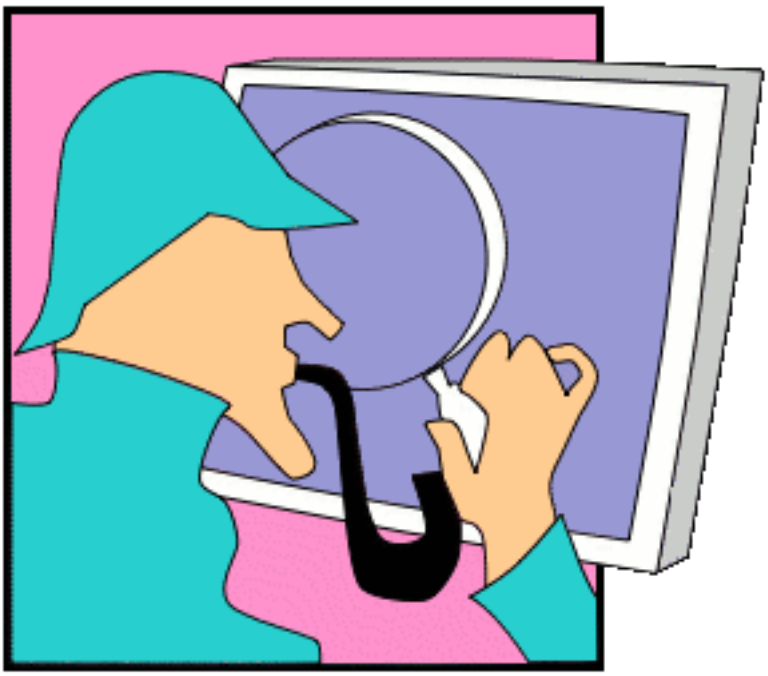
Program

Twenty-Second Annual Computer Security Applications Conference (ACSAC)

Practical Solutions To Real World Security Problems



December 11-15, 2006
Miami Beach Resort and Spa
Miami Beach, FL, USA

Presented by

ACSA
Applied Computer Security Associates

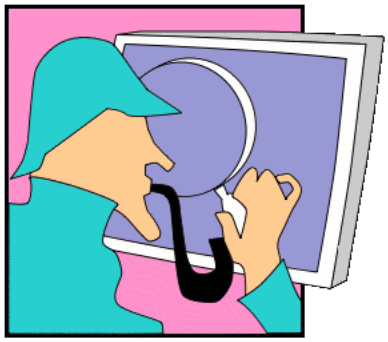
Conference Committee

Dan Thomsen, Cyber Defense Agency, LLC	Conference Chair
Christoph Schuba, Linköpings University	Program Chair
Rafae Bhatti, IBM Almaden Research Center	Site Arrangements Co-Chair
Laura Corriss, Barry University	Site Arrangements
Dan Faigin, The Aerospace Corporation	Tutorials Chair
Arthur Friedman, OASD(NII)/DoD CIO	Registration
Carrie Gates, CA Labs	Publicity
Tom Haigh, Cyber Defense Agency, LLC	Guest Speaker Liaison
Noel Hardy, Aspect Security	Recording Secretary
Tracy Hawkins, NSA	Registration
Paul Jardetzky, Network Applicances, Inc.	Panel Chair
Jay Kahn, The MITRE Corporation	Distribution Chair
Charles Payne, Adventium Labs	Program Co-Chair
Steven Rome, Booz Allen Hamilton, Inc.	Case Studies
Ron Ross, NIST	Case Studies
Harvey H. Rubinovitz, The MITRE Corporation	Workshop Chair
Pierangela Samarati, Università degli Studi di Milano	Program Co-Chair
Andre dos Santos, University of Puerto Rico at Mayagüez	Student Awards Chair
Ed Schneider, Institute for Defense Analysis	Treasurer
Linda Schliper, Trusted Computer Solutions	Mailing Lists
Cristina Serban, AT&T	Works in Progress Chair
Rick Smith, University of St. Thomas, Minnesota	Publicity
Robert H'obbes' Zakon, Zakon Group LLC	Web Advisor

Program Committee

Christoph Schuba, Linköpings University	PC Chair
Charles Payne, Adventium Labs	PC Co-Chair
Pierangela Samarati, Università degli Studi di Milano	PC Co-Chair
Tuomas Aura, Microsoft Research, UK	
Lujo Bauer, Carnegie Mellon University	
Terry Benzel, USC - ISI	
Konstantin Beznosov, University of British Columbia	
Rafae Bhatti, Florida International University	
Marc Dacier, Eurecom Institute	
Carrie Gates, CA Labs	
Dieter Gollmann, Hamburg University of Technology	
Wesley Higaki, Symantec Corporation	
Cynthia Irvine, Naval Postgraduate School	
Paul Jardetzky, Network Applicances, Inc.	
Jan Jürjens, TU München	
Myong Kang, Naval Research Laboratory	
James Kempf, DoCoMo Labs USA	
Angelos Keromytis, Columbia University	
Carl Landwehr, University of Maryland	
Peng Liu, Pennsylvania State University	
Javier Lopez, University of Malaga	
Bryan Lyles, Telcordia Technologies	
Patrick McDaniel, Pennsylvania State University	
John McDermott, Naval Research Laboratory	
Joon Park, Syracuse University	
Anoop Singhal, National Institute for Standards and Technology	
Andre Dos Santos, University of Puerto Rico at Mayagüez	
Giovanni Vigna, University of California Santa Barbara	
Simon Wiseman, QinetiQ	
Diego Zamboni, IBM Zürich Research Laboratory	

Welcome to the 22nd Annual Computer Security Applications Conference!



My job as conference chair has allowed me to work with an extremely talented group of people committed to bring you the best possible security conference. I sincerely wish to thank them for all their hard work over the course of the year.

The ACSAC team has constantly strived to improve the conference. This year we have added a new "behind the scenes" feature of an ACSAC steering committee. The goal of the steering committee is to look at the long-term direction the ACSAC conference needs to go in the changing computer security landscape. The steering committee is made up of past program and conference chairs and other individuals dedicated to the ACSAC mission of providing a solid venue to educate new security practitioners and a forum for discussion new security technology. The ACSAC conference emphasizes practical solutions to real world security problems. Since the real world keeps changing, ACSAC must keep changing as well. Many thanks to the steering committee for bringing their new ideas to ACSAC this year.

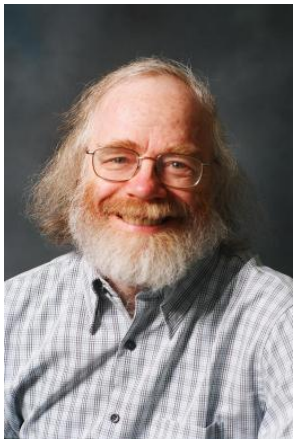
As conference chair, I would like to also thank you, the attendees, for choosing ACSAC as the venue to share your ideas and to learn. Never hesitate to send us your ideas and comments. This year we have an on-line survey at `http://www.acsac.org/survey`. Fill in the survey before January 3, 2007 and register for a chance to win an iPod Shuffle.

Enjoy the conference!

Dan Thomsen 2006 ACSAC Conference Chair

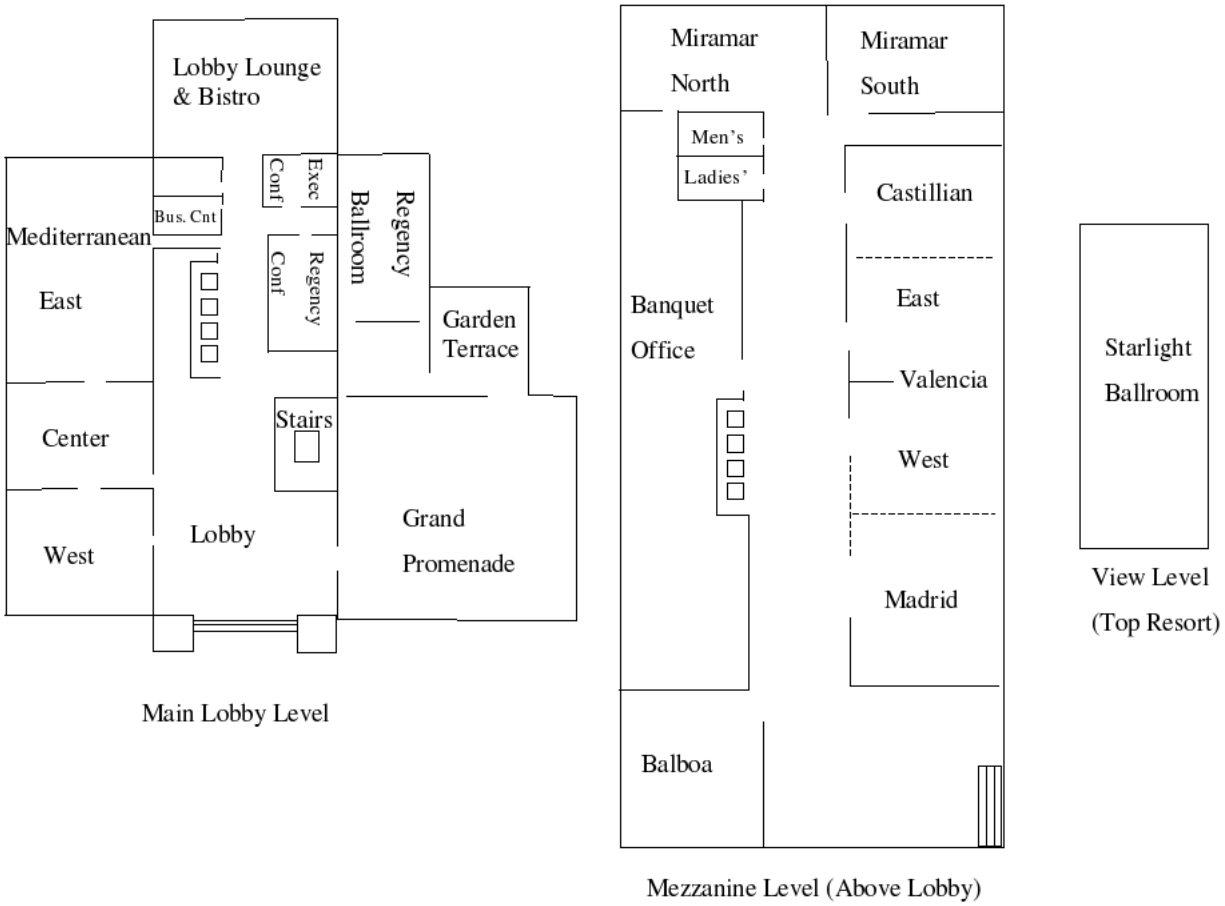
Highlights

- Welcome Reception for all attendees, Monday evening at 18:00. See page 11.
- Distinguished Practitioner **Dr. Dixie Baker**, SAIC, to speak on security and privacy in healthcare, Tuesday morning at 8:30. See page 12.
- **Dr. Steven Bellovin** to receive the *National Computer Systems Security Award* at a reception, Tuesday evening at 18:00. See page 20.
- **Best Paper Award** and **Best Student Paper Award** to be presented at the Tuesday evening reception.
- Invited Essayist **Mr. Brian Witten**, Symantec Corporation, to speak on security engineering, Wednesday morning at 8:30. See page 21.
- Classic Papers revisited by **Mr. Jeremy Epstein**, webMethods Inc., and **Dr. Peter G. Neumann**, SRI International, Thursday morning at 8:30. See page 30.



Dr. Steven M. Bellovin
NCSS Award Recipient

Meeting Locations All meeting locations are indicated in parentheses throughout the program. For the technical tracks on Tuesday through Thursday, the Mediterranean East room, which is the largest room, will host Track 2 and our Combined/Plenary sessions, while the Mediterranean Center room will host Track 1 and the Mediterranean West room will host Track 3. Breakfasts, lunches and breaks will be served in the Regency Ballroom.



Registration and Information Desk Hours On Sunday, the Desk will be open from 18:00 until 20:00. On Monday, the Desk will be open from 7:30 until 11:30, from 13:00 until 16:30, and then from 18:00 until 20:00. On Tuesday, Wednesday and Thursday, the Desk will open from 7:30 until 11:30, and then from 13:00 until 17:00. On Friday, the Desk will open from 7:30 until 10:30. The Desk also serves as the conference "Lost and Found Center" and is the location of the conference message board.

Session Etiquette Please be courteous of others around you during the Tutorial and Conference sessions. Try to enter and exit the session quietly. Please mute any beepers, cellular telephones, or similar devices, and please follow the directions of the session chair for asking questions. Thank you for your cooperation!

Invited Speakers

Distinguished Practitioner

Dr. Dixie B. Baker is a Technical Fellow and Vice President for Technology at Science Applications International Corporation (SAIC), where she serves as the Chief Technology Officer (CTO) for the Enterprise and Infrastructure Solutions Group (E&ISG). With a total staff of over 12,000 people, E&ISG leads SAIC's business in homeland security, health and life sciences, energy, environment, and enterprise solutions. As CTO, Dr. Baker serves as the Group's principal visionary and spokesperson on science and technology issues, develops partnerships and strategic alliances with technology suppliers, oversees research and development investments, and represents SAIC in national and international forums. In addition, Dr. Baker serves as a senior consultant on projects of strategic importance to the Group and to SAIC.

