FINAL PROGRAM

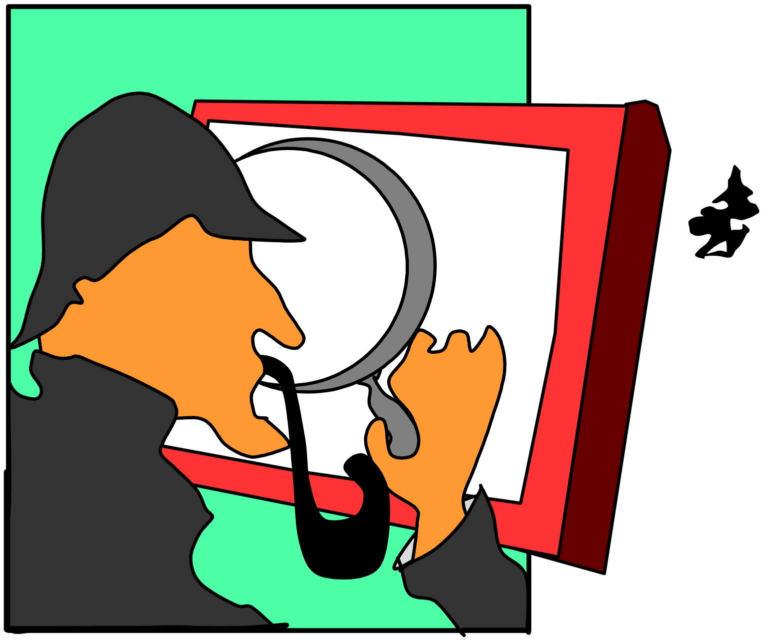
19th Annual Computer Security Applications Conference

Presented by
Applied
Computer
Security
Associates

Applied Computer Security Associates

Nineteenth Annual Computer Security Applications Conference (ACSAC)

Practical Solutions
To Real World Security Problems



December 8-12, 2003
Aladdin Resort & Casino
Las Vegas, NV, USA

ABOUT THE SPONSOR:
APPLIED COMPUTER SECURITY ASSOCIATES (ACSA)

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.

In 1989, ACSA began the **Distinguished Practitioner Series** at the annual conference. Each year, an outstanding computer security professional is invited to present a lecture of current topical interest to the security community.

In 1991, ACSAC began the **Best Paper by a Student Award**, presented at the Annual conference. This award is intended to encourage active student participation in the conference. The award winning student author receives an honorarium and all conference expenses. Additionally, our **Student Conferenceship** program assists selected students in attending the Conference by paying for the conference fee and tutorial expenses. Applicants must be undergraduate or graduate students, nominated by a faculty member at an accredited university or school, and show the need for financial assistance to attend this conference.

An annual prize for the **Outstanding Paper** has been established for the Annual Computer Security Applications Conference. The winning author receives a plaque and an honorarium. The award is based on both the written and oral presentations. The award at the 18th Annual Conference (in 2002) went to Matthew M. Williamson for his paper, **“Throttling Viruses: Restricting Propagation to Defeat Malicious Mobile Code.”**

The **Marshall D. Abrams Invited Essay** was initiated by ACSA in 2000 to stimulate development of provocative and stimulating reading material for students of Information Security, thereby forming a set of Invited Essays. Each year's Invited Essay addresses an important topic in Information Security not adequately covered by the existing literature.

The 2003 ACSAC continues the **Classic Papers** feature begun in 2001. The classic papers are updates of some of the seminal works in the field of Information Security that reflect developments in the research community and industry since their original publication.

ACSA continues to be committed to serving the security community by finding additional approaches for encouraging and facilitating dialogue and technical interchange. In the past, ACSA has sponsored small workshops to explore various topics in Computer Security (in 2000, the Workshop on Innovations in Strong Access Control; in 2001, the Workshop on Information Security System Rating and Ranking; in 2002, the Workshop on Application of Engineering Principles to System Security Design). In 2003, ACSA became the sponsor of the already established New Security Paradigms Workshop (NSPW). ACSA also maintains a Classic Papers Bookshelf that preserves seminal works in the field and a web site focusing on Strong Access Control/Multi-Level Security (www.sac-tac.org).

ACSA is pleased to present a **Works In Progress (WIP) session** on Wednesday afternoon. The session is meant to serve as a forum for introducing new ideas, reporting on ongoing work that may or may hot be complete, and stating positions on controversial issues or open problems.

For more information on ACSA and its activities, please visit www.acsac.org/acsa/. ACSA is always interested in suggestions from interested professionals and computer security professional organizations on other ways to achieve its of encouraging and facilitating dialogue and technical interchange.

To learn more about the conference, visit the ACSAC web page at

http://www.acsac.org

To be added to the Conference Mailing List, visit us on the World Wide Web at

http://www.acsac.org/acsac-join.html

For questions, contact the committee members using the following E-mail addresses:

General_chair@acsac.org
CaseStudies_chair@acsac.org
Panel_chair@acsac.org
Program_chair@acsac.org

Publicity_chair@acsac.org
Student_chair@acsac.org
Tutorial_chair@acsac.org

If electronic contact is not possible, please write to ACSAC, 2906 Covington Rd, Silver Spring, MD 20910-1206, USA.

CONFERENCE AND REGISTRATION INFORMATION

WELCOME TO ACSAC 19

Computers have become commonplace and users increasingly have the expectation that their information will be protected. World events have also demonstrated the importance of protecting information. As computer security professionals, our role is critical. Conferences such as ACSAC play a key role in keeping us up to date on advances in our profession and serve to provide an avenue of technical interchange that is vital.

We all face continued threats to our notion of privacy and security. Our information networks are routinely processing private, proprietary, sensitive, classified, and critical information. We are faced with balancing the addiction to information and instantaneous information exchange with the need to secure that information and to ensure its integrity. Achieving our security goals compels the application of maturing computer security technology to new and existing systems throughout their life cycles.

