330 Papers Student Papers</th>
<th>331–332 Incident Response Fundamentals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Secret and Below Interoperability (SABI)</td>
<td>Intrusion Detection</td>
<td>New Security Paradigms Workshop 2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Practices, Cures, and Risks</td>
<td>Security of Source-Available Systems</td>
</tr>
</tbody>
</table>

## Tuesday, October 17, 2000

<table>
<thead>
<tr>
<th>Room</th>
<th>8:30-10:00</th>
<th>10:30-12:00</th>
<th>1:30-3:00</th>
<th>3:30-5:00</th>
</tr>
</thead>
<tbody>
<tr>
<td>307</td>
<td>Certified vs. Secure PKI—Sham or Salvation? Federal Bridge Certification Authority (FBCA) Demonstration and Panel Part I Federal Bridge Certification Authority (FBCA) Demonstration and Panel Part II</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Solutions**

| Room  | 324–326 Solutions                  | 327–329 Progress of the Best Security Practices Subcommittee Critical Infrastructure Protection for Chief Information Officers or CIP for CIOs Access Certificates for Electronic Services (ACES)—Enabling Government to Citizen Interaction via the Internet |
|-------|-----------------------------------|--------------------------------------|-------------------------------|---------------------------|
| 330   | Papers Access Control Malicious Code Case Studies Common Criteria Issues |
| 331–332 | Security and Quality of Service Interactions RSA Digital Signature Standards Information Assurance Metrics: Prophecy, Process, or Pipedream Issues in High Performance Computing Security |
### Wednesday, October 18, 2000

<table>
<thead>
<tr>
<th>Room</th>
<th>8:30-10:00</th>
<th>10:30-12:00</th>
<th>1:30-3:00</th>
<th>3:30-5:00</th>
</tr>
</thead>
<tbody>
<tr>
<td>308</td>
<td>Distributed DDOS: Can We Survive?</td>
<td>How Do We Prevent Denials of Services</td>
<td>Black Hat — White Hat</td>
<td>Recent Trends in Hacking</td>
</tr>
<tr>
<td>309</td>
<td>Understanding FIPS 140-2 Validation</td>
<td>FP for FIPS 140-2: Lessons Learned</td>
<td>Testing of Crypto Modules Against FIPS 140-2</td>
<td>Cryptographic Module Validation Program</td>
</tr>
<tr>
<td>310</td>
<td>Single Sign-On: Myth or Reality</td>
<td>Biometrics – Understanding the Architecture, APIs, Encryption and Authentication Security for Integration into Existing Systems &amp; Applications</td>
<td>Scorecard for Online Authentication Technologies</td>
<td>The OM-AM Framework and Role-Based Access Control</td>
</tr>
<tr>
<td>330</td>
<td>Papers</td>
<td>Architectures</td>
<td>Refocused Views</td>
<td>Information Access Issues</td>
</tr>
</tbody>
</table>

### Thursday, October 19, 2000

<table>
<thead>
<tr>
<th>Room</th>
<th>8:30–10:00</th>
<th>10:30–12:00</th>
<th>1:00–6:00</th>
</tr>
</thead>
<tbody>
<tr>
<td>301–303</td>
<td>Collusion Detection Las Vegas Style</td>
<td></td>
<td></td>
</tr>
<tr>
<td>307</td>
<td>MLS &amp; Its Evolution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>308</td>
<td>Tracking the Virus Writer: The Legal Ramifications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>309</td>
<td>Anonymous in the Information Age</td>
<td></td>
<td></td>
</tr>
<tr>
<td>310</td>
<td>IA Technologies: 10 Years Past, Present &amp; Future</td>
<td></td>
<td></td>
</tr>
<tr>
<td>324–326 Solutions</td>
<td>Best Security Practices: Lowering Quality’s Total Cost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>327–329</td>
<td>Computer Security from the Trojan War to Now</td>
<td></td>
<td></td>
</tr>
<tr>
<td>330</td>
<td>Papers</td>
<td>Operating Systems and Their Effects on Information Security</td>
<td></td>
</tr>
<tr>
<td>331–332</td>
<td>Smart Card Security Users Group PP &amp; Projects</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
10:30am—12:00 noon