An internationally recognized thought leader in high-assurance architecture and information protection, Dr. Baker has applied her expertise primarily to the health and life sciences for the past ten years. She was the Principal Investigator for the Patient Centered Access to Secure Systems Online (PCASSO) project, a National Library of Medicine sponsored research project that is widely regarded as ground-breaking in providing patients safe and secure Web access to their complete medical records. Her research team's paper won the ACSAC's 1997 Best Paper Award. She has provided testimony to the National Committee on Vital and Health Statistics (NCVHS) as input to the development of the Health Insurance Portability and Accountability Act (HIPAA) security standards, and more recently, as guidance toward technology solutions for protecting the confidentiality of health records released to third parties. For the Centers for Disease Control and Prevention (CDC), she defined, and now is helping implement, an architecture that will enable the production, management, distribution, and use of semantically interoperable data-collection instruments for disease surveillance across the U.S.

Dr. Baker has published and lectured extensively in a number of technology and health-related areas, including information protection, high-assurance architecture, electronic medical records, and Internet safety. In 2001, she was awarded the John P. McGovern Lectureship in Information and Communications, presented by the Medical Library Association. In September 2004, at the invitation of the Ministry of Health of the Peoples Republic of China, she presented a keynote address and paper at the IDEAS04DH Workshop on Medical Information Systems, held in Beijing. Dr. Baker holds a Ph.D. in Education Research Methodologies and an M.S. in Computer Science from the University of Southern California, as well as M.S. and B.S. degrees from Florida State University and The Ohio State University respectively.

Dr. Baker will speak on the topic, *Privacy and Security in Public Health: Maintaining the Delicate Balance between Personal Privacy and Population Safety* during the opening session on Tuesday morning.

Invited Essayist

As Director of Government Research, **Mr. Brian Witten** leads all federally sponsored research and development within Symantec. Symantec Government Research is charged with the responsibility of developing technology for future Symantec products and services emerging from federally sponsored research solving nationally critical problems. Symantec pursues much of this research in partnership with world renowned universities. An experienced information security expert, Mr. Witten has also worked closely with both established industry leaders and early stage venture backed companies founded on disruptive technology.

Prior to joining Symantec, Mr. Witten worked at the Defense Advanced Research Projects Agency (DARPA), the U.S. military's central research and development organization charged with sponsoring revolutionary, high-payoff research to maintain the technological superiority of the U.S. military. While at DARPA, he focused on creation of new network security technologies to protect current and future information systems supporting "Network Centric Warfare." At DARPA, Mr. Witten managed an R&D investment portfolio of

more than $150 million in U.S. and international efforts.

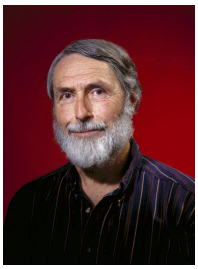
Mr. Witten began his technology career as an officer in the U.S. Air Force where he first began collaborating with leading academic institutions and commercial firms in information security research while assigned to Rome Laboratories and Air Force Research Labs (AFRL). Mr. Witten received his B.S. in Electrical and Computer Engineering from the University of Colorado.

Mr. Witten will speak on the topic, *Engineering Sufficiently Secure Computing*, during the opening session on Wednesday morning.

Classic Papers

Mr. Jeremy Epstein has been involved in information security for nearly 20 years, and is a well known researcher in the area. He is currently Senior Director of Product Security at webMethods, where he's responsible for analyzing and improving the security of all products, designing security for new products, assessing third party security products, and complying with security standards. He's also Lead Analyst with Cyber Defense Agency LLC where he leads several DARPA efforts. Prior to joining webMethods and CDA, he led a security research group at Network Associates, and was responsible for the C2 security evaluation of Novell NetWare. The research described in this classic paper was performed when he led a research group at TRW, Inc in the late 1980s and early 1990s. He has published over 20 papers in refereed research conferences including USENIX, IEEE, and ACSAC, as well as several articles in trade magazines. In his spare time, he works to improve security of electronic voting systems as a member of the Virginia legislature's committee on voting equipment recommendations. Mr. Epstein holds a BS in Computer Science from New Mexico Tech, an MS in Computer Sciences from Purdue University, and an ABD from George Mason University.

Mr. Epstein will speak on the topic, *Fifteen Years after TX: A Look Back at High Assurance Multi-Level Secure Windowing*, during the opening session on Thursday morning.



Dr. Peter G. Neumann has doctorates from Harvard and Darmstadt. After 10 years at Bell Labs in Murray Hill, New Jersey, in the 1960s, during which he was heavily involved in the Multics development jointly with MIT and Honeywell, he has been in SRI's Computer Science Lab since September 1971. He is concerned with computer systems and networks, trustworthiness/dependability, high assurance, security, reliability, survivability, safety, and many risks-related issues such as voting-system integrity, crypto policy, social implications, and human needs including privacy. He moderates the ACM Risks Forum, edits CACM's monthly Inside Risks column, chairs the ACM Committee on Computers and Public Policy, and chairs the National Committee for Voting Integrity (http://www.votingintegrity.org).

He created ACM SIGSOFT's Software Engineering Notes in 1976, and was its editor for 19 years and still contributes the RISKS section. He has participated in four studies for the National Academies of Science: Multilevel Data Management Security (1982), Computers at Risks (1991), Cryptography's Role in Security the Information Society (1996), and Improving Cybersecurity for the 21st Century: Rationalizing the Agenda (2006). His 1995 book, Computer-Related Risks, is still timely!

He is a Fellow of the ACM, IEEE, and AAAS, and is also an SRI Fellow. He received the National Computer System Security Award in 2002 and the ACM SIGSAC Outstanding Contributions Award in 2005. He is a member of the U.S. Government Accountability Office Executive Council on Information Management and Technology, and the California Office of Privacy Protection advisory council. He co-founded People For Internet Responsibility (PFIR, http://www.PFIR.org). He has taught courses at Darmstadt, Stanford, U.C. Berkeley, and the University of Maryland. See his website (http://www.csl.sri.com/neumann) for Senate and House testimonies, papers, bibliography, further background, etc.

Dr. Neumann will speak on the topic, *Risks of Untrustworthiness*, during the opening session on Thursday morning.

Tutorial Faculty

Dr. Frank Adelstein and **Professor Golden G. Richard III** are the vice-chair and chair, respectively, of the Digital Forensic Research Workshop, the premier workshop on research advances in the area of digital forensics. They have co-authored the book *Fundamentals of Mobile and Pervasive Computing* (from McGraw-Hill). Dr. Adelstein is the technical director of computer security at ATC-NY in Ithaca, NY. He is the principal designer of a live forensic investigation product (marketed as Online Digital Forensic Suite^{TM} and LiveWire Investigator^{TM}) and has worked in the area of live investigation for the last 5 years. He has also been the principal investigator on numerous research and development projects including security, wireless networking, intrusion detection, and training. Prof. Richard is an Associate Professor at the University of New Orleans, where he developed the Information Assurance curriculum and coordinated the effort to have the University of New Orleans certified by the National Science Foundation as a Center of Academic Excellence. He teaches courses in digital forensics, computer security, and operating systems internals. He is also a co-founder of Digital Forensic Solutions, LLC and is the author of the digital forensics tool "Scalpel."

Dr. Adelstein and Prof. Richard will co-present the full-day tutorial, *Live Forensics*, on Monday.

Dr. Thomas M. Chen is an associate professor in the Department of Electrical Engineering at Southern Methodist University in Dallas, Texas. He received the BS and MS degrees in electrical engineering from the Massachusetts Institute of Technology in 1984, and the PhD in electrical engineering from the University of California, Berkeley, in 1990. He is currently the editor-in-chief of IEEE Communications Magazine, a senior technical editor for IEEE Network, a past associate editor for ACM Transactions on Internet Technology, and past founding editor of IEEE Communications Surveys. He served as the treasurer for the IEEE Technical Committee on Security and Privacy 2004-2005. He is a member of the Technical Advisory Board for the Voice over IP Security Alliance. Prior to joining SMU, he was a senior member of the technical staff at GTE Laboratories (now Verizon) working on ATM research. He is the co-author of ATM Switching Systems (Artech House, 1995). He was the recipient of the IEEE Communications Societys Fred W. Ellersick best paper award in 1996. His research interests include network security, traffic modeling, network performance, and network management.

Dr. Chen will present the half-day tutorial, *Defenses Against Viruses, Worms, and Malicious Software*, on Monday afternoon.

Dr. Steven J. Greenwald is an Independent Consultant in the field of Information Systems Security specializing in distributed security, formal methods, security policy modeling, and related areas. He also works with organizational security policy consulting, evaluation, training, and auditing. Dr. Greenwald is also a Research Fellow of Virginia's Commonwealth Information Security Center (CISC) and an adjunct professor at James Madison University (an NSA Designated Center of Academic Excellence in Information Security Assurance) where he teaches several graduate courses for their M.S. degree in Computer Science concentrating in INFOSEC. Dr. Greenwald served as the 2001 General Chair of the New Security Paradigms Workshop (NSPW), has been past Program Chair for NSPW, and also serves on the program committees of other conferences. He is a member of the Association for Computing Machinery and the IEEE Computer Society. More information about him, including his publications, can be found at his web site at `http://www.gate.net/~sjg6`.

Dr. Greenwald will present the full-day tutorial, *Security Engineering*, on Monday.

Dr. Jan Jürjens is a Senior Lecturer (equiv. US Assoc. Prof.) at the Open University (the British long-distance university in Milton Keynes near London). He is the author of a book on Secure Systems Development with UML (Springer 2004) and an introductory book on IT-Security (Springer 2006) and about 50 papers and 10 invited talks in refereed international books, journals, and conferences, mostly on computer security and software engineering. He has created and lectured courses on secure systems development at the University of Oxford, the Technical University of Munich, Carlos III Univ. Madrid, and the University of Innsbruck, as well as over 30 tutorials on secure software engineering at international conferences. He is the initiator and current chair of the working group on Formal Methods and Software Engineering for Safety and Security (FoMSESS) within the German Society for Informatics (GI). He is a member of the executive

board of the Division of Safety and Security (Fachbereich Sicherheit) within the GI, the executive boad of the committee on Modeling (QFA Modellierung) of the GI, the advisory board of the Bavarian Competence Center for Safety and Security (KoSiB), the working group on e-Security of the Bavarian regional government, the IFIP Working Group 1.7 "Theoretical Foundations of Security Analysis and Design", and the IFIP Working Group on Critical Infrastructure Protection which is currently being founded. He has been leading various security-related projects with industry. Jan Jürjens studied Mathematics and Computer Science at the Univ. of Bremen (Germany) and the Univ. of Cambridge (GB). He has done research towards a PhD at the Univ. of Edinburgh (GB), Bell Laboratories (Palo Alto, USA), and the Univ. of Oxford (GB), received a DPhil (Doctor of Philosophy) in Computing from the Univ. of Oxford. Before joining the faculty at the Open University, he directed the Competence Center for IT-Security at the group on Software & Systems Engineering at the Technical University of Munich.

Dr. Jürjens will present the half-day tutorial, *Biometric Authentication Systems: Pitfalls and How to Avoid Them*, on Monday morning.

Dr. John McHugh holds the Canada Research Chair in Privacy and Security at Dalhousie University in Halifax, NS where he leads the Privacy and Security Laboratory. Prior to joining Dalhousie, he was a senior member of the technical staff with the CERT Situational Awareness Team, where he did research in survivability, network security, and intrusion detection. Recently, he has been involved in the analysis of large scale network flow data. He was a professor and former chairman of the Computer Science Department at Portland State University in Portland, Oregon. His research interests include computer security, software engineering, and programming languages. He has previously taught at The University of North Carolina and at Duke University. He was the architect of the Gypsy code optimizer and the Gypsy Covert Channel Analysis tool. Dr. McHugh received his PhD degree in computer science from the University of Texas at Austin. He has a MS degree in computer science from the University of Maryland, and a BS degree in physics from Duke University.

Dr. McHugh will present the full-day tutorial, *Acquisition and Analysis of Large Scale Network Data V.3*, on Friday.

Dr. Ron Ross is a senior computer scientist and information security researcher at the National Institute of Standards and Technology (NIST). His areas of specialization include security requirements definition, security testing and evaluation, and information assurance. Dr. Ross currently leads the Federal Information Security Management Act (FISMA) Implementation Project for NIST, which includes the development of key security standards and guidelines for the federal government, contractors supporting the federal government, and the critical information infrastructure. His recent publications include Federal Information Processing Standards (FIPS) Publication 199 (the security categorization standard), FIPS Publication 200 (the minimum security requirements standard), NIST Special Publication 800-53 (the security controls guideline), NIST Special Publication 800-53A (the security assessment guideline), and NIST Special Publication 800-37 (the system certification and accreditation guideline). Dr. Ross is also the principal architect of the risk management framework and nine-step process that integrates the suite of NIST security standards and guidelines into a comprehensive enterprise-wide information security program. Dr. Ross is a frequent speaker at public and private sector venues including federal agencies, state and local governments, and Fortune 500 companies. In addition to his responsibilities at NIST, Dr. Ross supports the U.S. State Department in the international outreach program for information security and critical infrastructure protection. Dr. Ross previously served as the Director of the National Information Assurance Partnership, a joint activity of NIST and the National Security Agency. A graduate of the United States Military Academy at West Point, Dr. Ross served in a variety of leadership and technical positions during his twenty-year career in the United States Army. While assigned to the National Security Agency, he received the Scientific Achievement Award for his work on an inter-agency national security project and was awarded the Defense Superior Service Medal upon his departure from the agency. Dr. Ross is a two-time recipient of the Federal 100 award for his leadership and technical contributions to critical information security projects affecting the federal government. During his military career, Dr. Ross served as a White House aide and as a senior technical advisor to the Department of the Army. Dr. Ross is a graduate of the Program Management School at the Defense Systems Management College and holds both Masters and Ph.D. degrees in Computer Science from the

United States Naval Postgraduate School.