This conference provides you with the ability to explore technology applications in complementary aspects: policy issues and operational requirements for both commercial and government systems; hardware and software tools and techniques being developed to satisfy system requirements; and specific examples of systems applications and implementations. The conference also provides two days of tutorials that allow you to keep up to date with technology and to sharpen your technical edge.

We thank you for coming to the 19th ACSAC and we hope that you find the conference valuable.

ON-SITE CONFERENCE REGISTRATION & INFORMATION DESK HOURS

The Conference Registration and Information Desk will be located next to the Diamond 1 Meeting Room and staffed during the hours listed below. The Registration and Information Desk also serves as the conference “Lost and Found Center” and is the location of the Conference Message Board.

Sunday, December 7th	6:00 – 8:00 PM
Monday, December 8th	7:30 – 11:30 AM 1:00 – 5:00 PM
Tuesday December 9th	7:30 – 11:30 AM 1:00 – 4:30 PM 6:00 – 8:00 PM
Wednesday and Thursday (December 10th and 11th)	7:30 – 11:30 AM 1:00 – 5:00 PM
Friday, December 12th	7:30 AM– 12:00 PM

ALADDIN TELEPHONE NUMBERS

To contact guests or get other information:

- From the US or Canada, call 702-785-5555.
- From Mexico, call 001-888-747-1732 (toll-free).
- From other nations, call 1-702-785-5555.

CONFERENCE COMMITTEE

Conference Chair:	Daniel Faigin *The Aerospace Corporation*	Multimedia/Proceedings:	Art Friedman *National Security Agency*
Program Chair:	LouAnna Notargiacomo *The MITRE Corporation.*	Site Arrangements:	Meg Weinberg *Mitretek Systems, Inc.*
Program Co-Chair:	Daniel Thomsen *Tresys Technology*	Special Interest Liaison:	Jeremy Epstein *webMethods, Inc.*
Program Co-Chair: (Europe)	Christoph Schuba *Sun Microsystems, Inc.*	Registration:	Edward A. Schneider *Institute for Defense Analyses*
Recording Secretary:	David Chizmadia *Promia, Inc.*	Web Advisor	Robert H’ obbes’ Zakon *Zakon Group LLC.*
Treasurer (Jan-Aug):	Kenneth Eggers *Cygnacom Solutions, Inc.*	Publicity Chair:	Elizabeth A. Foreman *Mitretek Systems, Inc.*
Treasurer (Aug-Dec):	Edward A. Schneider *Institute for Defense Analyses*	Conference Chair Emerita/ ACSA President	Dee Akers *The MITRE Corporation*
Panel/Forum Chair:	Jody Heaney *The MITRE Corporation*	Conference Chair Emerita/ ACSA Vice President	Ann Marmor-Squires *Northrop Grumman*
Tutorial Chair:	Daniel Faigin *The Aerospace Corporation*	ACSA Chair/ ACSA Treasurer	Marshall Abrams *The MITRE Corporation*
Student Awards Chair:	Andre Luiz Moura dos Santos *The Georgia Institute of Technology*	ACSA Communications	Jay J. Kahn *The MITRE Corporation*
Case Studies Chair:	Steve Rome *Booz Allen Hamilton*	SIGSAC Issues Workshop Coordinator	Harvey H.Rubinovitz *The MITRE Corporation*

CONFERENCE LOCATION

CONFERENCE LOCATION

ACSAC 19 is being held in Las Vegas, NV, USA, at the Aladdin Resort & Casino, which is located 2 miles from the McCarran International Airport at 3667 Las Vegas Blvd. South, which is south of Flamingo Road and just north of Harmon Avenue. It's across from the Bellagio and next door to the Paris Hotel.

The Aladdin Resort & Casino features two 4,500-square-foot heated outdoor pools, a 7,000-seat theater; a full-service spa along with fitness equipment, saunas, and steam rooms; the Desert Passage mall with over 130 shops and more than 20 restaurants; a Business Center; and two wedding chapels.

The Aladdin Resort & Casino has 2,567 rooms ranging from 450 to 1,250 square feet. Each room has two telephones, a desktop computer, and a modem port with CAT-5 computer cables for high-speed Internet access. The price for using these capabilities is $9.95 per day (24 hours).

A Business Center is located on the Meeting and Convention floor at which you can get photocopies and print-outs and send or receive packages and faxes.

Guests do not have to pass through the casino to reach their rooms and the conference facilities are located on a floor separate from the casino.

MEALS AND SPECIAL DIET REQUESTS

The Conference Committee has selected lunch menus that we hope everyone will enjoy. For individuals who have special dietary needs, we have arranged to offer a vegetarian meal at lunch that will feature some combination of pasta, vegetables, and/or fruits. If you have requested a special meal, please check your registration packet to ensure that your lunch tickets indicate your dietary request. If there are problems, please contact the Conference Registration desk.

SAFETY

The Aladdin Resort & Casino is located on the Las Vegas Strip where guests can walk or use shuttle buses, city buses, and trolleys to go to and return from the various hotels and casinos.

The Las Vegas Metropolitan Police Department has the following tips for visitors:

- In crowded areas or situations, keep your purse or wallet close to your body.
- Avoid carrying large amounts of cash or wearing flashy jewelry. Carry only what you will need for the day or evening. Leave valuables (e.g., credit cards, airline tickets) in your room safe.
- Make sure your family or friends have contact numbers for you while you are in Las Vegas.

TAXES

Clark County has a sales tax of 7.25 percent. A lodging tax of 9 percent is charged for each night. The rental car tax is 6 percent. Hotel shows charge a 10-percent entertainment tax.

LOCAL GROUND TRANSPORTATION

TAXI: Las Vegas has three major cab companies:

- ABC Union (702) 736-8444
- ACE (702) 873-2227
- Whittlesea Blue Cab (702) 384-6111

Basic fares are $2.30 for the first mile and $1.80 each additional mile. Trips to the airport incur a $1.20 surcharge.

Expect to pay about $10-$11 one way from a Strip hotel/casino to the airport.

LIMOUSINE: Three major limousine services are available:

- Ambassador Limo (702) 362-6200
- Bell Trans (702) 385-5466
- Presidential Limo (702) 731-5577

Limousine service is about $40-$55 per hour. The limousine services also serve the airport.