Rooms 301—303

An Introduction to Consequence-Based Risk Assessment (p. 738)

This tutorial will present the basics steps involved in a consequence-based IT risk assessment, the advantages of a consequence-based approach, and the differences and relationships among threat, vulnerability, and risk. It will show how qualitative threat, vulnerability and consequence information can be combined to derive a qualitative value for risk and offer an easy-to-understand graphical way to present risk assessment results. The tutorial will conclude with a brief discussion of uncertainty and risk mitigation.

Technical Degree of Difficulty = 1

Room 307

Security for High-Speed Internets (p. 721)

Chair: Jeff Ingle, Community Management, Staff
Chris Kubie, NSA

The explosion in the growth of the Internet and private networks has been driving faster network speeds and increased services. New technologies and protocols are flooding this growth and are expected to meet the increasing bandwidth demands. Security could be an enabling factor in this growth, but there are some strong challenges in providing the security and survivability for future networking. Some of the security and survivability challenges in future networking include encryption, authentication, key management, data integrity, the role of firewalls and guards, and scaling network and security management.

Technical Degree of Difficulty = 4

Room 308

How Do We Prevent Denials of Service? (p. 723)

Chair: Peter G. Neumann, SRI International
Steve Bellows, AT&T Labs
Virgil Ogier, University of Maryland
J.F. Mergen, Genuity
Mary Schaefer, ARPA

Subsequent to earlier denial-of-service (DoS) flooding attacks, the flurry of distributed denial-of-service attacks in February 2000 has intensified the realization that the problems we face are complex in our information infrastructures—both prevention and integrity in operating systems, networking, protocols, mailer environments, and many other applications, and operational practice. This panel explores what (if anything) can be done to combat denial of service from a total systems/network perspective, hopefully without too seriously compromising the performance that everyone has come to expect.

Technical Degree of Difficulty = 5

Room 309

A Protection Profile for FIPS 140-2,
Lessons Learned (p. 740)
Chair: Miles Smid, CygnaCom Solutions
Jean Petry, CygnaCom Solutions
Shari Galitzer, CygnaCom Solutions
Ray Snouffer, NIST

NIST's Cryptographic Module Validation program has been highly successful validating over 90 cryptographic modules as being compliant with FIPS 140-1. Recently, NIST has drafted a revision of the standard (Draft FIPS 140-2) that offers several improvements, but the testing process remains basically intact. This presentation will explore the feasibility of developing a Common Criteria based Protection Profile for Draft FIPS 140-2. The presentation will cover the lessons learned when trying to map a previously existing standard into the Common Criteria and in developing the corresponding protection profile.

Technical Degree of Difficulty = 3

Room 310

Biometrics—Understanding the Architecture, APIs, Encryption and Authentication Security for Integration into Existing Systems & Applications (p. 729)

William H. Satow, I/O Software, Inc.

This session will explain how to implement and build biometric technology to augment current security systems while explaining specific issues. We will investigate the major biometric technologies, where they fit, and the questions you should ask when looking at these products. Learn how to approach biometric authentication including:

- Seamlessly developing biometrics to enhance your existing security.
- Developing a common methodology for software developers looking to integrate biometrics into their applications.
- Client/Server programming issues to consider.
- User enrollment problems and solutions.
- Developing APIs (Application Programming Interface) to implement a secure system.

Technical Degree of Difficulty = 5

Room 324—326

Desktop Security
Chair: Oscar Marcia, Deleite & Touche (TBD)

For almost four decades now we have worried about Trojan Horse attacks against the mainframe. To date, we have resisted such attacks by recognizing and removing known attack objects. While this worked reasonably well against broad attacks, there is every reason to believe that such defenses will be useless against focused attacks. This panel will present several commercial-off-the-shelf products for securing the desktop. These products may be standalone or integrated with strong authentication called for in the first panel. They may permit some user control but permit management to implement policies which users cannot override.