Dr. Ross will present the full-day tutorial, *Using the Certification and Accreditation Process to Manage Enterprise Risk*, on Friday.

Mr. Richard Rushing is a recognized IT security expert with 20 years experience as a system analyst, engineer, consultant and architect. Richard has set security standards and policies for entire organizations and taught workshops on IDS, Security Protocols, and Network Security. Richard was most recently Chief Technical Officer of VeriSign's Network Security Services division where he identified and developed products and services to maintain VeriSign's focus on leading-edge security solutions. A much-in-demand speaker on information security, Richard has presented at leading security conferences, including Networld+Interop, RSA, Computer Security Institute, SANS Security Conferences, InfoSec and CyberTerrorism.

Mr. Rushing will present the full-day tutorial, *Next Generation Wireless Risks and Defenses*, on Friday.

Monday, December 11, 2006

Workshop *Host Based Security Assessment: Standards to Implementations*
Moderator: Dr. Harvey Rubinovitz, The MITRE Corporation
Time: 8:30 - 17:00 (Miramar South)

This workshop will focus on the security assessments, including how they may be defined in standards by either government agencies or by commercial organizations, how technology is being implemented and utilized to perform the assessments, and how on-going enforcement is accomplished. The workshop will also examine the need to facilitate the research and development of the next generation of standards and implementations to assist in the creation of more secure configurations. Pre-registration is required as there is registration fee to cover the cost of the workshop and lunch and snack.

Tutorial M1 *Building Biometric Authentication Systems: Pitfalls and How to Avoid Them*
Speaker: Dr. Jan Jürjens, The Open University
Time: 8:30 - 12:00 (Castilian)

Based on practical experiences from related industrial R&D projects, the tutorial gives a hands-on introduction into how to correctly build biometric authentication systems and how to securely embed them into the system context. The tutorial will report on experiences and lessons learnt, and on common pitfalls in designing such systems. Tutorial participants will gain up-to-date knowledge on the state of the art in biometric authentication and on how to use this technology securely. A textbook on secure systems development used during the tutorial is distributed to each participant.

Tutorial M2 *Defenses Against Viruses, Worms, and Malicious Software*
Speaker: Dr. Tom Chen, Southern Methodist University
Time: 8:30 - 12:00 (Castilian)

This tutorial will give an overview of computer viruses, worms, and Trojan horses. The tutorial is organized into three major parts. The first part introduces the audience to the self-replicating mechanisms of viruses and worms, and describes how malicious software programs function. The possible effects on hosts and networks is described with real-life examples.

The second part of the tutorial gives an overview of current host-based and network-based defenses. Hosts are protected by antivirus software and operating system patching. Network-based defenses consist of various network equipment such as firewalls, intrusion detection systems, server proxies, and routers. In addition to explaining each type of defense, the limitations of each defense are pointed out. The limitations are important to understanding why malware outbreaks continue to be a major problem today and into the foreseeable future.

The third part of the tutorial gives an overview of some current research areas in improving defenses. The automation of defenses will be critical in the face of new worms that can be much faster than todays manual, reactive defenses. Automated defenses will first depend on accurate detection of new outbreaks. New outbreaks must be detected before a virus/worm signature is available, so new behavior-based detection methods must be used. Unfortunately, behavior-based detection can result in a high number of false positives, so current research is seeking to improve the accuracy of behavior-based detection. After detection of a new outbreak, automated defenses will exercise some action to quarantine the worm. Examples proposed by Cisco and Microsoft will be described. Also, the use of tarpits and rate throttling to slow down outbreaks will be explained.

Tutorial M3 *Live Forensics*
Speakers: Dr. Frank Adelstein, ATC-NY and Dr. Golden Richard, University of New Orleans
Time: 8:30 - 17:00 (Madrid)

This tutorial covers the area of live forensics, including the types of information that can be gathered, how the evidence can be analyzed, and how it can work in conjunction with traditional methods, as well as satisfy forensic requirements. We will briefly review static disk analysis techniques, briefly cover network packet analysis, and then discuss gathering information on a live machine. The tutorial includes demonstrations. At the end, the students should understand what live state information is available on a computer, some of the different methods to gather the information, and the best practices that should be observed when performing a live analysis.

Tutorial M4 *Security Engineering*
Speaker: Dr. Steven J. Greenwald, Independent Consultant
Time: 8:30 - 17:00 (Balboa)

Based on Ross Anderson's carefully researched and eminently practical book *Security Engineering: A Guide to Building Dependable Distributed Systems*, this tutorial will cover how to make distributed systems more secure with the help of both technological mechanisms and management strategies. It will cover the entire field of computer security, although it is, of course, severely limited by the one-day format.

Real-world examples of how information systems have been defeated will be covered, as well as the uses of technology, policy, psychology, and legal issues.. Practical examples such as the security of ATM machines, multi-level security, information warfare, hardware security, e-commerce, intellectual property protection, biometrics, and tamper resistance will be covered. Each section will examine what goes wrong.

□ □ □

Welcome Reception

Please join us from 18:00 until 21:00 in the Regency Ballroom for hors d'oeuvres and drinks and an opportunity to meet others in the security community. This is also a good opportunity for session chairs to meet their speakers!

Tuesday, December 12, 2006

7:30 **Continental Breakfast (Regency Ballroom) sponsored by** 

8:30 **Introductory remarks (Mediterranean East)**
Dan Thomsen, Cyber Defense Agency, LLC, Conference Chair
Christoph Schuba, Linköpings University, Program Chair

Introduction of the Distinguished Practitioner
Marshall Abrams, The MITRE Corporation

Distinguished Practitioner
Privacy and Security in Public Health: Maintaining the Delicate Balance between Personal Privacy and Population Safety
Dr. Dixie Baker, SAIC

> Amidst threats of pandemic avian influenza and bioterrorist attack, public health surveillance and preparedness have never been more important. Early detection of biological events, electronic reporting of laboratory test results, efficient exchange of case reports across jurisdictions, and timely alerting of health threats are critical components of effective health protection. Essential to public health surveillance and preparedness is the timely availability of information relating to individuals' healthcare behaviors and clinical conditions — posing a threat to personal privacy. Public health is challenged to maintain an optimal balance between protecting the nation's health and respecting the personal privacy of its citizens.

10:00 **Break (Regency Ballroom)**

10:30 **Track 1 (Mediterranean Center): Applied Distributed Collaboration**
Track 1 Chair: Christoph Schuba, Linköpings University

Shamon: A System for Distributed Mandatory Access Control ◇
Jonathan McCune, Carnegie Mellon University
Stefan Berger, IBM
Ramon Caceres, IBM
Trent Jaeger, Pennsylvania State University
Reiner Sailer, IBM

> We define and demonstrate an approach to securing distributed computation based on a shared reference monitor (Shamon) that enforces mandatory access control (MAC) policies across a distributed set of machines. The Shamon enables local reference monitor guarantees to be attained for a set of reference monitors on these machines. We implement a prototype system on the Xen hypervisor with a trusted MAC virtual machine built on Linux 2.6 whose reference monitor design requires only 13 authorization checks, only 5 of which apply to normal processing (others are for policy setup). We show that, through our architecture, distributed computations can be protected and controlled coherently across all the machines involved in the computation.

A Framework for Collaborative DDoS Defense ◇
George Oikonomou, University of Delaware
Jelena Mirkovic, University of Delaware
Peter Reiher, University of California, Los Angeles
Max Robinson, The Aerospace Corporation

> Increasing use of the Internet for critical services makes flooding distributed denial-of-service (DDoS) a top security threat. A distributed nature of DDoS suggests that a distributed

mechanism is necessary for a successful defense. Three main DDoS defense functionalities attack detection, rate limiting and traffic differentiation are most effective when performed at the victim-end, core and source-end respectively. Many existing systems are successful in one aspect of defense, but none offers a comprehensive solution and none has seen a wide deployment. We propose to harvest the strengths of existing defenses by organizing them into a collaborative overlay, called DefCOM, and augmenting them with communication and collaboration functionalities. Nodes collaborate during the attack to spread alerts and protect legitimate traffic, while rate limiting the attack. DefCOM can accommodate existing defenses, provide synergistic response to attacks and naturally lead to an Internet-wide response to DDoS threat.

V-COPS: A Distributed Vulnerability-based Cooperative Alert System ◇
Shiping Chen, George Mason University
Dongyu Liu, George Mason University
Songqing Chen, George Mason University
Sushil Jajodia, George Mason University

The efficiency of promptly releasing security alerts of established analysis centers has been greatly challenged by the continuous emergence of various large scale network attacks, such as worms. With a limited number of sensors deployed over the Internet and a long attack verification period, when the alert is released by analysis centers, the best time to stop the attack may have passed. On the other hand, (1) most of the past large scale attacks targeted known vulnerabilities, and (2) today numerous Internet systems have integrated detection tools, such as virus detection software and intrusion detection systems (IDS), the power of which could be harnessed to defend against large scale attacks. In this paper, we propose V-COPS a vulnerability-based cooperative alert distribution system, by leveraging existing independent local attack detection systems. VCOPS is capable of promptly propagating genuine alerts with critical vulnerability information, based on which relevant stakeholders can take preventive actions in time. Extensive analysis and experiments have been performed to study the performance of V-COPS. The preliminary results show V-COPS is effective.

Track 2 (Mediterranean East): Client Access in Untrusted Environment 10:30
Chair: Jay Kahn, The MITRE Corporation Track 2

Delegate: A Proxy Based Architecture for Secure Website Access from an Untrusted Machine ◇
Ravi Chandra Jammalamadaka, University of California, Irvine
Timothy W.van der Horst, Brigham Young University
Sharad Mehrotra, University of California, Irvine
Kent E. Seamons, Brigham Young University
Nalini Venkatasubramanian, University of California, Irvine

Performing sensitive online transactions using computers found in cybercafes and public libraries is risky. The untrusted nature of these machines creates a target rich environment. A simple keystroke logger, a common payload of many viruses, records and transmits the secret information (e.g., passwords, credit card numbers, PIN numbers) entered into these machines. In addition, sophisticated malware can hijack a users authenticated session to perform unauthorized transactions masquerading as the user. This paper presents Delegate, a proxy-based architecture that enables a user to access web sites without disclosing personal information to untrusted machines. Delegate enforces rules at the proxy to detect and prevent session hijacking. This architecture leverages users trusted mobile devices, e.g., cell phones, and requires no modification to web servers or the untrusted machines. Delegate is designed to provide a balance between security and usability.

KLASSP: Entering Passwords on a Spyware Infected Machine Using a Shared-Secret Proxy ◇
Dinei Florencio, Microsoft
Cormac Herley, Microsoft

In this paper we examine the problem of entering sensitive data, such as passwords, from an untrusted machine. By untrusted we mean that it is suspected to be infected with spyware which snoops on the users activity. Using such a machine is obviously undesirable, and yet roaming users often have no choice. They are in no position to judge the security status of internet cafe, airport lounge or business center machines. Either malice or negligence on the part of an administrator means that any such machine can easily be running a keylogger. The roaming user has no reliable way of determining whether it is safe, and has no alternative to typing the password. We consider whether it is possible to enter data to confound spyware assumed to be running on the machine in question. The difficulty of mounting a collusion attack on a single users password makes the problem more tractable than it might appear. We explore several approaches. In the first, we show how the user can embed a password in random keystrokes to confuse spyware, while leaving the actual login unaffected. In the second we employ a proxy server to strip random keys. In the third we again employ a proxy that inverts a key mapping performed by the user. We examine also several potential attacks.

Vulnerability Analysis of MMS User Agents ◇
Collin Mulliner, University of California, Santa Barbara
Giovanni Vigna, University of California, Santa Barbara

The Multimedia Messaging Service (MMS) is becoming more popular, as mobile phones integrate audio and video recording functionality. Multimedia messages are delivered to users through a multi-step process, whose end-points are the MMS User Agents that reside on the users mobile phones. The security of these components is critical, because they might have access to private information and, if compromised, could be leveraged to spread an MMS-based worm. Unfortunately, the vulnerability analysis of these components is made more difficult by the fact that they are mostly closed-source and the testing has to be performed through the mobile phone network, which makes the testing time-consuming and costly. This paper presents a novel approach to the security testing of MMS User Agents. Our approach takes into account the effects of the infrastructure on the delivery of MMS messages and then uses a virtual infrastructure to speed up the testing process. Our testing approach was able to identify a number of previously unknown vulnerabilities, which, in one case, allowed for the execution of arbitrary code.