PUBLIC TRANSPORTATION: Citizens Area Transit

Buses run every 7-10 minutes on the Strip. The fare is $2.00 on the Strip and $1.25 elsewhere. Exact change is required and transfers are free. CAT buses serve other Las Vegas routes from 5:30 am to 1:30 am for a fare of $1.00. Call CAT at (702) 228–7433 for schedule information.

Air-conditioned trolleys also run on the Strip every 20 minutes for a charge of $1.65 (exact change). More information can be obtained by calling (702) 382-1404.

AIRPORT SHUTTLES: Several shuttle buses operate 24/7 between the Strip hotels/casinos and the airport—for example:

- Bell Transport: 702: 739-7990/800-274-7433, $4.25
- CLS Transportation: 702-740-4545, $4.00
- Gray Line: 702: 384-1234/800-634-6579, $4.00

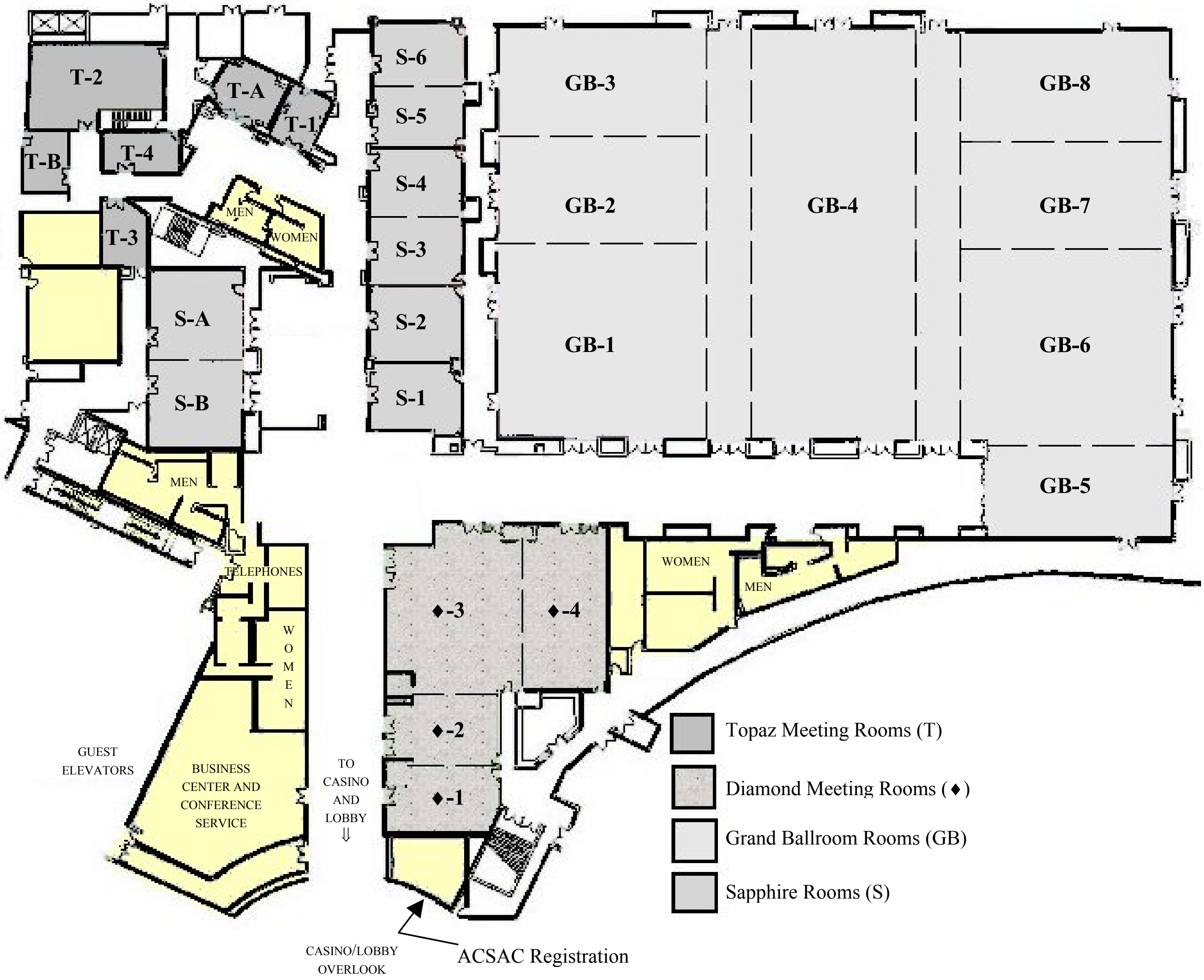
The above prices are for one-way trips per person (and may be subject to change). Be sure to ask whether round-trip fares are available and what you must do to call for a pick-up at the hotel to the airport (some shuttle services may require 24-hours notice).

PARKING: The Aladdin Resort & Casino provides free parking for its guests. Other hotel and commercial garages have ample parking at an average rate of $1-$2 per hour.

MESSAGE BOARD

Conference participants may leave messages to other participants at the Message Board located at the Registration desk. Please have Conference non-participants who need to get a message to you to call your room at your hotel and leave a voice-mail message for you or call you directly at your cell phone before or after the Conference sessions or during the half-hour breaks between sessions.