Technical Degree of Difficulty = 1
Room 301-303
Information Security Year in Review—Technical Vulnerabilities (p. 766)
David Kennedy, ICSA, Inc.
A 90-minute review of the major technical vulnerabilities discovered in systems during the previous 12 months (Oct 99-Sep 00). The tutorial will include discussions of technical problems and draw from CERT advisories, hard-ware and software vendor's advisories and public discussion forums. The intended audience is Information Security (IS) managers and professionals who are too busy to monitor all of these forums. The tutorial will provide a snapshot of major problems and trends that have emerged since the last NISSG.
Technical Degree of Difficulty = 5

Room 307
Security for Domain Name System—Ready for Prime Time (p. 749)
Chair: Olaf Gutmann, NAI
David Conrad, NetworkSEC
Edward Lewis, NAI
John Nguyen, RSA
An operational reality of the latest release of the BIND software by the Internet Software Consortium. Besides being able to trust the name-to-address mapping, DNS will offer benefits to other protocols by making public keys available through DNS, and by accommodating certificates.
This panel will be of interest in learning how it can be secured and anyone that wants to make plans to take advantage of DNSSEC.
Technical Degree of Difficulty = 5

Room 308
Black Hat—White Hat (p. 751)
Chair: G. Mark Hardy, Guidewell, Inc.
Mari Fabro, Guidewell, Inc.
Ray Kaplan, Guidewell, Inc.
Ralph Logan
Black Hat: Netology (internet organization without rules)
This panel discussion will feature a lively interaction between several well-known “white hat” security experts, and a number of “black hat” speakers (the “dark side” of the hacking community). The goal of this session is to provide a question-answer session for attendees to investigate the latest methods used to protect information assets, and what methods are used to attack them. Warning: the black hat presenters will not hesitate to “call it like it is.”
Technical Degree of Difficulty = 4

Room 309
Testing of Cryptographic Modules Against FIPS 140-2 (p. 768)
Chair: Randall Easter, NIST
Annabelle Lee, NIST
Ray Snuffer, NIST
On July 17, 1995, NIST established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to FIPS 140-1, and other FIPS cryptography-based standards. The CMVP offers a documented methodology for conformance testing through a defined set of security requirements in FIPS 140-1 & 2 and other cryptographic standards. The panelists will provide detailed information on the philosophy and goals of cryptographic module testing, the CMVP, conformance/compliance testing, and cryptographic module laboratory accreditation.
Technical Degree of Difficulty = 4

Room 310
Scorecard for Online Authentication Technologies
B. Williams, RSA Security, Inc.
Authentication—the independent validation of the identity of a user, server, or process—is critically important for e-commerce. This session provides a common set of criteria by which to evaluate different mechanisms and an objective scorecard of several popular choices, including username/password, hardware tokens, software tokens, Kerberos, digital certificates, smart cards, and biometrics.
Technical Degree of Difficulty = 4

Room 320—322
End-to-End Encryption
Chair: David Kennedy, ICSA, Inc.
(TBD)
The modern network often provides multiple paths between any two points. Such routing improves the probability that a path will be available and may also provide additional bandwidth on demand. However, these paths may not follow the path that management expects. If the traffic is successfully limited to a reliable path, this path may not be the cheapest, most convenient, or even available when needed. This panel will present a number of commercial-off-the-shelf solutions that secure the traffic all the way from the client to the server. These solutions work across arbitrary networks.