10:30 **Track 3 (Mediterranean West): Vulnerability Management**
Track 3

Using the National Vulnerability Database in Enterprise Information Security Programs
Peter Mell, NIST
Tony Sager, NSA

Understanding the critical vulnerabilities in enterprise information systems and how to take effective actions to eliminate those vulnerabilities and mitigate risks to important organizational missions is a top priority for both public and private sector organizations today. The National Institute of Standards and Technology in collaboration with the Department of Homeland Securitys National Cyber Security Division and US CERT has initiated a comprehensive project to develop a broad-based database of key vulnerabilities in information systems. The National Vulnerability Database (NVD) is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. The NVD is based on and synchronized with the Common Vulnerabilities and Exposures (CVE) vulnerability naming standard. Linking the vulnerability database to standardized security controls (i.e., safeguards and countermeasures) necessary to protect information systems and recommended configuration settings for commercial products that are employed within those systems in a new and innovative part of the NVD effort that promises to have a significant effect on the overall, security of both public and private sector enterprises. This session covers the latest activities in

the NVD, the expansion into the configuration settings area, and the application of automated tools and standardized specification languages to bring greater efficiencies to the process.

Lunch (Regency Ballroom) sponsored by  12:00

Track 1 (Mediterranean Center): Network Intrusion Detection 13:30
Chair: Giovanni Vigna, University of California, Santa Barbara Track 1

Backtracking Algorithmic Complexity Attacks Against a NIDS ◇
Randy Smith, University of Wisconsin, Madison
Cristian Estan, University of Wisconsin, Madison
Somesh Jha, University of Wisconsin, Madison

Network Intrusion Detection Systems (NIDS) have become crucial to securing modern networks. To be effective, a NIDS must be able to counter evasion attempts and operate at or near wire-speed. Failure to do so allows malicious packets to slip through a NIDS undetected. In this paper, we explore NIDS evasion through algorithmic complexity attacks. We present a highly effective attack against the Snort NIDS, and we provide a practical algorithmic solution that successfully thwarts the attack. This attack exploits the behavior of rule matching, yielding inspection times that are up to 1.5 million times slower than that of benign packets. Our analysis shows that this attack is applicable to many rules in Snorts ruleset, rendering vulnerable the thousands of networks protected by it. Our countermeasure confines the inspection time to within one order of magnitude of benign packets. Experimental results using a live system show that an attacker needs only 4.0 kbps of bandwidth to perpetually disable an unmodified NIDS, whereas all intrusions are detected when our countermeasure is used.

NetSpy: Automatic Generation of Spyware Signatures for NIDS ◇
Hao Wang, University of Wisconsin, Madison
Somesh Jha, University of Wisconsin, Madison
Vinod Ganapathy, University of Wisconsin, Madison

We present NetSpy, a tool to automatically generate network-level signatures for spyware. NetSpy determines whether an untrusted program is spyware by correlating user input with network traffic generated by the untrusted program. If classified as spyware, NetSpy also generates a signature characterizing the malicious substrate of the spywares network behavior. Such a signature can be used by network intrusion detection systems to detect spyware installations in large networks. In our experiments, NetSpy precisely identified each of the 7 spyware programs that we considered and generated network-level signatures for them. Of the 9 supposedly benign programs that we considered, NetSpy correctly characterized 6 of them as benign. The remaining 3 programs showed network behavior that was highly suggestive of spying activity.

Detecting Policy Violations through Traffic Analysis ◇
Jeffrey Horton, University of Wollongong
Rei Safavi-Naini, University of Wollongong

Restrictions are commonly placed on the permitted uses of network protocols in the interests of security. These restrictions can sometimes be difficult to enforce. As an example, a permitted protocol can be used as a carrier for another protocol not otherwise permitted. However, if the observable behaviour of the protocol exhibits differences between permitted and non-permitted uses, it is possible to detect inappropriate use. We consider SSH, the Secure Shell protocol. This is an encrypted protocol with several uses. We attempt firstly to classify SSH sessions according to some different types of traffic for which the sessions have been used, and secondly, given a policy that permits SSH use for interactive traffic, to identify when a session appears to have been used for some other purpose.

13:30 **Track 2 (Mediterranean East): Panel**
Track 2

Challenges for Web Services Security
Anoop Singhal, Ph.D., NIST (Panel Chair)
Mike McIntosh, IBM Research, Yorktown Heights
Prof. Carl Gunter, Department of Computer Science, Univ. of Illinois
Jeremy Epstein, webMethods Inc.
Rafae Bhatti, CERIAS, Purdue University
Karen Goertzel, Manager Software Security, Booz Allen Hamilton, Inc.
Thomas Ray, Director of Security Services, Washington Mutual Card Services

The advance of Web services technologies promises to have far-reaching effects on the Internet and enterprise networks. Web services based on the eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), and related open standards, and deployed in Service Oriented Architectures (SOA) allow data and applications to interact without human intervention through dynamic and ad hoc connections. Web services technology can be implemented in a wide variety of architectures, can co-exist with other technologies and software design approaches, and can be adopted in an evolutionary manner without requiring major transformations to legacy applications and databases. The security challenges presented by the Web services approach are formidable and unavoidable. Many of the features that make Web services attractive, including greater accessibility of data, dynamic application-to-application connections, and relative autonomy (lack of human intervention) are at odds with traditional security models and controls. Difficult issues and unsolved problems exist, such as the following:

- Confidentiality and integrity of data transmitted via Web services protocols in service-to-service transactions, including data that transits intermediary (pass-through) services.
- Functional integrity of the Web services themselves, requiring both establishment in advance of the trustworthiness of services to be included in service orchestrations or choreographies, and the establishment of trust between services on a by-transaction basis.
- Availability in the face of denial of service attacks that exploit vulnerabilities unique to Web service technologies, especially targeting core services, such as discovery service, on which other services rely.

13:30 **Track 3 (Mediterranean West): Personal Identification Verification**
Track 3

FIPS 201: The Standard and Its Effect on the Public and Private Sectors
Bill MacGregor, NIST
Invited Speaker, GSA
Invited Speaker, Bearing Point

In response to Homeland Security Presidential Directive #12, the National Institute of Standards and Technology initiated a new program for improving the identification and authentication of federal employees and contractors for access to federal facilities and information systems. Federal Information Processing Standard (FIPS) 201 was developed to satisfy the Personal Identity Verification (PIV) requirements of HSPD 12, approved by the Secretary of Commerce, and issued on February 25, 2005. In addition to the core PIV security standards, a number of guidelines, reference implementations, and conformance tests have been identified as being needed to: implement and use the PIV system; protect the personal privacy of all subscribers of the PIV system; authenticate identity source documents to obtain the correct legal name of the person applying for a PIV card; electronically obtain and store required biometric data (e.g., fingerprints, facial images) from the PIV system subscriber;

create a PIV card that is personalized with data needed by the PIV system to later grant access to the subscriber to Federal facilities and information systems; assure appropriate levels of security for all applicable Federal applications; and provide interoperability among Federal organizations using the standards. This session provides the latest implementation information from organizations managing the deployment of the PIV technologies.

Break (Regency Ballroom) 15:00

Track 1 (Mediterranean Center): Network Security 15:30
Chair: Cristina Serban, AT&T Track 1

Practical Attack Graph Generation for Network Defense ◇
Kyle Ingols, MIT Lincoln Laboratory
Richard Lippmann, MIT Lincoln Laboratory
Keith Piwowarski, MIT Lincoln Laboratory

Attack graphs are a valuable tool to network defenders, illustrating paths an attacker can use to gain access to a targeted network. Defenders can then focus their efforts on patching the vulnerabilities and configuration errors that allow the attackers the greatest amount of access. We have created a new type of attack graph, the multiple-prerequisite graph, that scales nearly linearly as the size of a typical network increases. We have built a prototype system using this graph type. The prototype uses readily available source data to automatically compute network reachability, classify vulnerabilities, build the graph, and recommend actions to improve network security. We have tested the prototype on an operational network with over 250 hosts, where it helped to discover a previously unknown configuration error. It has processed complex simulated networks with over 50,000 hosts in under four minutes.

Secure Distributed Cluster Formation in Wireless Sensor Networks ◇
Kun Sun, Intelligent Automation, Inc.
Pai Peng, Opsware Inc.
Peng Ning, North Carolina State University
Cliff Wang, Army Research Office

In wireless sensor networks, clustering sensor nodes into small groups is an effective technique to achieve scalability, self-organization, power saving, channel access, routing, etc. A number of cluster formation protocols have been proposed recently. However, most existing protocols assume benign environments, and are vulnerable to attacks from malicious nodes. In this paper, we propose a secure distributed cluster formation protocol to organize sensor networks into mutually disjoint cliques. Our protocol has the following properties: (1) normal nodes are divided into mutually disjoint cliques; (2) all the normal nodes in each clique agree on the same clique memberships; (3) while external attackers can be prevented from participating in the cluster formation process, inside attackers that do not follow the protocol semantics can be identified and removed from the network; (4) the communication overhead is moderate; (5) the protocol is fully distributed.

Specification-Based Intrusion Detection in WLANs ◇
Rupinder Gill, Queensland University of Technology
Jason Smith, Queensland University of Technology
Andrew Clark, Queensland University of Technology

Wireless networking technologies based on the IEEE 802.11 series of standards fail to authenticate management frames and network card addresses and suffer from serious vulnerabilities that may lead to denial of service, session hijacking, and address masquerading attacks. In this paper, we describe and implement a specification-based intrusion detection system for IEEE 802.11 wireless infrastructure networks, which not only provides attack detection, but also implements policy compliance monitoring. The specification used by our

intrusion detection system is derived from network protocol state transition models and site security policy constraints. We also perform an experimental and comparative analysis of the technique to assess its effectiveness. The results indicate that the approach is superior at successful ly detecting a greater variety of attacks than other existing approaches.

15:30 **Track 2 (Mediterranean East): Security in Systems**
Track 2 Chair: Lujo Bauer, Carnegie Mellon University

From Languages to Systems: Understanding Practical Application Development in Security-typed Languages ◇
Boniface Hicks, Pennsylvania State University
Kiyan Ahmadizadeh, Pennsylvania State University
Patrick McDaniel, Pennsylvania State University

Security-typed languages are an evolving tool for implementing systems with provable security guarantees. However, to date, these tools have only been used to build simple "toy" programs. As described in this paper, we have developed the first real-world, security-typed application: a secure email system written in the Java language variant Jif. Real-world policies are mapped onto the information flows controlled by the language primitives, and we consider the process and tractability of broadly enforcing security policy in commodity applications. We find that while the language provided the rudimentary tools to achieve low-level security goals, additional tools, services, and language extensions were necessary to formulate and enforce application policy. We detail the design and use of these tools. We also show how the strong guarantees of Jif in conjunction with our policy tools can be used to evaluate security. This work serves as a starting point — we have demonstrated that it is possible to implement real-world systems and policy using security-typed languages. However, further investigation of the developer tools and supporting policy infrastructure is necessary before they can fulfill their considerable promise of enabling more secure systems.

An Internet Voting System Supporting User Privacy ◇
Aggelos Kiayias, University of Connecticut
Michael Korman, University of Connecticut
David Walluck, University of Connecticut

This work introduces the ADDER system, an Internet-based, free and open source electronic voting system which employs strong cryptography. Our system is a fully functional e-voting platform and enjoys a number of security properties, such as robustness, trust distribution, ballot privacy, auditability and verifiability. It can readily implement and carry out various voting procedures in parallel and can be used for small scale boardroom/department-wide voting as well as largescale elections. In addition, ADDER employs a flexible voting scheme which allows the system to carry out procedures such as surveys or other data collection activities. ADDER offers a unique opportunity to study cryptographic voting protocols from a systems perspective and to explore the security and usability of electronic voting systems.

A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs ◇
Lillian Røstad, Norwegian University of Science and Technology
Ole Edsberg, Norwegian University of Science and Technology

In healthcare, role-based access control systems are often extended with exception mechanisms to ensure access to needed information even when the needs don't follow the expected patterns. Exception mechanisms increase the threats to patient privacy, and therefore their use should be limited and subject to auditing. We have studied access logs from a hospital EPR system with extensive use of exception-based access control. We found that the uses of the exception mechanisms were too frequent and widespread to be considered exceptions. The huge size of the log and the use of predefined or uninformative reasons for access make it infeasible to audit the log for misuse. The informative reasons that were given provided starting points for

requirements on how the usage needs should be accomplished without exceptionbased access. With more structured and fine-grained logging, analysis of access logs could be a very useful tool for learning how to reduce the need for exception-based access.

Track 3 (Mediterranean West): Case Studies 15:30
Chair: Ed Keefe, FBI Track 3

Challenges for Secure Web Services
Anoop Singhal, NIST

The advance of Web services technologies promises to have far-reaching effects on the Internet and enterprise networks. Web services based on the eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), and related open standards, and deployed in Service Oriented Architectures (SOA) allow data and applications to interact without human intervention through dynamic and ad hoc connections. Web services technology can be implemented in a wide variety of architectures, can co-exist with other technologies and software design approaches, and can be adopted in an evolutionary manner without requiring major transformations to legacy applications and databases. The security challenges presented by the Web services approach are formidable and unavoidable. Many of the features that make Web services attractive, including greater accessibility of data, dynamic application-to-application connections, and relative autonomy (lack of human intervention) are at odds with traditional security models and controls. Difficult issues and unsolved problems exist, such as the following:

- Confidentiality and integrity of data transmitted via Web services protocols in service-to-service transactions, including data that transits intermediary (pass-through) services.
- Functional integrity of the Web services themselves, requiring both establishment in advance of the trustworthiness of services to be included in service orchestrations or choreographies, and the establishment of trust between services on a by-transaction basis.
- Availability in the face of denial of service attacks that exploit vulnerabilities unique to Web service technologies, especially targeting core services, such as discovery service, on which other services rely.