HOTEL MAP



Room	Activities	Room	Activities
Sapphire 1 (S-1)	Tutorials M1, T5	Diamond 3 (♦-3)	Technical Track B
Sapphire 2 (S-2)	Tutorial M2. SIGSAC Workshop.	Diamond 4 (♦-4)	Technical Track A, Works In Progress
Sapphire 3 (S-3)	Tutorials M3, T7, T8	Grand Ballroom 5 (GB-5)	Case Studies Track
Sapphire 4 (S-4)	Tutorials M4, T6		
Grand Ballroom 1 (GB-1)	Tutorial and Conference Lunches, Conference Dinner, Plenary Sessions, Breaks	Outside Diamond 1 (♦-1)	ACSAC Registration

TUTORIAL PROGRAM

Tutorials At-A-Glance

	Monday, December 8, 2003
M1	**Information System Security Basics** Dr. Steven J. Greenwald, *Independent Consultant* 8:30 AM to 5:00 PM Sapphire 1
M2	**Network Security Protocols: Theory and Current Standards** Dr. Radia Perlman, *Sun Microsystems* and Mr. Charlie Kaufman, *Microsoft Corporation* 8:30 AM to 5:00 PM Sapphire 2
M3	**Distributed Denial of Service Attacks: Background, Diagnosis and Mitigation** Dr. Sven Dietrich and Dr. John McHugh, *CERT Research Center* 8:30 AM to 5:00 PM Sapphire 3
M4	**The Worm & Virus Threat** Mr. Dan Ellis, *MITRE* and Dr. Nicholas Weaver, *UC Berkeley* 8:30 AM to 5:00 PM Sapphire 4

	Tuesday, December 9, 2003		
T5	**Web Application Security** Mr. David Wichers, *Aspect Security* 8:30 AM to 5:00 PM Sapphire 1		
T6	**Golden Rules of Secure Software Development** Dr. Holger Peine, *Fraunhofer IESE Research Institute* 8:30 AM to 5:00 PM Sapphire 4		
T7	**Information Assurance in the US Department of Defense** Mr. Timothy Lelesi & Mr. Charles Lavine *The Aerospace Corporation* 8:30 AM to 12:00 PM Sapphire 3	T8	**Computer and Intrusion Forensics** Prof. George Mohay *Queensland University of Technology* 1:30 PM to 5:00 PM Sapphire 3

Tutorial Lunches

Attendees enrolled in ACSAC Tutorials are provided lunch on the day of their tutorial in Grand Ballroom 1. Please note that lunch is included in both the full day and the half-day tutorial fees.

Tutorial Materials

Although everyone attending a tutorial will be provided a copy of the materials used by the instructor, only those who pre-register for the tutorial will be guaranteed the tutorial materials at the beginning of the tutorial instruction.

Please note that the tutorial registration fees are for tutorials only; registration for the technical portion of the Conference is separate.

Tutorial Evaluations

At the back of each tutorial notes handout, you will find a Tutorial Evaluation form. Please complete this form and return it to the box at the Tutorials Registration Desk next to the Diamond 1 Meeting Room.

You may also mail your completed evaluation forms to Daniel Faigin, ACSAC Tutorial Chair, The Aerospace Corporation, Mail Stop MI/055, P.O. Box 92957, Los Angeles, CA 90009-2957.

TUTORIAL PROGRAM

M1
Monday, 12/8/2003
8:30 AM to 5 PM
Sapphire 1

Information System Security Basics

Dr. Steven J. Greenwald
Independent Consultant

Designed for the person who is new to the field of Information Systems Security, this is an intensive one-day survey of the most important fundamentals of the field. It is designed to bring students "up to speed" on important basic issues, and otherwise fill fundamental gaps in their knowledge. Therefore, its emphasis is mostly historical in nature, and not necessarily topical. However, it contains material that every effective practitioner in our field needs to know.

The ideal student is someone who is either entering the field for the first time, needs a refresher regarding the basics, or is starting to prepare for the CISSP exam. This is a high-speed, low-drag course that covers a very broad range of material. Each student will be given a textbook, and an annotated bibliography of seminal papers and reports (most available on the web) that are covered during the tutorial and which may be used for future study and reference. A major goal of this tutorial is that the student should be able to effectively understand, research, and apply such material when it is later encountered.

About the Instructor:

Dr. Steven J. Greenwald is an independent consultant in the field of Information Systems Security and he specializes in distributed security, formal methods, security policy modeling, resource-based security and related areas. His work has included organizational security policy consulting, evaluation, training, and auditing. He is a Research Fellow at Virginia's Commonwealth Information Security Center (CISC) and is a member of the adjunct faculty at James Madison University's Computer Science department where he teaches in their graduate INFOSEC program (a National Security Agency-designated Center of Academic Excellence in Information Security Assurance). Dr. Greenwald was formerly a computer scientist in the Formal Methods Section of the U.S. Naval Research Laboratory, and he is past General Chair and past Program Chair of the New Security Paradigms Workshop (NSPW). Dr. Greenwald earned his Ph.D. degree in Computer and Information Science from the University of Florida (with a dissertation in the field of information systems security).

M2
Monday, 12/8/2003
8:30 AM to 5:00 PM
Sapphire 2

Network Security Protocols: Theory and Curent Standards

Radia Perlman, *Sun Microsystems, Inc.*, and Charlie Kaufman, *Microsoft Corporation*

This tutorial covers the concepts addressed in network security protocols and describes the current standards. It approaches the problems first from a generic conceptual viewpoint, covering the problems and the types of technical approaches for solutions. For example, how would encrypted email work with distribution lists? What are the performance and security differences in basing authentication on public key technology versus secret key technology? What kinds of mistakes do people generally make when designing protocols?

Armed with a conceptual knowledge of the toolkit of tricks that allow authentication, encryption, key distribution, etc., the instructors describe the current standards, including Kerberos, S/MIME, SSL, IPsec, PKI, and web security.

About the Instructors:

Dr. Radia Perlman is a Distinguished Engineer at Sun Microsystems, Inc. She also teaches network security protocols at Harvard University. She is known for her contributions to bridging (spanning tree algorithm) and routing (link state routing) as well as security (sabotage-proof networks). She is the author of *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols* (Addison-Wesley, 1999), and co-author of *Network Security: Private Communication in a Public World* (Prentice Hall, 2002). She is one of the 25 people whose work has most influenced the networking industry, according to *Data Communications Magazine*. She has a B.S. and M.S. in Mathematics and a Ph.D. in Computer Science from MIT. As the inventor of many of the algorithms that make switching and routing robust and efficient, she holds about 50 patents.