Room 327—329
Cybersecurity in the Year 2000: Not Just for Systems Administrators Anymore (p. 752)
Chair: Richard Shullan, HHS
Danny Markle, HHS
Rhona Large, The Center for Support of Families
Marianne Scanlon, NIST
This panel will look at the issues of cybersecurity as they affect child support enforcement programs. At the Federal and State levels of government, this program provides substantial benefits to single parents and their children. National information systems support State efforts to increase the amount of child support collected. Because of the scope of the data, and the sensitivity of the information, we have taken active steps to ensure privacy and security of data.
Technical Degree of Difficulty = 1

Room 330
Paper Sessions: Information Access Issues
Session Chair: Frank Hendricks, NAI
Controlling Primary and Secondary Access to Digital Information (p. 351)
Marshall D. Abrams, The MITRE Corporation
A Query Facility for Common Intrusion Detection Framework (p. 317)
Shulamit Yisraeli, George Mason University
Secure X.500 Border Directory Proxy Server

Room 331—332
Innovations in Biometric Authentication Technologies (p. 766)
Chair: Jeff Dunn, NAI
Cathy Tilton, SAFELINK
Fernando Padia, NIST
With the advent of the new century, it has become apparent that there is a great need for biometrics. Utilized alone or integrated with other mechanisms such as smart cards, encryption keys, and digital signatures, biometrics can be set to provide nearly all aspects of the economy and our daily lives. The need for biometrics can be found in commerce, in Federal, State and Local governments, in the military and in commercial applications. Trustworthy electronic commerce and electronic government, for example, can be achieved through the utilization of strong personal authentication procedures. Trust in these electronic transactions will be essential to the healthy growth of the global economy.
Technical Degree of Difficulty = 4
Room 309

The Cryptographic Module
Validation Program: FIPS 140-2...The Next Generation (p. 790)
Chair: Annabellee Lee, NIST
Reyn Stevens, NIST
Tom Casar, CSE, California
In the fall of 1998, FIPS 140-1 entered a regular scheduled 5-year review to consider new and revised requirements needed to meet technological and economic change. A revised draft standard was produced based on the public comments received, previously issued implementation guidance and a "line-by-line" review by the NIST, CSE, and the testing laboratory staff. Completion of the FIPS 140-1 update to FIPS 140-2 is anticipated by October 2000. Technical Degree of Difficulty: 2

Room 310

The OAM Framework and Role-Based Access Control (p. 600)
Ravi S. Sandhu, George Mason University
Cyberspace security is fundamentally about control of authority and trust. We don't know what form future systems will take, but they will surely be very different from today's. We can postulate they will be large-scale, highly decentralized, pervasive, cross organizational boundaries and evolve rapidly. Current security doctrine cannot deal with this complex and fluid environment that is inevitably emerging. This tutorial will discuss the speaker's recently proposed OAM framework as a promising approach to security engineering in this brave new world. Technical Degree of Difficulty: 3

Room 311

SNMPv3 with Security and Administration (p. 770)
Chair: Jeffrey D. Case, SNMP Research Inc.
Russ Mundy, SNMP Research Inc.
The Internet standard management framework, based on SNMP, has become a global standard for managing Internets and Internets. As a result of these application environments, there are requirements for strong security for the management function in many environments. This panel session will describe SNMPv3 from the standards view, the vendor view, and the user view. The session will also address the security architecture, layering, and operations, including key management and coexistence and transition issues. Technical Degree of Difficulty: 4

Room 308

Recent Trends in Hacking (p. 771)
Chair: Peter Mell, NIST
Tom Longstaff, CERT
Jeff Moss, DEFCON
Andy Balinsky, Gigo
Chris Rouland, NSS
If hacking techniques remained constant, the problem of computer security would have been solved long ago. Instead, previously unseen hacking paradigms emerge each year that take advantage of new features in software and circumvent security mechanisms. This panel will begin with a history of hacking events and developments starting from the 1970s to the present day. Then, experts from the hacking community, an incident handling organization and a security vendor will discuss emerging hacking trends from their unique vantage point. Technical Degree of Difficulty: 4

Room 327–329

Professional Certification of Information Security Professionals (p. 773)
Chair: Lynn McNulty, RSA Security
James Wade, Air Touch Cellular
William Murray, Deloitte & Touche
Shirley Malia, Critical Infrastructure Assurance Office
Joan Hash, Social Security Administration
This panel will focus on the current state of efforts to elevate the status and effectiveness of information security specialists through the development of professional certification programs. Recent changes to the Federal Government's information technology occupation series recognize that information security has become a separate and distinct career field. The Office of Personnel Management recognizes Professional certification as one of the criteria for qualifying for government information security positions. The members of the panel will discuss various aspects of professional certification. Technical Degree of Difficulty: 1