While many of the Web services challenges have been met with existing standards, there are a number of challenges that standards organizations are currently addressing — particularly in the area of Web services discovery and reliability. Few of these challenges will be addressed by any of the emerging web services security standards, the majority of which are limited to extending, enhancing, or augmenting current web services security standards in order to better provide message integrity, message confidentiality, and consumer/provider authentication.

Best Practices in Identity and Access Management
Paul Henry, Secure Computing

Today's requirements for Identity & Access Management (IAM) go well beyond our historical reliance on usernames and passwords. Regulatory demands as well as threats both internal and external to our networks have redefined the requirements for IAM. This presentation takes an in-depth look at the requirements for building an IAM and includes: How Did We Get Here (Usernames and passwords are obsolete), Two Factor Authentication (It is not what you use but how you use it), Centralized Access Policy Management (Policy must be enforced at all endpoints), Scan and Block (Permit access only from trusted machines). Attendees will walk away with a firm understanding of creating an IAM that can mitigate many of the risks associated with todays hostile network environment.

Preventing Identity Theft and Data Security Breaches: The Problem with Regulation
Brooke Oberwetter, CEI

Analysis of the possible effects of federal legislation suggests that comprehensive regulation of security practices might have the unintended consequences of locking in current technologies and thwarting market incentives for both collaboration among firms when necessary and competition between them to produce newer and more innovative solutions for cybersecurity problems. The objective of this presentation is to underscore the idea that private innovations — and private actors such as security firms — are much better suited for meeting the constantly evolving challenges of computer security than federal regulators could ever be.

17:00 **Tuesday sessions end**

18:00-21:00 **Reception and Exhibits (Starlight Ballroom)**

NIST National Institute of Standards and Technology Technology Administration U.S. Department of Commerce

Steven Bellovin to Receive NIST/NSA Security Award

Steven M. Bellovin, a pioneer researcher on network security, will be presented with the 2007 National Computer Systems Security Award by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The prestigious honor, first awarded in 1988, recognizes individuals for scientific or technological breakthroughs, outstanding leadership, highly distinguished authorship or significant long-term contributions in the computer security field.

Bellovin, currently a professor of computer science at Columbia University, was one of the originators of USENET as a graduate student at the University of North Carolina in the late 1970s. During more than 20 years of research at Bell Labs and AT&T Labs Research, Bellovin was one of the first researchers to recognize the importance of firewalls to network security, explore protocol failures, discuss routing security and utilize encrypted key exchange protocols.

Bellovin has served on numerous National Research Council computer security committees, was an Internet Engineering Task Force (IETF) security director from 2002-2004, and was a member of the now-defunct Department of Homeland Security's Science and Technology Advisory Board. He is the co-author of "Firewalls and Internet Security: Repelling the Wily Hacker," and holds several patents on cryptographic and network protocols.

For more about Bellovin, go to his Web site at `http://www.cs.columbia.edu/~smb`.

Reception sponsored by:

at&t Booz | Allen | Hamilton CS@CU COMPUTER SCIENCE AT COLUMBIA UNIVERSITY

Textbooks donated by Addison Wesley

Wednesday, December 13, 2006

Continental Breakfast (Regency Ballroom) sponsored by  7:30

Introduction of the Invited Essayist (Mediterranean East) 8:30
Dan Thomsen, Cyber Defense Agency, LLC

Invited Essayist
Engineering Sufficiently Secure Computing
Brian Witten, Symantec Corporation

We propose an architecture of four complimentary technologies increasingly relevant to a growing number of home users and organizations: cryptography, separation kernels, formal verification, and rapidly improving techniques relevant to software defect density estimation. Cryptographic separation protects information in transmission and storage. Formally proven properties of separation kernel based secure virtualization can bound risk for information in processing. Then, within each strongly separated domain, risk can be measured as a function of people and technology within that domain. Where hardware, software, and their interactions are proven to behave as and only as desired under all circumstances, such hardware and software can be considered to not substantially increase risk. Where the size or complexity of software is beyond such formal proofs, we discuss estimating risk related to software defect densities, and emerging work related to binary analysis with potential for improving software defect density estimation.

Break (Regency Ballroom) 10:00

Track 1 (Mediterranean Center): Applied Sandboxing 10:30
Konstantin Beznosov, University of British Columbia Track 1

A Module System for Isolating Untrusted Software Extensions ◇
Philip Fong, University of Regina
Simon Orr, University of Regina

With the recent advent of dynamically extensible software systems, in which software extensions may be dynamically loaded into the address space of a core application to augment its capabilities, there is a growing interest in protection mechanisms that can isolate untrusted software components from a host application. Existing languagebased environments such as the JVM and the CLI achieves software isolation by an interposition mechanism known as stack inspection. Expressive as it is, stack inspection is known to lack declarative characterization and is brittle in the face of evolving software configurations. A run-time module system, ISOMOD, is proposed for the Java platform to facilitate software isolation. A core application may create namespaces dynamically and impose arbitrary name visibility policies to control whether a name is visible, to whom it is visible, and in what way it can be accessed. Because ISOMOD exercises name visibility control at load time, loaded code runs at full speed. Furthermore, because ISOMOD access control policies are maintained separately, they evolve independently from core application code. In addition, the ISOMOD policy language provides a declarative means for expressing a very general form of visibility constraints. Not only can the ISOMOD policy language simulate a sizable subset of permissions in the Java 2 security architecture, it does so with policies that are robust to changes in software configurations. The ISOMOD policy language is also expressive enough to completely encode a capability type system known as Discretionary Capability Confinement. In spite of its expressiveness, the ISOMOD policy language admits an efficient implementation strategy. In short, ISOMOD avoids the technical difficulties of interposition by trading off an acceptable level of expressiveness. Name visibility control in the style of ISOMOD is therefore a lightweight alternative to interposition.

How to Automatically and Accurately Sandbox Microsoft IIS ◇
Wei Li, Rether Networks, Inc.
Lap-chung Lam, Rether Networks, Inc.
Tzi-cker Chiueh, Rether Networks, Inc.

Comparing the system call sequence of a network application against a sandboxing policy is a popular approach to detecting control-hijacking attack, in which the attacker exploits such software vulnerabilities as buffer overflow to take over the control of a victim application and possibly the underlying machine. The long-standing technical barrier to the acceptance of this system call monitoring approach is how to derive accurate sandboxing policies for Windows applications whose source code is unavailable. In fact, many commercial computer security companies take advantage of this fact and fashion a business model in which their users have to pay a subscription fee to receive periodic updates on the application sandboxing policies, much like anti-virus signatures. This paper describes the design, implementation and evaluation of a sandboxing system called BASS that can automatically extract a highly accurate application-specific sandboxing policy from a Win32/X86 binary, and enforce the extracted policy at run time with low performance overhead. BASS is built on a binary interpretation and analysis infrastructure called BIRD, which can handle application binaries with dynamically linked libraries, exception handlers and multi-threading, and has been shown to work correctly for a large number of commercially distributed Windows-based network applications, including IIS and Apache. The throughput and latency penalty of BASS for all the applications we have tested except one is under 8%.

Data Sandboxing: A Technique for Enforcing Confidentiality Policies ◇
Tejas Khatiwala, University of Illinois at Chicago
Raj Swaminathan, University of Illinois at Chicago
V.N. Venkatakrishnan, University of Illinois at Chicago

When an application reads private / sensitive information and subsequently communicates on an output channel such as a public file or a network connection, how can we ensure that the data written is free of private information? In this paper, we address this question in a practical setting through the use of a technique that we call "data sandboxing". Essentially, data sandboxing is implemented using the popular technique of system call interposition to mediate output channels used by a program. To distinguish between private and public data, the program is partitioned into two: one that contains all the instructions that handle sensitive data and the other containing the rest of the instructions. This partitioning is performed based on techniques from program slicing. When run together, these two programs collectively replace the original program. To address confidentiality, these programs are sandboxed with different system call interposition based policies. We discuss the design and implementation of a tool that enforces confidentiality policies on C programs using this technique. We also report our experiences in using our tool over several programs that handle confidential data.

10:30 **Track 2 (Mediterranean East): Malware**
Track 2 Chair: Anoop Singhal, National Institute for Standards and Technology

On Detecting Camouflaging Worm ◇
Wei Yu, Texas A&M University
Xun Wang, Ohio State University
Prasad Calyam, Ohio State University
Dong Xuan, Ohio State University
Wei Zhao, Texas A&M University

Active worms pose major security threats to the Internet. In this paper, we investigate a new class of active worms, i.e., Camouflaging Worm (C-Worm in short). The C-Worm has the capability to intelligently manipulate its scan traffic volume over time, thereby camouflaging its

propagation from existing worm detection systems. We analyze characteristics of the C-Worm and conduct a comprehensive comparison between its traffic and non-worm traffic. We observe that these two types of traffic are barely distinguishable in the time domain, however, their distinction is clear in the frequency domain, due to the recurring manipulative nature of the C-Worm. Motivated by our observations, we design a novel spectrum-based scheme to detect the CWorm. Our scheme uses the Power Spectral Density (PSD) distribution of the scan traffic volume and its corresponding Spectral Flatness Measure (SFM) to distinguish the CWorm traffic from non-worm traffic. We conduct extensive performance evaluations on our proposed detection scheme against the C-Worm. The performance data clearly demonstrates that our proposed scheme can effectively detect the C-Worm propagation.

Bluetooth Worms: Models, Dynamics, and Defense Implications ◇
Guanhua Yan, Los Alamos National Laboratory
Stephan Eidenbenz, Los Alamos National Laboratory

Recent occurrences of mobile worms like Cabir, Mabir and CommWarrior have created growing concerns over the security of data stored on mobile devices such as cell phones and PDAs. These worms have in common that they all use Bluetooth communication as their infection channel. In order to prepare effective defense strategies against such worms, we study the nature, characteristics, and spreading dynamics of Bluetooth worms in the safe environment of simulation. Our key findings are: (i) Mobility may not boost the Bluetooth worm propagation; instead, link instability owing to it has negative impact on the worm spreading speed; (ii) The inherent capacity constraints imposed by the wireless channel (e.g. interference) and the specifics of the Bluetooth protocol can significantly slow down the Bluetooth worm propagation; (iii) Intelligently designed worms can improve their propagation speed to a noticeable degree by strategically selecting worm model parameters or exploiting out-of-band propagation capabilities.

Back to the Future: A Framework for Automatic Malware Removal and System Repair ◇
Francis Hsu, University of California, Davis
Hao Chen, University of California, Davis
Thomas Ristenpart, University of California, San Diego
Jason Li, University of California, Davis
Zhendong Su, University of California, Davis

Malware, software with malicious intent, has emerged as a widely-spread threat to system security. It is difficult to detect malware reliably because new and polymorphic malware programs appear frequently. It is also difficult to remove malware and repair its damage to the system because it can extensively modify a system. We propose a novel framework for automatically removing malware from and repairing its damage to a system. The primary goal of our framework is to preserve system integrity. Our framework monitors and logs untrusted programs operations. Using the logs, it can completely remove malware programs and their effects on the system. Our framework does not require signatures or other prior knowledge of malware behavior. We implemented this framework on Windows and evaluated it with seven spyware, trojan horses, and email worms. Comparing our tool with two popular commercial anti-malware tools, we found that our tool detected all the malwares modifications to the system detected by the commercial tools, but the commercial tools overlooked up to 97% of the modifications detected by our tool. The runtime and space overhead of our prototype tool is acceptable. Our experience suggests that this framework offers an effective new defense against malware.

Track 3 (Mediterranean West): Case Studies 10:30
Chair: Ed Giorgio, Booz Allen Hamilton Track 3

Trusted Storage
Dave Anderson, Seagate Research

Storage Systems, such as disk drives, and other computing-system peripherals are critical components of a security, privacy, and trust configuration of a computing platform. This session provides a framework with which to understand why and how peripheral devices should be secured as independent roots of trust. The framework provides a generic security model for all peripheral devices, and shows how peripherals can be configured as roots of trust, each playing a complementary role in establishing the overall security and privacy goals of platform-based and networked computing. The session begins with security measures for storage systems that exist today and their relative effectiveness. It will then go into where and how to secure access control of the storage system, discussing in detail what needs to be controlled and how to grant control in a secure manner. The Trusted Computing Group's Trusted Storage Use Cases will be reviewed in depth, highlighting the technical requirements being solved by the formal specifications. Relationships and cooperation with other industry storage standards (eg, SCSI and ATA) will be discussed, and the TCG's specification for secure and trusted storage will be outlined.

Putting Trust into the Network: Securing Your Network through Trusted Access Control
Steve Hanna, Juniper Networks

Today, client network connection requests are granted or denied based on the client's ability to prove their credentials, including passwords, machine certificates and user certificates. This approach ignores the possibility that the client platform contains malicious code (e.g. viruses, Trojans, malware) that spreads through the network once IP connectivity is granted. Trusted Computing and its hardware elements provide the most reliable and secure method to ascertain end-point integrity for clients seeking connectivity to a network. Through trusted network connection protocols and trusted platform mechanisms, platforms can be authenticated before being given full network connectivity. This speaker will address the architecture, applications, status of the Trusted Network Connect specification which is backed by more than 90 companies and also discuss how to properly implement it.