Mr. Charlie Kaufman recently joined Microsoft as Security Architect for the Common Language Runtime Group. He is co-author of the book, *Network Security: Private Communication in a Public World* (Prentice-Hall, 2002). He served on the National Academy of Sciences expert panel whose members wrote the book, *Trust In Cyberspace*. He is currently editor of the new Internet Key Exchange (IKEv2) protocol document for the IP Security Working Group (IPsec) of the IETF and also serves on the Internet Architecture Board. He has contributed to a number of IETF standards efforts, including chairing the Web Transaction Security Working Group. He was previously a Distinguished Engineer at IBM where he was Chief Security Architect for Lotus Notes and Domino and, before that, Network Security Architect for Digital. He holds over 25 patents in the fields of computer security and computer networking.

M3
Monday, 12/8/2003
8:30 AM to 5:00
Sapphire 3

Distributed Denial of Service Attacks: Background, Diagnosis and Mitigation

Dr. Sven Dietrich and Dr. John McHugh
CERT Research Center

In the beginning, security was equated to confidentiality and it was considered better for a system to fail than to leak protected information. As the field matured, it became acceptable to give equal weight to integrity and availability. Concurrently, attackers realized that reducing the utility of computing systems to authorized users could be as effective as compromising sensitive information. Now denial-of-service attacks that exhaust processing or communication resources have become commonplace.

The tutorial traces the development of denial-of-service attacks from early, machine-crashing exploits to attacks that exploit server vulnerabilities or protocol pathologies to the present-day, distributed-denial-of-service (DDoS) attacks. Self imposed denial-of-service attacks in which a system administrator suspends a necessary service in the face of a real or threatened attack are also considered.

A substantial portion of the tutorial is devoted to understanding DDoS attacks and developing appropriate responses. The instructors also survey current research that may lead to ways of thwarting such attacks in the future.

About the Instructors:

Dr. Sven Dietrich is a member of the technical staff at the CERT® Research Center where he does research in survivability and network security. His work has included intrusion detection, distributed denial-of-service analysis, and the security of Internet Protocol (IP) communications in space. He was a senior security architect at the NASA Goddard Space Flight Center and has taught Mathematics and Computer Science at Adelphi University. His research interests include computer security, cryptographic protocols, and quantum cryptography. Dr. Dietrich has a Doctor of Arts degree in Mathematics, an MS degree in Mathematics, and a BS degree in Computer Science and Mathematics from Adelphi University.

Dr. John McHugh is a senior member of the technical staff at the CERT® Research Center where he does research in survivability, network security, and intrusion detection. He was a professor and former chairman of the Computer Science Department at Portland State University. His research interests include computer security, software engineering, and programming languages. Dr. McHugh received his PhD degree in Computer Science from the University of Texas at Austin. He has an MS degree in Computer Science from the University of Maryland and a BS degree in Physics from Duke University.

M4
Monday, 12/8/2003
8:30 AM to 5:00 PM
Sapphire 4

The Worm & Virus Threat

Daniel Ellis, ***The MITRE Corporation*****, and Nicholas Weaver,** ***University of California Berkeley***

Mobile malicious code (mobile malcode) has resulted in the loss of tens of billions of dollars to the international economy. Mobile malcode is a significant and increasing threat: First, many instances of such code could have caused greater damage than they did. Second, advancements in malcode technology allow far more potent attacks. Third, the vulnerabilities that pervade our infrastructure and modern life are not being adequately removed but are instead becoming more tightly coupled. And, fourth, users and economies are becoming more dependent on fragile infrastructures.

This tutorial discusses the different types of mobile malcode, including viruses and network worms. The focus is more on the latter since the antivirus industry offers reasonably robust defenses against viruses but much poorer defenses against worms. The tutorial presents the history of worms and viruses, the anatomy of malicious malcode, what postures and countermeasures help mitigate the threat, and an overview of current efforts to combat the threat. A detailed analysis of several examples of contemporary mobile malcode is also presented.

Students will gain an understanding of what worm and virus threats are, why these threats exist, what can be done now to help protect their organizations from these threats, and the research areas which might offer substantial protection in the future.

About the Instructors:

Mr. Dan Ellis is a Ph.D. student at George Mason University and a researcher at MITRE. His interests are in information security, intrusion detection, and malicious code. His research is focused on developing defensive postures and countermeasures that are adequate to combat the worm threat in an enterprise setting.

Mr. Nicholas Weaver is currently completing his Ph.D. at the University of California at Berkeley. His research interests involve FPGA (Field Programmable Gate Arrays) and computer security. His FPGA work is focused on high performance applications, alternate FPGA architectures, and performance-enhancing FPGA tools. His security work has focused on the threats of high-speed worms and other Internet-scale attacks, and automatic, network level defenses to counter these threats.

T5
Tuesday, 12/9/2003
8:30 AM to 5:00 PM
Sapphire 1

Web Application Security

Mr. David Wichers
Aspect Security

The security of an organization's web applications is critical to a successful online presence. In fact, for some organizations, particularly e-commerce and financial organizations, the security of their web sites may be the most important IT security issue that they are facing today. Unfortunately, the security of their custom web applications is frequently an organization's weakest area.

Most developers learn what they know about security on the job—usually by making mistakes. This tutorial focuses on the most common application security problems facing customized web applications today. It describes the most common vulnerabilities present in today's web applications and practical techniques for identifying and removing such vulnerabilities from web applications.

This course start with material designed to raise awareness of just how insecure most web applications are. The tutorial then demonstrates how hackers are able to attack web applications and what some of the common vulnerabilities are. The next modules detail a number of specific security areas. The instructor discusses the foundational principles, describes best practices, and reviews code examples of design patterns for solutions.

About the Instructor:

Mr. David Wichers is the Corporate Operations Officer (COO) of Aspect Security, a company that specializes in web application security. Mr. Wichers has over fourteen years of experience in areas such as application security, security architectures, secure design, database security, multilevel security, and security testing. He has been involved in the design and development of trusted operating systems, trusted databases, secure routers, secure guards, and large integrated systems for a wide variety of Government customers. Mr. Wichers has a BS in Computer Systems Engineering from Arizona State University and a Masters degree in Computer Science from the University of California at Davis.