Room 330

Paper Session: Re-focused Views
Session Chair: (TBD)
Database Security 2000 (p. 388)
John R. Campbell, NSA
Privilege Management of Mobile Agents (p. 362)
Wayne Jansen, NIST
Towards XSL as a Secure Intelligent Agent Communication Language (p. 371)
Alexander N. Korzyky, Sr., Virginia Commonwealth University

Room 331–332

Certificates in the Internet: State, Issues, and Futures (p. 784)
John Linn, RSA Laboratories
This presentation examines current progress, issues, and future directions in IETF work on Internet certificate usage. A certificate profile and operational protocols have been published. Current topics include high assurance qualified certificate management protocols, alternative applications, and time stamping, and attributes certificates for application. Technical Degree of Difficulty: 4
Thursday, October 19, 2000

8:30am—10:00am

Rooms 301—303

Collusion Detection Las Vegas Style (p. 813)
Jeff Jonas, Systems Research & Development

Protecting an organization's assets is becoming an increasingly complex task. The back-and-forth war between attack and defense in turn means creating more sophisticated policies, procedures, and controls. However, even the most advanced protection measures can be rendered useless by collusion. Collusion Detection Technology (CDITECH) provides organizations with a new weapon against the insidious threat of collusion. Technical Degree of Difficulty = 2

Room 307

Multi-level Security (MLS) and Its Evolution to Date (p. 792)
Chair: G.R. "Greg" Clugston, Impact Innovations Group, LLC
Christian Cooke, Impact Innovations Group, LLC
Thomas Bes, Impact Innovations Group, LLC

This panel will discuss the evolution of MLS starting with early efforts in the middle of the last millennium, early use of mechanical ciphers to maintain levels of data security. The panel will go on to discuss MLS in a computerized age taking a look at systems developed for the government and in the private sector. Technical Degree of Difficulty = 3

Room 308

Tracking the Virus Writer—The Legal Ramifications (p. 794)
Chair: Christine M. Orshesky, Esq., Esq., LLC
Cheryl "Jimmie" Kuo, Network Associates, Inc.
Jessica Herrera, Department of Justice
Sarah Gordon, IBM Research (TBD, FBI)

The growing prevalence of denial of service virus attacks has brought law enforcement attention to the computer virus and malware situation. This panel is composed of law enforcement professionals and those that assist in virus investigations and as such can provide insight into the legal requirements and ramifications of virus writing and virus distribution. It is the aim of the panel to provide the online community with ways to effectively address this threat and affect decisions made about appropriate punitive or restitution matters. Technical Degree of Difficulty = 2/3

Room 309

Anonymity in the Information Age (p. 827)
Chair: Blaine Burnham, University of Nebraska
Tony Bertini, Guardiant Technologies
Ed McPherson, PwC
Hans von Spakovsky
Robby Wagner

Anonymity in the information age is positioned to be one of the most contentious issues to be resolved. This panel will explore the issues of just what is the notion of anonymity, how does this notion translate to processes on the Internet, what are the legitimate uses of the available mechanisms, and the method of implementation? The panel will also discuss the stakeholders and what is their take on the status of the discussion. Technical Degree of Difficulty = 2

Room 310

Information Assurance Technologies: 10 Years Past, Present, & Future (p. 810)
Chair: Jack Murphy, Electronic Data Systems
Gary Moore, Extract Technologies, Inc.
Tom Haigh, Source Computing Corporation
Robert Giovagnoli, DEFENSE
Ronald Henning, Harris Corporation

In the next decade Information Assurance will continue to dominate the attention of many CIOs. Simple amateurish e-mail viruses continue to plague CIOs. Professional hackers are becoming more sophisticated every year in identifying and exploiting network, host, and application vulnerabilities. Rapid, effective response to these threats is one of today's biggest problems. This panel consists of five representatives of the Information Assurance industry who will discuss the evolution of Information Assurance technologies and solutions over the next 10 years. Technical Degree of Difficulty = 2-4