Employing Encryption to Combat Data Theft
Derek Tumulak, Ingrian Networks

In the wake of continued data thefts and security breaches and increasingly rigorous security and privacy mandates, encryption of data at rest is becoming a necessity for about any organization that manages sensitive customer or employee data. This presentation will provide an overview of the industry mandates for encryption of data at rest, an overview of the pros and cons of various encryption solutions, and offer best practices for deploying an encryption solution.

12:00 **Lunch (Regency Ballroom) sponsored by** 

13:30 **Track 1 (Mediterranean Center): Applied Detection Technologies**
Track 1 Chair: Arthur R. Friedman, OASD(NII)/DoD CIO

Static Detection of Vulnerabilities in x86 Executables ◇
Greg Banks, University of California, Santa Barbara
Marco Cova, University of California, Santa Barbara
Viktoria Felmetsger, University of California, Santa Barbara
Giovanni Vigna, University of California, Santa Barbara

In the last few years, several approaches have been proposed to perform vulnerability analysis of applications written in high-level languages. However, little has been done to automatically identify security-relevant flaws in binary code. In this paper, we present a novel approach to the identification of vulnerabilities in x86 executables in ELF binary format. Our approach is based on static analysis and symbolic execution techniques. We implemented our approach in a

proof-of-concept tool and used it to detect taint-style vulnerabilities in binary code. The results of our evaluation show that our approach is both practical and effective.

Foreign Code Detection on the Windows/X86 Platform ◇
Susanta Nanda, Stony Brook University
Wei Li, Stony Brook University
Lap-Chung Lam, Rether Networks
Tzi-cker Chiueh, Stony Brook University

As new attacks against Windows-based machines emerge almost on a daily basis, there is an increasing need to lock down individual users desktop machines in corporate computing environments. One particular way to lock down a user computer is to guarantee that only authorized binary programs are allowed to run on that computer. A major advantage of this approach is that binaries downloaded without the users knowledge, such as spyware, adware, or code entering through buffer overflow attacks, can never run on computers that are locked down this way. This paper presents the design, implementation and evaluation of FOOD, a foreign code detection system specifically for the Windows/X86 platform, where foreign code is defined as any binary programs that do not go through an authorized installation procedure. FOOD verifies the legitimacy of binary images involved in process creation and library loading to ensure that only authorized binaries are used in these operations. In addition, FOOD checks the target address of every indirect branch instruction in Windows binaries to prevent illegitimate control transfers to either dynamically injected mobile code or pre-existing library functions that are potentially damaging. Combined together, these techniques strictly prevent the execution of any foreign code. Experiments with a fully working FOOD prototype show that it can indeed stop all spyware and buffer overflow attacks we tested, and its worst-case run-time performance overhead associated with foreign code detection is less than 35%.

PolyUnpack: Automating the Hidden-Code Extraction of Unpack-Executing Malware ◇
Paul Royal, Georgia Institute of Technology
Mitch Halpin, Georgia Institute of Technology
David Dagon, Georgia Institute of Technology
Robert Edmonds, Georgia Institute of Technology
Wenke Lee, Georgia Institute of Technology

Modern malware often hide the malicious portion of their program code by making it appear as data at compile time and transforming it back into executable code at runtime. This obfuscation technique poses obstacles to researchers who want to understand the malicious behavior of new or unknown malware and to practitioners who want to create models of detection and methods of recovery. In this paper we propose a technique for automating the process of extracting the hidden-code bodies of this class of malware. Our approach is based on the observation that sequences of packed or hidden code in a malware instance can be made self-identifying when its runtime execution is checked against its static code model. In deriving our technique, we formally define the unpack-executing behavior that such malware exhibits and devise an algorithm for identifying and extracting its hidden-code. We also provide details of the implementation and evaluation of our extraction technique; the results from our experiments on several thousand malware binaries show our approach can be used to significantly reduce the time required to analyze such malware, and to improve the performance of malware detection tools.

Track 2 (Mediterranean East): Panel 13:30 Track 2

Partnering with Industry and Academia - The DHS S&T Approach to Cyber Security Research, Development, Test, and Evaluation
Dr. Douglas Maughan, U.S. Department of Homeland Security (DHS), Science and Technology (S&T) Directorate (Chair)

Dr. Steve Crocker, Shinkuro
Dave Jevans, Anti-Phishing Working Group and IronKey
Tom Aubuchon, Chevron Pipeline
Terry Benzel, USC-ISI
Mark Schertler, Voltage Security OR Dr. Ulf Lindqvist, SRI International

The Science and Technology (S&T) Directorate in the U.S. Department of Homeland Security (DHS) has the mission to conduct research, development, test and evaluation (RDT&E), and timely transition of cyber security capabilities to operational units within DHS, as well as federal, state, local, and critical infrastructure sector operational end users for homeland security purposes. Collaboration and partnerships with academia, research labs, and private industry is required for success in this mission, and this panel will present some of the partnerships that DHS S&T is currently involved in and supporting. The speakers will present their projects and their experiences of working with DHS S&T and the other partners.

- The DNSSEC Deployment Initiative is a community-based, international effort to transition the current state of DNSSEC to large-scale deployment that will strengthen the Internet domain name system against attacks.
- The DHS-SRI International Identity Theft Technology Council (ITTC) is a working forum where experts and leaders from the government, private, financial, IT, venture capitalist, and academia and science sectors come together to address the problem of identity theft and related criminal activity on the Internet.
- Project LOGIIC is a 12-month technology integration and demonstration project jointly supported by industry partners and DHS S&T. The project demonstrates an opportunity to reduce vulnerabilities of oil and gas process control environments by sensing, correlating and analyzing abnormal events to identify and prevent cyber security threats. It is also an illustration of a successful model for collaboration between infrastructure owners, technology providers, research labs, and the Government.
- The DETER testbed, jointly supported by NSF and DHS S&T, is a shared testbed infrastructure that is specifically designed for medium-scale repeatable experiments, and especially for experiments that may involve "risky" code such as self-propagating malware.
- The Secure Wireless Data Program is a collaboration between the U.S. and Canadian governments and multiple industry partners. SRI International leads an integration of new and innovative security technologies followed by trials to test the solution in real-case scenarios. The program is focused on overlays and complementary technologies that can be used to enhance security with minimal impact on the usability of the basic mobile data platform.

13:30 Track 3

Track 3 (Mediterranean West): Industrial Control System Security

An Overview of Emerging Standards, Guidelines, and Implementation Activities
Stu Katzke, NIST
Joe Weiss, KEMA

Industrial and process control systems are an integral part of the critical infrastructure and the protection of those systems is a priority for the federal government. From air traffic control systems to the systems managing the nations largest electric power grids, industrial controls systems are playing an increasingly important role in the economic and national security interests of the United States. Until recently, industrial control systems had little resemblance to traditional information systems in that they were isolated systems running proprietary software and control protocols. However, as these systems are integrated more closely into mainstream organizational information systems to promote connectivity, efficiency, and remote

access capabilities, they have started to resemble the more traditional information systems. While the change in industrial control system architecture supports new information system capabilities, it introduces many of the same vulnerabilities that exist in current networked information systems. This session addresses the emerging industrial and process control security standards within the public and private sectors and the overall effect of those standards and activities in helping to secure these important systems.

Break (Regency Ballroom) 15:00

Combined Track 1 and 2 (Mediterranean East): Works in Progress Session 15:30
Chair: Cristina Serban, AT&T Track 1–2

- Maarten Rits and Mohammad Ashiqur Rahaman - SAP Labs France: Secure SOAP Requests in Enterprise SOA
- Edward Colbert, Dan Wu, Yue Chen and Barry Boehm - University of Southern California: Cost Estimation for Secure Software and Systems
- Eduardo B. Fernandez and Maria M. Larrondo-Petrie - Florida Atlantic University: A Methodology to build secure systems using patterns
- Tugkan Tuglular - Izmir Institute of Technology: Test Case Generation for Firewall Testing
- Kimberly Caplan, Tresys Technology: Authoring Tool for Common Criteria Documents
- Uciel Fragoso-Rodriguez, Maryline Laurent-Maknavicius and Jose Incera-Dieguez - Instituto Tecnolgico Autnomo de Mxico, Mexico: Federated Identity Architectures Evaluation
- John McDermott and Myong Kang - NRL: An Open-Source High-Robustness VMM
- Tim Kelley, Indiana University: A Method for Increasing Transmission Rates in Covert Timing Channels
- Rosalie M. McQuaid, William Heinbockel, Joseph Judge, Peter Kertzner and Brian Soby - MITRE Corporation: Security Information Management for Enclave Networks (SIMEN)
- William Claycomb and Dongwan Shin - New Mexico Tech: Designing and Implementing Access Control for Impromptu Collaboration
- Takuya Mishina, Yuji Watanabe, Yasuharu Katsuno and Sachiko Yoshihama - IBM Research, Tokyo Research Laboratory: Semantic Fine-grained Data Provenance Tracking
- Ravi Chandra Jammalamadaka and Sharad Mehrotra - University of California, Irvine: Outsourcing Data Sharing Requirements to an Untrusted Service Provider
- Kris Britton - NSA Center for Assured Software: Software Assurance Analysis Methodology
- Ron Finkbine - Indiana University Southeast: A Database for Managing Mutant Programs
- David Botta, Rodrigo Werlinger, Andr Gagn, Konstantin Beznosov, Lee Iverson, Brian Fisher and Sidney Fels - University of British Columbia: HOT Admin: Human, Organization, and Technology Centered Improvement of IT Security Administration
- Coimbatore Chandersekaran, Edward A. Schneider and William R. Simpson - Institute for Defense Analyses: Evaluating Security in Distributed Service-Oriented Systems
- Francisco Nunes, Arnaldo Dias Belchior - Universidade de Fortaleza, Brazil: Software Development Secure Process Implementation
- Houssain Kettani - Jackson State University, MS: A Cryptographic Application of Number Systems Base Conversion
- Sashikanth Chandrasekaran - Oracle: Event Processing to Verify Compliance with Security Policies [a case study]

The order of the presentations is subject to change.

Track 3 (Mediterranean West): Case Studies 15:30
Chair: Ron Ritchey, Booz Allen Hamilton Track 3

CANADIAN-US Security Enhanced BlackBerry Trial
Mark Schertler, Voltage

BlackBerry devices are representative of today's state-of-the-art for small portable communications devices and are widely deployed in the private sector, as well as by U.S. and Canadian government agencies at the federal, state and local levels. In order to study and enhance security for Blackberry devices the joint Canada-US Public Safety Technical Program (PSTP) initiated a joint US Canadian trial. Trial partners include Defense Research and Development Canada (DRDC), an agency of the Department of National Defense (DND); and the Homeland Security Advanced Research Projects Agency (HSARPA), an agency of the United States Department of Homeland Security (DHS). The trial was directed at improving the security of existing, proven BlackBerry technology for use by the public safety, emergency preparedness, and law enforcement communities in both countries. The trial's research focused on overlays and complementary technologies that can be used to enhance security with minimal impact on the usability of the basic BlackBerry system. The trial had the following objectives:

- Improve the security of BlackBerry technology security with minimal impact on the usability of the basic BlackBerry system
- Explore opportunities and requirements for the secure use of BlackBerry devices by the public safety, emergency preparedness, and law enforcement communities.
- Demonstrate policy enforcement and procedure constraints by integrating policy scanning and encryption technologies.
- Demonstrate the reduction of public key infrastructure overhead through use of new public key technologies developed in government sponsored research.
- Improve mission assurance by extending the coverage of BlackBerry communications beyond the terrestrial cellular phone system through mobile satellite ground stations that can be mounted on small marine vessels and all-terrain wheeled vehicles.
- Improve interoperability by stimulating the development of inexpensive mobile communications nodes for first responders that support multiple emerging wireless access protocols, new portable devices and digital services.
- Examine the secure e-mail solution jointly developed by Canadas Communication Security Establishment (CSE) and the USs National Security Agency (NSA).

This discussion will cover the objectives of the trial, execution and results.

Wi-Fi Protected Access for Protection and Automation
Dennis Holstein, OPUS Publishing

CIGRE Study Committee B5 commissioned a survey of applications using Wi-Fi in protection and automation schemes and an analysis of the mitigation of security vulnerabilities offered by IEEE 802.11i on system reliability and performance. Working Group (WG) B5.22 was further tasked to recommend design requirements and prioritized security levels needed for Wi-Fi protected access related to critical mission protection and automation functions. This presentation summarizes the findings of that investigation. Design requirements and security levels needed for Wi-Fi protected access are prioritized in terms of their mitigation of risk related to critical mission protection and automation functions. Specific mechanisms needed to adequately implement Wi-Fi are identified and related to existing or emerging standards.

XL Global Services: A Compelling Case Study in Data Privacy
Mark Schertler, Voltage

XL Global Services provides IT Services to the XL Capital group of companies. A $50 billion corporation with locations in worldwide, Global Chief Security Officer Tom Dunbar is charged with the Herculean mission of being able to assure that sensitive data will remain privacy-protected and secure according to corporate policies and legislative requirements. With 3,400 local, mobile and remote users, a solution for leveraging digital communications had to feature (a) strong encryption with digital signature support to verify email senders, while ultimately being simple and usable; (b) enterprise scalability, while remaining smoothly flexible; and (c) auditable support of complex regulatory compliance laws, while providing lowest possible total cost of ownership. In this presentation, Mark Schertler will outline the data privacy implementation, while sharing tips, Best Practices, and real-world usable guidance for information technology and security pros.