T6
Tuesday, 12/9/2003
8:30 AM to 5:00 PM
Sapphire 4

Golden Rules of Secure Software Development

Dr. Holger Peine
Fraunhofer IESE Research Institute

This tutorial teaches important guiding principles to avoid security problems in software design and implementation. No specific technology is taught but general principles of good security engineering are presented. The tutorial starts with a short refresher on what software security is—motivated by the flaws found in a small piece of real-world software (a Java applet for login).

The main part of the tutorial then presents 19 rules of secure software development in the form of Do's and Don'ts. Each rule is illustrated by examples of good and bad practice, and enriched by discussions of inherent problems and possible trade-offs against other goals of software development. The audience is invited to contribute their own experiences and opinions in these discussions. The tutorial continues with some considerations on the general benefits and limitations of such a rule-based approach. The rules part is then rounded off by naming the various sources for the rules and mentioning what other rules have been suggested and why they were not included here.

Finally, the initial example of the login application is revisited and the students are invited to critique the application's design in light of their new knowledge. The tutorial closes with a short direction to security patterns as "the next step" from the general rules.

About the Instructor:

Dr. Holger Peine has studied and worked as a research assistant at the University of Kaiserslautern, Germany, doing research in operating systems, distributed systems, networking, and security. He received a Ph.D. in Computer Science for his award-winning research in run-time support for mobile code, and is the designer and principal implementer of the Ara platform for secure execution of general mobile code. He currently works with the IT security group at the Fraunhofer IESE Research Institute in Kaiserlautern, developing tools for the security evaluation of IT systems and performing security evaluations of software, systems and processes. One focus of his present work are the techniques and tools for the development of secure software.

T7
Tuesday, 12/9/2003
8:30 AM to 12:00 PM
Sapphire 3

Information Assurance in the US Department of Defense

Mr. Timothy Lelesi and Mr. Charles Lavine
The Aerospace Corporation

This tutorial presents an overview of the DoD's approach to Information Assurance (IA). Recently signed DoD policy outlines a new framework for achieving IA, describes responsibilities and procedures for its implementation, and functions as an umbrella under which existing and forthcoming, lower-level, IA-related policy will be integrated. This tutorial describes how DoD Directive 8500.1 and Instruction 8500.2 implement a defense-in-depth approach for IA through the integration of processes and mechanisms--including system certification and accreditation, and IA product acquisition and evaluation.

A goal of this tutorial is to provide a high level understanding of the DoD's new direction, the primary policy, and the processes associated with it.

About the Instructors:

Mr. Timothy Lelesi has worked in the Information Assurance industry for over 10 years, performing vulnerability assessments and system security engineering. Last year, he joined The Aerospace Corporation's Trusted Computer Security Department at which he performs system security engineering and assessments for major space system programs.

Mr. Charles Lavine has worked in the Information Assurance industry for the past 15 years—all at The Aerospace Corporation. He has participated in the NSA's product evaluation programs and performed system security engineering support for space systems. Mr. Lavine is the Director of The Aerospace Corporation's Trusted Computer Systems Department.

T8
Tuesday, 12/9/2003
1:30 to 5:00 PM
Sapphire 3

Computer and Intrusion Forensics

Prof. George Mohay
Queensland University of Technology

Computer forensics relates to the investigation of situations in which there is possible evidence of computer crime. Such evidence is often referred to as digital or electronic evidence. Computer crime in its broad sense includes crimes in which:

- The computer is the target of the crime, or
- The computer is a repository of evidence for a crime (e.g., memos), or
- The computer is the tool by which a crime was committed (e.g., electronic fraud).

This tutorial focuses on the principles which should direct the collection, analysis and presentation of the digital evidence available to an investigator and the techniques that are used to ensure that those principles are met. It is increasingly the case that IT professionals, especially those with a responsibility for computer security, are required to gather, analyze and present evidence of computer crime.

About the Instructor:

Prof. George Mohay is an Adjunct Professor in the Information Security Research Center and at the Queensland University of Technology (QUT) in Brisbane, Australia. He was previously Head of the School of Software Engineering and Computing Science at QUT in 1992 to 2002. His teaching and research interests lie in the areas of concurrency, distributed systems, security, intrusion detection, and computer forensics. He has worked as a visiting researcher while on sabbatical leave at Stanford University in 1981, Loughborough University in 1986, Bristol University in 1990, and the Australian National University in 2000. He received his B.Sc. in 1966 and his Ph.D.in 1970. He supervises Ph.D. and masters students in the areas of security, intrusion detection and computer forensics, and is involved as Chief Investigator in several security- and forensics-related research projects.

ACM SPECIAL INTEREST GROUP WORKSHOP

ISSUES 2003: SECURE WEB SERVICES

Chair: Dr. Harvey H. Rubinovitz

Tuesday, 9 December 2003
8:30 AM - 4:30 PM
SAPPHIRE 2

ACSAC is pleased to once again host a Workshop of the ACM's Special Interest Group on Security, Audit, and Control (SIGSAC). Previous ACSAC attendees have agreed that these workshops provide a useful and exciting forum for information technology professionals – for example, standards developers, software developers, security engineers, security officers – to exchange ideas, concerns, and opinions. This year's workshop focuses on Secure Web Services.

Web Services and XML technologies are changing how people conduct business electronically and they are significantly improving enterprise efficiency. Unfortunately, as with many technologies, good security has not been part of initial product releases.

The security community has taken a great interest in Web Services technology as the amount of transaction processing has increased. The challenge for users of these new technologies is how long they must wait until the Web Services are as secure as the other components to protect against disclosure or unauthorized modification of sensitive information. Several proposed standards are emerging to fill the security gap—for example: WS-Security, Security Assertion Markup Language (SAML), eXtensible Access Control Markup Language (XACML), eXtensible Rules Markup Language (XrML), eXtensible Key Management System (XKMS), and Electronic Business Extensible Markup Language (ebXML). Also being considered are XML encryption and XML signatures. Efforts to secure Simple Object Access Protocol (SOAP) messaging and secure IBM Universal Description, Discovery and Integration (UDDI) management are also ongoing.