Room 324—326

Best Security Practices: Lowering Quality's Total Cost of Ownership in an Age of Growing Complexity (p. 628)
Chair: James P. Craft, United States Agency for International Development (USAID)
Tom Burke, Computer Sciences Corporation
Jack L. Brock Jr., GAO
Gay L. Copeland, Computer Sciences Corporation
Robert E. Giovagnoli, DEFENSE

Best practices efforts have provided useful benchmarks to guide users embarking into areas of new endeavor. The CIO Council's Best Security Practices website takes this idea to a new level. The Federal government is facing enormous costs to secure its IT infrastructure. Avoiding some of these costs will take a new definition of best practices. Technical Degree of Difficulty = 2

Room 327—333

Smart Card Security Users Group
Protection Profile & Projects
Chair: Kenneth Ayer, Visa International
Fernando Laurence, Europay International
Marc Reckert, Visa International

Smart Cards have been around for more than 20 years and are widely used in the financial services and telecommunications industries. They have recently been improved to carry multiple applications, potentially including private keys that can work in conjunction with secure network access. Their security has been assured by proprietary testing and evaluation by their users and the payment associations users have formed to facilitate their common business interests. Recently efforts have been made to bring this security testing into the Common Criteria (ISO/IEC 15408) process. This is not straightforward. This panel will provide an overview of the experiences of the Smart Card Security Users Group (American Express, Europay, JCB, MasterCard, Microsoft, Visa, and MAP) in adapting the Common Criteria evaluation of smart cards. Technical Degree of Difficulty = 3
Thursday, October 19, 2000, 1:00pm—6:00pm

Investigating Computer Virus and Other Malware Incidents

Christine M. Ornesky, iFase, LLC

With the increasing spread of computer viruses and worms that can lurk in an organization, it is no longer feasible to rely solely on single-point detection and repair techniques. Virus-related incidents must be investigated to determine where the virus originated, where it spread, and what damage it may have caused or may cause in the future. This workshop will show you how to make those determinations through effective response and investigation techniques for computer viruses and other malware incidents. The workshop will provide a brief foundation on the functionality of computer viruses and other forms of malware with an emphasis on the ways they can enter an organization, the ways they spread, and the types of damage they can cause.

Key techniques in the response and investigation of such incidents will be discussed and demonstrated. You will have a hands-on opportunity to investigate several computer virus and malware incidents.

Staying Ahead of the Hackers Network Vulnerability Testing

Ken Cutler, Information Security Institute

Protecting and auditing Internet-TCP/IP network technology is a major challenge. In this state-of-the-art session, you will learn how to systematically test the security of important security hot spots for entire TCP/IP networks as well as for individual systems. You will receive the necessary knowledge to build a versatile and powerful cyberspace audit toolkit to test for serious TCP/IP network security vulnerabilities that are frequently exploited by hackers and other intruders. The session agenda includes: an evaluation of the significance of recent incidents, advisories, and trends in network attacks and vulnerability conditions; a systematic, graduated plan for “discovering” a network and identifying serious vulnerabilities sources for obtaining vital information and tools associated with detecting serious Internet/Web security exposures; methods for reviewing freeware, shareware, and commercial tools for auditing the security of individual servers, firewalls, and entire TCP/IP networks, including network discovery tools, network mappers, port scanners, network security scanning tools, host security scanning tools, and firewall and web server security testing techniques. This session assumes a working knowledge of TCP/IP and client/server technology.

Information System Survival School

Gail Brooks, Mary Washington College

Are you just getting started in information security? This course has been designed to help you come up to speed on the significance of computer and network attacks that are directed at your systems! No prerequisites are needed. The axioms of information assurance, confidentiality, integrity, and availability are introduced with examples of real attacks and defensive countermeasures. The most current attacks on the Internet are detailed against an historical backdrop so students can develop a sense of perspective. One attack—the RingZero proxy scanning trojan—is discussed in depth by the analysts who discovered it. This illustrates not just the significance of trojan-based attacks, but the kind of team-based analysis needed to run aground new hacker ploys. A discussion of information warfare at the national level and the issues of infrastructure protection will lead into a “from the trenches” process for incident handling.