Wednesday sessions end 17:00

Thursday, December 14, 2006

7:30 **Continental Breakfast (Regency Ballroom)**

8:30 **Introduction of the Classic Papers (Mediterranean East)**
Tom Haigh, Adventium Labs and the Cyber Defense Agency, LLC

Fifteen Years after TX: A Look Back at High Assurance Multi-Level Secure Windowing
Jeremy Epstein, webMethods, Inc.

> Research in the late 1980s and early 1990s produced a prototype high assurance multi-level secure windowing system that allowed users to see information of multiple classifications on the same screen, performing cut & paste from low to high windows. This retrospective discusses the motivations for the project, reviews the architecture and implementation of the prototype, discusses developments in the intervening years, and concludes with lessons learned.

Risks of Untrustworthiness
Peter G. Neumann, SRI International Computer Science Lab

> This paper revisits the risks of untrustworthiness, and considers some incidents involving computer-based systems that have failed to live up to what had been expected of them. The risks relate to security, reliability, survivability, human safety, and other attributes, and span a variety of applications and critical infrastructures such as electric power, telecommunications, transportation, finance, medical care, and elections. The range of causative factors and the diversity of the resulting risks are both enormous. Unfortunately, many of the problems seem to recur far too often. Various lessons therefrom and potential remedies are discussed.

10:00 **Break (Regency Ballroom)**

10:30 **Track 1 (Mediterranean Center): Applied Randomization**
Track 1 Chair: Steven J. Greenwald, Independent Consultant

Address-Space Randomization for Windows Systems ◇
Lixin Li, Global Infotek
James Just, Global Infotek
R. Sekar, Stony Brook University

> Address-space randomization (ASR) is a promising solution to defend against memory corruption attacks that have contributed to about three-quarters of USCERT advisories in the past few years. Several techniques have been proposed for implementing ASR on Linux, but its application to Microsoft Windows, the largest monoculture on the Internet, has not received as much attention. We address this problem in this paper and describe a solution that provides about 15-bits of randomness in the locations of all (code or data) objects. Our randomization is applicable to all processes on a Windows box, including all core system services, as well as applications such as web browsers, office applications, and so on. Our solution has been deployed continuously for about a year on a desktop system used daily, and is robust enough for production use.

Address Space Layout Permutation (ASLP): Towards Fine-Grained Randomization of Commodity Software ◇
Chongkyung Kil, North Carolina State University
Jinsuk Jun, North Carolina State University
Christopher Bookholt, North Carolina State University
Jun Xu, North Carolina State University
Peng Ning, North Carolina State University

> Address space randomization is an emerging and promising method for stopping a broad range

of memory corruption attacks. By randomly shifting critical memory regions at process initialization time, address space randomization converts an otherwise successful malicious attack into a benign process crash. However, existing approaches either introduce insufficient randomness, or require source code modification. While insufficient randomness allows successful brute-force attacks, as shown in recent studies, the required source code modification prevents this effective method from being used for commodity software, which is the major source of exploited vulnerabilities on the Internet. We propose Address Space Layout Permutation (ASLP) that introduces high degree of randomness (or high entropy) with minimal performance overhead. Essential to ASLP is a novel binary rewriting tool that can place the static code and data segments of a compiled executable to a randomly specified location and performs finegrained permutation of procedure bodies in the code segment as well as static data objects in the data segment. We have also modified the Linux operating system kernel to permute stack, heap, and memory mapped regions. Together, ASLP completely permutes memory regions in an application. Our security and performance evaluation shows minimal performance overhead with orders of magnitude improvement in randomness (e.g., up to 29 bits of randomness on a 32-bit architecture).

Known/Chosen Key attacks against Software Instruction Set Randomization ◇
Yoav Weiss, Discretix Technologies Ltd.
Elena Gabriela Barrantes, Universidad de Costa Rica

Instruction Set Randomization (ISR) has been proposed as a form of defense against binary code injection into an executing program. One proof-of-concept implementation is Randomized Instruction Set Emulator (RISE), based on the open-source Valgrind IA-32 to IA-32 binary translator. Although RISE is effective against attacks that are not RISE-aware, it is vulnerable to pure data and hybrid data-code attacks that target its data, as well to some classes of bruteforce guessing. In order to enable the design of a production version, we describe implementation-specific and generic vulnerabilities that can be used to overcome RISE in its current form. We present and discuss attacks and solutions in three categories: known-key attacks that rely on the key being leaked and then used to pre-scramble the attacking code; chosen-key attacks that use implementation weaknesses to allow the attacker to define its own key, or otherwise affect key generation; and key-guessing ("brute force") attacks, about which we explore the design of minimalistic loaders which can be used to minimize the number of mask bytes required for a successful key-guessing attack. All the described attacks were tested in real-world scenarios.

Track 2 (Mediterranean East): Intrusion Detection 10:30
Chair: Carrie Gates, CA Labs Track 2

Automatic Evaluation of Intrusion Detection Systems ◇
Frédéric Massicotte, Communications Research Center
Fran cois Gagnon, Carleton University
Yvan Labiche, Carleton University
Lionel Briand, Carleton University
Mathieu Couture, Carleton University

An Intrusion Detection System (IDS) is a crucial element of a network security posture. Although there are many IDS products available, it is rather difficult to find information about their accuracy. Only a few organizations evaluate these products. Furthermore, the data used to test and evaluate these IDS is usually proprietary. Thus, the research community cannot easily evaluate the next generation of IDS. Toward this end, DARPA provided in 1998, 1999 and 2000 an Intrusion Detection Evaluation Data Set. However, no new data set has been released by DARPA since 2000, in part because of the cumbersomeness of the task. In this paper, we propose a strategy to address certain aspects of generating a publicly available documented data set for testing and evaluating intrusion detection systems. We also present a

tool that automatically analyzes and evaluates IDS using our proposed data set.

Offloading IDS Computation to the GPU ◇
Nigel Jacob, Tufts University
Carla Brodley, Tufts University

Signature-matching Intrusion Detection Systems can experience significant decreases in performance when the load on the IDS-host increases. We propose a solution that off-loads some of the computation performed by the IDS to the Graphics Processing Unit (GPU). Modern GPUs are programmable, stream-processors capable of high performance computing that in recent years have been used in non-graphical computing tasks. The major operation in a signature-matching IDS is matching values seen operation to known black-listed values, as such, our solution implements the string-matching on the GPU. The results show that as the CPU load on the IDS host system increases, PixelSnorts performance is significantly more robust and is able to outperform conventional Snort by up to 40%.

Anomaly Based Web Phishing Page Detection ◇
Ying Pan, Singapore Management University
Xuhua Ding, Singapore Management University

Many anti-phishing schemes have recently been proposed in literature. Despite all those efforts, the threat of phishing attacks is not mitigated. One of the main reasons is that phishing attackers have the adaptability to change their tactics with little cost. In this paper, we propose a novel approach, which is independent of any specific phishing implementation. Our idea is to examine the anomalies in web pages, in particular, the discrepancy between a web sites identity and its structural features and HTTP transactions. It demands neither user expertise nor prior knowledge of the website. The evasion of our phishing detection entails high cost to the adversary. As shown by the experiments, our phishing detector functions with low miss rate and low false-positive rate.

10:30 **Track 3 (Mediterranean West): Case Studies**
Track 3 Chair: Gary Wilson, Booz Allen Hamilton

Certification and Accreditation at National Oceanographic and Atmospheric Administration (NOAA), National Environmental Satellite, Data, and Information Service (NESDIS)
Dan Gambel, Mitretek Systems

In 2004 NOAA systems were identified by the Department of Commerce as being deficient in having current and compliant accreditation packages approved. NOAA operates a significant number of legacy systems that were developed prior to current standards and guidelines for IT security. As a result, the documentation of the security of the various systems was fragmentary and incomplete. In an attempt to achieve accreditation for these national critical and mission critical systems, NOAA elected to standardize the content of the security plans, an approach that was not acceptable to DOC Office of Inspector General. Mark Noto was brought into the security team by a newly appointed CIO to correct the problems with the process. The approach to fixing the problems was to assemble a team of existing contractors and NOAA staff into red teams to define the specific requirements for the System Security Plans, Risk assessment, testing, and Contingency documentation. Once the documentation requirements were adequate, three packages covering the three most critical systems were prepared and submitted for post-certification review by NOAA and DOC OIG. Based on comments on the initial package, a number of changes were made to the process, especially on details of the architecture and consistency of the scanning and inventory. Based on the revised requirements NOAA NESDIS has prepared, certified and approved packages for all active National and Mission critical systems and are progressing through mission essential systems. The presentation will address the current process and how the senior officials are responding to the

information being provided. In addition, the NOAA process modification necessary to accommodate FISMA will be identified and, where available, solutions applicable to NOAA will be provided.

Using Predictive Analytics and Modeling to Improve Insider Threat Detection and Cyber Threat Identification
Peter Frometa, SPSS Inc

A valuable approach to insider threat detection and cyber threat identification involves applying predictive analysis. Learn how predictive analysis can be leveraged to identify key characteristics of valid versus invalid network access attempts and web traffic patterns, as well as uncovering patterns in documented malicious activity. As millions of cases pass through network ports on a daily basis, predictive analytic techniques can also be applied to better predict and prevent activity that signals potentially suspicious behavior, or cases that could indicate malicious web robots or intrusion attempts. One of the many major advantages of this approach is that, instead of focusing efforts solely on specific, previously named viruses, predictive analytics looks at the behavior as a whole, and targets specific patterns or anomalies, greatly enhancing the likelihood of identifying and stopping new viruses or emerging variants as well as potential hacker activity. Through the incorporation of additional structured data sources such as employee key card access files, log-on audit logs, and file access logs; and unstructured data sources such as the content of web pages, downloaded files and documents, and intelligence reports; predictive analytics allows cyber threat identification to incorporate not only external threats, but those that exist internal to an organization as well (insider threats).

The Business of Enterprise Privacy, Compliance
Mark Schertler, Voltage

While there has been significant focus on compliance as a driver for security investments, as well as significant FUD generated by vendors, the use of security products can drive significant business value at the intersection of compliance with core business drivers. This presentation examine how, even faced by daunting regulatory requirements and significant fines, many organizations can achieve concrete, measurable, and near-term business value when deploying enterprise privacy and security solutions that also deliver business process efficiencies. The focus will be specifically on case studies from the insurance and financial services industries.

Lunch (Regency Ballroom) 12:00

Track 1 (Mediterranean Center): Messaging Security 13:30
Chair: John Totah, Sun Microsystems, Inc. Track 1

Addressing SMTP-based Mass-Mailing Activity Within Enterprise Networks ◇
David Whyte, Carleton University
Paul van Oorschot, Carleton University
Evangelos Kranakis, Carleton University

Malicious mass-mailing activity on the Internet is a serious and continuing threat that includes mass-mailing worms, spam, and phishing. A mechanism commonly used to deliver such malicious mass mail is an SMTP engine, which turns an infected system into a malicious mail server. We present a technique that enables, within a single mailing attempt in many popular network environments, detection and containment of (even zero-day) SMTP-engine based mass-mailing activity. Contrary to other mass-mailing detection techniques our approach is content independent and requires no attachment processing, network traffic correlation, statistical measures, or system behavioral analysis. It relies instead on the observation of DNS MX queries within the enterprise network. This stateless detection technique requires minimal computational resources making it ideally suited for real-time wire-speed deployment.

Using Attribute-Based Access Control to Enable Attribute-Based Messaging ◇
Rakesh Bobba, University of Illinois
Omid Fatemieh, University of Illinois
Fariba Khan, University of Illinois
Carl Gunter, University of Illinois
Himanshu Khurana, University of Illinois

Attribute Based Messaging (ABM) enables message senders to dynamically create a list of recipients based on their attributes as inferred from an enterprise database. Such targeted messaging can reduce unnecessary communications and enhance privacy, but faces challenges in access control. In this paper we explore an approach to ABM based on deriving access control information from the same attribute database exploited by the addressing scheme. We show how to address three key challenges. First, we demonstrate a manageable access control system based on attributes. Second we show how this can be used with existing messaging systems to provide a practical deployment strategy. Third, we show that such a system can be efficient enough to support ABM for mid-size enterprises. Our implementation can dispatch ABM messages approved by XACML review for an enterprise of at least 60,000 users with only seconds of latency.

Enhancing Signature-based Collaborative Spam Detection with Bloom Filters ◇
Jeff Yan, University of Newcastle upon Tyne
Pook Leong Cho, University of Newcastle upon Tyne

Signature-based collaborative spam detection (SCSD) systems provide a promising solution addressing many problems facing statistical spam filters, the most widely adopted technology for detecting junk emails. In particular, some SCSD systems can identify previously unseen spam messages as such, although intuitively this would appear to be impossible. However, the SCSD approach usually relies on huge databases of email signatures, demanding lots of resource in signature lookup, storage, transmission and merging. In this paper, we report our enhancements to two representative SCSD systems. In our enhancements, signature lookups can be performed in constant time, independent of the number of signatures in the database. Space-efficient representation can significantly reduce signature database size. A simple but fast algorithm for merging different signature databases is also supported. We use the Bloom filter technique and a novel variant of this technique to achieve all this.