This year's Workshop focuses on the relationship between Web Services and security, how the technology is being implemented and utilized to encode information from data obtained from local and remote computers today, and the need to facilitate the research and development of the next generation of secure Web Services.

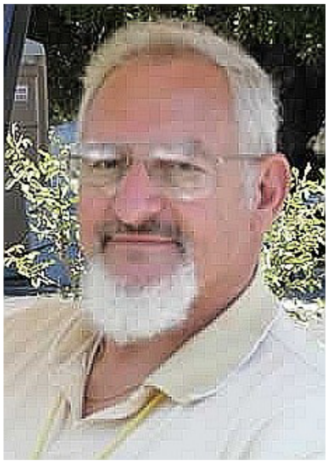
Discussion may also cover the issue of interoperability—especially between evolving specifications at different stages of maturity as well as between competing specifications that provide the same functionality. Some case studies involving Web Services implementations using .Net Framework and/or Java Platforms may also be discussed.

Please note that registration for this Workshop does not include registration for any ACSAC 19 sessions. Workshop participants can continue their discussions at the ACSAC Tutorial lunch for $25.00 in the Grand Ballroom 1.

The SIGSAC Workshop has been a regular feature of ACSAC. To suggest ideas for future workshops, please contact Harvey H. Rubinovitz, Workshop Chairman, directly by mail at The MITRE Corporation, M/S S145, 202 Burlington Road, Bedford, MA 01730; by telephone at (781) 271-3076; or by electronic mail at hhr@mitre.org.

ACSAC INVITED SPEAKERS

2003 DISTINGUISHED PRACTITIONER
CLARK WEISSMAN
NORTHRUP GRUMMAN



Clark Weissman is head of the Information Assurance/Multilevel Security (IA/MLS) Group within Avionics and Systems Software R&D at Northrop Grumman, Information Systems. Clark has 47 years of experience in secure systems research, development, and management. He currently is Principal Investigator of a DARPA-funded R&D program on "Security/Trust as a Polymorphic Computing Architecture Constraint" that is formally modeling a new cryptographic approach to building trusted avionics systems and MLS-PCA that are responsive to the DOD Joint Vision for 2020 (JV2020). He is leading an internal IRAD project to implement a prototype of the MLS-PCA model using a Grid Computing network to simulate the thousands of avionics processors involved.

Prior to joining Northrop Grumman in 2000, Clark performed dozens of security tasks for DOD and industry as an independent consultant. He was a Visiting Professor at the Naval Postgraduate School where he lectured on the Flaw Hypothesis Method, he served as Lead Security Developer of the unique Class A1-certified BLACKER MLS appliqué to the Defense Data Network, and he was R&D Division Manager and Chief Technologist at Unisys Defense Systems.

Clark has a long career of public service to his profession—serving on NSA Network Security Working Groups, three National Science Foundation Export Control software panels, and as Chairman or Cochairman of several conferences. He is author of the long-selling LISP1.5 Primer (1968.) and of dozens of professional papers. He holds a BS in Aeronautical Engineering from MIT (1956) and has performed graduate studies at Rutgers, USC, and UCLA.

2003 INVITED ESSAYIST
LANCE SPITZNER
HONEYPOT TECHNOLOGIES, INC.

Lance Spitzner admits that he is a "geek" who constantly plays with computers—especially in the area of network security. Since security is a constantly changing environment, he can practice the tactics that he learned in the US Army where he served for seven years, four of which as an Armor Officer in the Army's Rapid Deployment Force. Following the military, he received his MBA at the University of Illinois, Chicago, and became involved in the world of information security.

His passion is researching honeypot technologies and using them to learn more about information security attacks. He is founder of the Honeynet Project, moderator of the honeypot maillist, author of *Honeypots: Tracking Hackers* (Addison Wesley, 2002), co-author of *Know Your Enemy* (Addison Wesley, 2001), and author of several whitepapers. He has also spoken at various conferences and organizations. When not actively leading the Honeynet Project, Lance consults for Honeypot Technologies, Inc.

In the past several years there has been extensive research into honeypot technologies, primarily for detection and information gathering. However, little research has been done for one of the most dangerous threats—the advanced insider, the trusted individual who knows the internal organization. These individuals are not after your systems: they are after your information. Lance's presentation discusses how honeypot technologies can be used to detect, identify, and gather information on these specific threats.

WEDNESDAY MORNING, DECEMBER 10TH, 2003

8:30 AM – 10:00 AM OPENING PLENARY

Grand Ballroom 1

8:30 AM	**Opening Remarks**	Daniel Faigin, The Aerospace Corporation, USA Conference Chair
8:35 AM	**Welcome to Las Vegas**	Hotel Manager
8:40 AM	**Distinguished Practitioner**	*"MLS-PCA: A High Assurance Security Architecture for Future Avionics"* Clark Weissman, Northrup Grumman Corporation
9:50 AM	**Technical Program Introduction**	Daniel Thomsen, Tresys Technology, USA Program Co-Chair

10:00 AM – 10:30 AM BREAK Grand Ballroom 1

SESSIONS AT A GLANCE

Wednesday, December 10th, 2003

Time	TRACK A Diamond 4	TRACK B Diamond 3	TRACK C Grand Ballroom 5
10:30 AM –12:00 PM	Intrusion Detection I	Network Security	Java Security
1:30 – 3:00 PM	Defensive Information Warfare	Security for Wireless Sensor Networks	Network Management
3:30 – 5:00 PM	Applied Cryptography	Recovery and Forensics	Authentication
5:15 – 6:30 PM	Works In Progress Diamond 4		

Thursday, December 11th, 2003

Time	TRACK A Diamond 4	TRACK B Diamond 3	TRACK C Grand Ballroom 5
10:30 – 12:00 PM	Software Safety and Program Correctness	Classic Papers	Defensive Computer Environment
1:30 – 3:00 PM	Event Correlation	Security Engineering and Management	Cryptography and Analysis
3:30 – 5:00 PM	Enterprise Security	Themes and Highlights of the New Security Paradigms Workshop	Professionalization