Cryptography for Beginners: What Is It and How Can I Use It?

Jim Litchko, Litchko & Associates, Inc.

As with all things technical or bureaucratic, these three letter acronyms surrounding e-commerce can present a conundrum to information professionals charged with securing the business transactions of their company. This session bridges the technical, the bureaucratic, and the social. Specifically, the session offers you an exploration of cryptographic basics, concentrating on the tools and methods necessary for privacy for business transactions and their
uses in electronic commerce. This is not a technical presentation to discuss technical characteristics of the schemes. The session is specifically aimed at the individual who cares less about the mathematics behind the techniques and more about what, why, and how of cryptographic tools for protecting digital information. The word “practical” is key. Using blocks, pens, boxes, rope, and real-world case studies, the instructor will explain what secret key, public, and hashing algorithms are and how they address security problems for electronic commerce and everyday situations. More importantly, you will learn when it is appropriate to use cryptography and when it is not. Examples from such fields as military, banking, Internet gambling, healthcare, and more will be featured.

Introduction to the National Certification and Accreditation Approach (The NIACAP)
Mark S. Loepker, National Security Agency
Barry Stauffer, Comptek Technologies, Inc.

The National Information Assurance Certification and Accreditation Process (NIACAP) establishes a national standard process, a set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the Information Assurance (IA) and security posture of an organization. The NIACAP focuses on the organization's mission and information system (IS) business case. In this workshop you will see that the process is designed to certify that the IS meets well-defined and agreed-to accreditation requirements and will continue to maintain the accredited security posture throughout the system life cycle. You will also see that the NIACAP is adaptable to any type of IS and any computing environment and mission. You will learn how the process can be adapted to include existing system certifications and evaluated products, and how users of the process must align the process with their program strategies and integrate the activities into their enterprise system life cycle. You will see that NIACAP maps to any system life-cycle process, its four phases are independent of the life-cycle strategy.

Introduction to the Common Criteria (CC), Common Evaluation Methodology (CEM), and Common Criteria Toolbox
Michael McEvilly, Mitretek Systems, Inc.
Gary Greiner, Mitretek Systems, Inc.
Frank Belkin, The MITRE Corporation

With the growing need for an internationally recognized and flexible criteria to specify security requirements and to replace the inflexible Trusted Computer Systems Evaluation Criteria (TCSEC), DoD 5200.28, the Common Criteria for Information Technology Security Evaluation, ISO/TEC Standard 15408 was developed by an International community. This workshop is designed for individuals just becoming familiar with the Common Criteria. Three separate sessions will be offered focusing on the Common Criteria, Common Evaluation Methodology, and Common Criteria Toolbox. Upon completion of the sessions, you will have a greater understanding of the IT U functional and nine assurance security requirements in the CC, how to assemble the requirements into protection profiles and security targets that comply with the normative, how to select functional and assurance requirements based on an objective, how the evaluation methodology is employed in the security testing process, and how the automated tools can be used to make the requirements specification process more efficient and expedient. You will learn how the CC offers consumers and producers of commercial-off-the-shelf (COTS) products a flexible and extensible approach for defining security requirements in IT products and systems. You will see that with the need for security enabled and enhanced information technology (IT) to support consumer needs and the critical infrastructure, the CC provides a framework for stipulating requirements and a comprehensive approach for testing IT products and systems using a Common Evaluation Methodology. Thus, the criteria provides an internationally recognized basis for specifying and testing a wide range of technologies such as operating systems, database management systems, PKI, firewalls, smart cards, telecommunications switches, networking devices, middleware, and applications. Using the Common Criteria can help:

- Convey consumer security requirements to IT product developers
- Determine if IT product developers produced what was specified
- Improve the ways consumers achieve assurance in IT products and systems

Slides booklet, CD of the CC, and the Toolbox will be available for each attendee.