13:30 **Track 2 (Mediterranean East): Countermeasures**
Track 2 Chair: Rick Smith, University of St. Thomas

Extended protection against stack smashing attacks without performance loss ◇
Yves Younan, Katholieke Universiteit Leuven
Davide Pozza, Politecnico di Torino
Frank Piessens, Katholieke Universiteit Leuven
Wouter Joosen, Katholieke Universiteit Leuven

In this paper we present an efficient countermeasure against stack smashing attacks. Our countermeasure does not rely on secret values (such as canaries) and protects against attacks that are not addressed by state-of-the-art countermeasures. Our technique splits the standard stack into multiple stacks. The allocation of data types to one of the stacks is based on the chances that a specific data element is either a target of attacks and/or an attack vector. We have implemented our solution in a C-compiler for Linux. The evaluation shows that the overhead of using our countermeasure is negligible.

PAST : Probabilistic Authentication of Sensor Timestamps ◇
Ashish Gehani, University of Notre Dame
Surendar Chandra, University of Notre Dame

Sensor networks are deployed to monitor the physical environment in public and vulnerable locations. It is not economically viable to house sensors in tamper-resilient enclosures as they are deployed in large numbers. As a result, an adversary can subvert the integrity of the data being produced by gaining physical access to a sensor and altering its code. If the sensor output is timestamped, then tainted data can be distinguished once the time of attack is determined. To prevent the adversary from generating fraudulent timestamps, the data must be authenticated using a forward-secure protocol. Previous work requires the computation of n hashes to verify the (n+1)th reading. This paper describes PAST, a protocol that allows timestamps to be authenticated with high probability using a small constant number of readings. In particular, PAST is parameterized so that the metadata overhead (and associated power consumption) can be reduced at the cost of lower confidence in the authentication guarantee. Our protocol allows arbitrary levels of assurance for the integrity of timestamps (with logarithmically increasing storage costs) while tolerating any predefined fraction of compromised base stations. Unlike prior schemes, PAST does not depend on synchronized clocks.

Towards Database Firewall: Mining the Damage Spreading Patterns ◇
Kun Bai, Pennsylvania State University, University Park
Peng Liu, Pennsylvania State University, University Park

Access control and integrity constraints are well known approaches to ensure data integrity in commercial database systems. However, due to operational mistakes, malicious intent of insiders or vulnerabilities exploited by outsiders, data stored in a database can still be compromised. When the database is under an attack, rolling back and re-executing the damaged transactions are the most used mechanisms during system recovery. This kind of mechanism either stops (or greatly restricts) the database service during repair, which causes unacceptable availability loss or denialof-service for mission critical applications, or may cause serious damage spreading during on-the-fly recovery where many clean data items are accidentally corrupted by legitimate new transactions. To resolve this dilemma, we devise a novel mechanism, called database firewall in this paper. This firewall is designed to protect good data from being corrupted due to damage spreading. Pattern mining and Bayesian network techniques are adopted in the framework to mine frequent damage spreading patterns and to predict the data integrity in the face of attack. Our approach provides a probability based strategy to estimate the data integrity on the fly. With this feature, the database firewall is able to enforce a policy of transaction filtering to dynamically filter out the potential spreading transactions.

Track 3 (Mediterranean West): Certification and Accreditation 13:30 Track 3

Understanding the Risks to Enterprises and their Information Technology Infrastructure
Ron Ross, NIST
Julie Mehan, Hatha Systems

Understanding the risks to enterprise missions resulting from the operation of highly-connected and complex information systems and networks is a top priority for public and private sector organizations today. Establishing a cost-effective and disciplined approach to assessing the effectiveness of the security controls (i.e., safeguards and countermeasures) employed to protect enterprise information systems and the critical missions supported by those systems is the driving force behind todays certification and accreditation (C&A) efforts. Many efforts are underway both nationally and internationally, to streamline the C&A process and to promote activities that facilitate credible, risk-based decisions on the part of authorizing officials (a.k.a. designated accreditation authorities). This session addresses two of the most significant C&A processes currently employed by the federal government to address the security issues related to federal information systems; NIST Special Publication 800-37 covering the C&A process for federal non-national security systems and the Defense Departments Information Assurance

Certification and Accreditation Process covering the needs of the warfighter and key military applications and systems.

15:00 **Ice Cream Social (Regency Ballroom) sponsored by** 

15:30 **Track 1 (Mediterranean Center): Information Flow and Leakage**

Track 1 Chair: Ed Schneider, IDA

A General Dynamic Information Flow Tracking Framework for Security Applications ◇
Lap Chung Lam, Rether Networks, Inc.
Tzi-cker Chiueh, Stony Brook University

Many software security solutions require accurate tracking of control/data dependencies among information objects in network applications. This paper presents a general dynamic information flow tracking framework (called GIFT) for C programs that allows an application developer to associate applicationspecific tags with input data, instruments the application to propagate these tags to all the other data that are control/data-dependent on them, and invokes application-specific processing on output data according to their tag values. To use GIFT, an application developer only needs to implement input and output proxy functions to tag input data and to perform tag-dependent processing on output data, respectively. To demonstrate the usefulness of GIFT, we implement a complete GIFT application called Aussum, which allows selective sandboxing of network client applications based on whether their inputs are tainted or not. For a set of computation-intensive test applications, the measured elapsed time overhead of GIFT is less than 35%.

Covert and Side Channels due to Processor Architecture ◇
Zhenghong Wang, Princeton University
Ruby Lee, Princeton University

Information leakage through covert channels and side channels is becoming a serious problem, especially when these are enhanced by modern processor architecture features. We show how processor architecture features such as simultaneous multithreading, control speculation and shared caches can inadvertently accelerate such covert channels or enable new covert channels and side channels. We first illustrate the reality and severity of this problem by describing concrete attacks. We identify two new covert channels. We show orders of magnitude increases in covert channel capacities. We then present two solutions, Selective Partitioning and the novel Random Permutation Cache (RPCache). The RPCache can thwart most cache-based software side channel attacks, with minimal hardware costs and negligible performance impact.

CryptoPage: an Efficient Secure Architecture with Memory Encryption, Integrity and Information Leakage Protection ◇
Guillaume Duc, ENST Bretagne
Ronan Keryell, ENST Bretagne

Several secure computing hardware architectures using memory encryption and memory integrity checkers have been proposed during the past few years to provide applications with a tamper resistant environment. Some solutions, such as HIDE, have also been proposed to solve the problem of information leakage on the address bus. We propose the CRYPTOPAGE architecture which implements memory encryption, memory integrity protection checking and information leakage protection together with a low performance penalty (3% slowdown on average) by combining the Counter Mode of operation, local authentication values and Merkle trees.

Protecting Privacy in Key-Value Search Systems ◇
Yinglian Xie, Carnegie Mellon University

David O'Hallaron, Carnegie Mellon University
Michael Reiter, Carnegie Mellon University

This paper investigates the general problem of efficiently performing key-value search at untrusted servers without loss of user privacy. Given key-value pairs from multiple owners that are stored across untrusted servers, how can a client efficiently search these pairs such that no server, on its own, can reconstruct the key-value pairs? We propose a system, called Peekaboo, that is applicable and practical to any type of key-value search while protecting both data owner privacy and client privacy. The main idea is to separate the key-value pairs across different servers. Supported by access control and user authentication, Peekaboo allows search to be performed by only authorized clients without reducing the level of user privacy.

Track 2 (Mediterranean East): Panel 15:30
Track 2

Highlights from the 2006 New Security Paradigms Workshop (NSPW)
Chair: Carol Taylor, University of Idaho

This panel highlights a selection of the most interesting and provocative papers from the 2006 New Security Paradigms Workshop. The URL for more information is `http://www.nspw.org`. The panel consists of authors of the selected papers, and the session is moderated by the workshop's general chairs. We present selected papers focusing on exciting major themes that emerged from the workshop. These are the papers that will provoke the most interesting discussion at ACSAC.

Track 3 (Mediterranean West): Minimum Security Requirements 15:30
Track 3

FIPS 200: The Standard and Its Effect on the Public and Private Sectors
Ron Ross, NIST
Graydon McKee, Unisys (Invited)

The Federal Information Security Management Act of 2002 places significant requirements on Federal agencies for the protection of information and information systems including those systems comprising the critical infrastructure of the United States. The National Institute of Standards and Technology (NIST) is leading the development of key information system security standards and guidelines as part of its FISMA Implementation Project. One of the principal security standards, Federal Information Processing Standard (FIPS) 200, identifies minimum security requirements for federal information and information systems. The FIPS 200 minimum security requirements are linked to another NIST publication, Special Publication 800-53, which describes the minimum security controls (safeguards and counter measures) necessary to protect enterprise missions in the face of ever-increasing and sophisticated attacks. This session provides insights into the effects of the legislation and the implementing security standards and guidance on the public and private sector.

Thursday sessions end (except Track 1, which ends at 17:30) 17:00

Friday, December 15, 2006

Tutorial F5 *Next-Generation Wireless Risks & Defenses*
Speaker: Mr. Richard Rushing, AirDefense
Time: 8:30 - 17:00 (Madrid)

This session will look at the current and future generation of wireless attack tools. This set of attack tools out on the Internet can damage, destroy, and infiltrate most wireless networks. This session will enable network and security administrators of organizations to build defenses and strategies against attacks and wireless network breaches or infections.

Tutorial F6 *Using the Certification and Accreditation Process to Manage Enterprise Risk*
Speaker: Dr. Ron Ross, National Institute of Standards and Technology and Dr. Julie Meehan, Hatha Systems
Time: 8:30 - 17:00 (Castilian)

This tutorial provides an in depth look at the process of certification and accreditation of information systems as a critical activity in managing enterprise risk. The fundamental concepts of security certification and accreditation as described in NIST Special Publication 800-37 will be discussed in the context of an integrated risk management framework. The integrated risk framework includes the principal components of an enterprise information security program to include categorizing the information system according to system criticality/sensitivity, selecting appropriate security controls (i.e., safeguards and countermeasures) for the system, determining security control effectiveness, and determining residual risk to the enterprise's mission or business case. Each phase of the NIST four-phase certification and accreditation process will be described as well as the roles and responsibilities of individuals within the enterprise participating in the process. The tutorial also examines the U.S. Department of Defense approach to certification and accreditation. Upon completion of the tutorial, attendees will have a fundamental understanding of the major components of an information security program, how the certification and accreditation process fits into the program, and what types of information are required by authorizing officials to make credible risk-based decisions on whether to place information systems into operation or continue their operation.

Tutorial F7 *Acquisition and Analysis of Large Scale Network Data V.3*
Speaker: Dr. John McHugh, Dalhousie University
Time: 8:30 - 17:00 (Miramar South)

With the advent of low cost mass storage devices and inexpensive computer memory, it has become possible to collect and analyze large amounts of network data covering periods of weeks, months, or even years. This tutorial will present techniques for collecting and analyzing such data, both from network flow data that can be obtained from many routers or derived from packet header data and directly from packet data such as that collected by TCPDump, Ethereal, and Network Observer. This version of the course will contain examples from publicly available packet data such as the Dartmouth Crawdad wireless data repository and will deal with issues such as the acquisition of data in IP-unstable environments such as those involving DHCP. Because of the quantity of the data involved, we develop techniques, based on filtering of the recorded data stream, for identifying groups of source or destination addresses of interest and extracting the raw data associated with them. The address groups can be represented as sets or multisets (bags) and used to refine the analysis. These can be used to partition incoming traffic into that which might be legitimate and that which is probably not since it is not addressed to active systems. Further analysis of the questionable traffic develops smaller partitions that can be identified as scanners, DDoS backscatter, etc. based on flag combinations and packet statistics. Traffic to and from hosts whose sources appear in both partitions can be examined for evidence that its destinations in the active set have been compromised. The analysis can also be used to characterize normal traffic for a customer network and to serve as a basis for identifying anomalous traffic that may warrant further examination.

Sponsors

ACSAC Steering Committee	ACSA
Marshall Abrams, The MITRE Corporation	Marshall Abrams, The MITRE Corporation (Chair & Treasurer)
Jeremy Epstein, webMethods, Inc.	Jeremy Epstein, webMethods, Inc. (Vice President)
Daniel Faigin, The Aerospace Corporation	Daniel Faigin, The Aerospace Corporation (Secretary)
Steve Rome, Booz Allen Hamilton	Steve Rome, Booz Allen Hamilton (President)
Ron Ross, National Institute of Standards	Steven Greenwald, Independent Consultant
Ravi Sandhu, George Mason University	Harvey Rubinovitz, The MITRE Corporation (Assistant Treasurer)
Christoph Schuba, Linköpings University	Ann Marmor-Squires, The Sq Group (Chair Emerita)
Ann Marmor-Squires, The Sq Group	Mary Ellen Zurko, IBM Corporation
Dan Thomsen, Cyber Defense Agency, LLC	

ACSA had its genesis in the first Aerospace Computer Security Applications Conference in 1985. That conference was a success and evolved into the Annual Computer Security Applications Conference (ACSAC). ACSA was incorporated in 1987 as a non-profit association of computer security professionals who have a common goal of improving the understanding, theory, and practice of computer security. ACSA continues to be the primary sponsor of the annual conference. For more information on ACSA and its activities, please visit `http://www.acsac.org/acsa/`.

ACSAC welcomes ATSEC as an ACSAC Platinum sponsor.

Finally, ACSAC wishes to thank the following organizations for their logistical support.