Friday, December 12th, 2003

Time	TRACK A Diamond 4	TRACK B Diamond 3
8:30 – 10:00 AM	OS Security	Intrusion Detection II
10:30 – 12:00 PM	Access Control	Miracle Cures and Toner Cartridges: Finding solutions to the Spam Problem

WEDNESDAY, DECEMBER 10TH, 2003

10:30 PM – 12:00 PM 🗣 SESSIONS		
TRACK A **Diamond 4**	**TRACK B** **Diamond 3**	**TRACK C: Case Studies** **Grand Ballroom 5**
Intrusion Detection I **Chair: Christoph Schuba** **Sun Microsystems, USA** ♣ *Bayesian Event Classification for Intrusion Detection* Christopher Kruegel, Darren Mutz, William Robertson and Fredrik Valeur, University of California, Santa Barbara, USA ♣ *Intrusion Detection: A Bio-Informatics Approach* Scott Coull, Joel Branch and Boleslaw Szymanski, Rensselaer Polytechnic Institute, USA; Eric Breimer, Siena College, USA ♣ *A Stateful Intrusion Detection System forWorld-WideWeb Servers* Giovanni Vigna, William Robertson, Vishal Kher and Richard A. Kemmerer, University of California, Santa Barbara, USA	**Network Security** **Chair: John Viega** **Virginia Polytechnic Institute, USA** ♣ *Behavioral Authentication of Server Flows* James P. Early and Carla E. Brodley, Purdue University, USA ♣ *A Multi-View Tool for Checking the Security Semantics of Router Configurations* Reinhard Schwarz and Holger Peine, Fraunhofer IESE Research Institute, GERMANY ♣ *S-ARP: A Secure Address Resolution Protocol* Danilo Bruschi, Alberto Ornaghi and Emilia Rosti, Universita Degli Studi di Milano, ITALY	**Java Security** **Chair: Mike Jacobs** **SRA International, USA** • *Pure Java Server Signature Modules* Peter Lipp, IAIK – Graz University of Technology, AUSTRIA • *Input Validation Filter for Java Servlet* Ikuya Morikawa, Fujitsu Laboratories, JAPAN ▪ *A Novel Approach for Creating Secure Java Based Enterprise Applications* Yekesa Kosuru, Oracle, USA
12:00 PM – 1:30 PM 🍽 LUNCH Grand Ballrooms 1 and 2		
1:30 pm – 3:00 pm 🗣 SESSIONS		
Defensive Information Warfare **Chair: Thomas Daniels** **Iowa State University, USA** ♣ *Design, Implementation and Test of an Email Virus Throttle* Matthew Williamson, Hewlett-Packard Labs, UK ♣ *Efficient Minimum-Cost Network Hardening via Exploit Dependency Graphs* Steven Noel, Sushil Jajodia, Brian O'Berry and Michael Jacobs, George Mason University, USA ♣ *An IP Traceback Technique against Denial-of-Service Attacks* Zhaole Chen and Moon-Chuen Lee, The Chinese University of Hong Kong, CHINA	**PANEL** **Security for Wireless Sensor Networks** **Chair: Ronald Watro** **BBN Technologies, USA** • David Carman, Network Associates Laboratories, USA • Daniel Coffin, BBN Technologies, USA • Bruno Duerte, SRI, USA • Vipin Swarup, The MITRE Corporation, USA	**Network Management** **Chair: Tom Russell** **Booz Allen Hamilton, USA** • *Tools and Techniques for Analyzing Type Enforcement Policies in Security Enhanced Linux* Frank Mayer, Tresys Technology, USA • *High Assurance In-line Network Encryption – A Discussion of Management Requirements in Today's Network Architectures* Stephen Lewis, AEP Systems, USA • *Highly Auditable Self-Service Life-Cycle Management for Electronic Security Credentials* Peter Tapling, USA

Papers marked with a ♣ symbol were anonymously peer-reviewed by four or more reviewers before acceptance.

WEDNESDAY AFTERNOON, December 10th, 2003

3:00 PM – 3:30 PM ☕ BREAK GRAND BALLROOM 1

3:30 PM – 5:00 PM 🗣 SESSIONS

Applied Cryptography

Chair: Vipin Swarup
The MITRE Corporation

- ♣ *An Intrusion-Tolerant Password Authentication System*
  Xunhua Wang and M. Hossain Heydari, James Madison University, USA, and Hua Lin, PFPC Inc., USA
- ♣ *Modeling of Multiple Agent-based Cryptographic Key Recovery Protocol*
  Shinyoung Lim, Sangseung Kang and Joochan Sohn, Electronics & Telecommunications Research Institute, KOREA
- ♣ *Practical Random Number Generation in Software*
  John Viega, Virginia Polytechnic Institute, USA

Recovery and Forensics

Chair: Eugene Spafford
Purdue University, USA

- ♣ *Multi-Version-Data-Objects-Based Attack Recovery of Workflow*
  Meng Yu, Peng Liu and Wanyu Zang, School of Information Sciences and Technology, Pennsylvania State University, USA
- ♣ *Automatic Reassembly of Document Fragments via Context-Based Statistical Models*
  Kulesh Shanmugasundaram and Nasir Memon, Polytechnic University, USA
- ♣ *Automated Analysis for Digital Forensic Science: Semantic Integrity Checking*
  Tye Stallard and Karl Levitt, University of California, Davis, USA

Authentication

Chair: Rick Wilson
National Security Agency, USA

- *Non-Signature Based IDS,*
  Dameon Packer, Mazu Networks, USA
- *Federated Identity in OneHealthPort*
  Ravi Sandhu, NSD Security, USA
- *HYDRA –The Unhackable Server*
  Eric Uner, Bodacion Technologies, Inc., USA

5:15 PM – 6:30 PM 🗣 Works in Progress Diamond 4

Chair: Christoph Schuba
Sun Microsystems, Inc., USA

- *Wireless Intrusion Detection Systems (WIDS)*
  Dragan Pleskonjic, Conwex, Yugoslavia
- *Embedded Monitors for Detecting Intrusions in Cryptographic and Application Protocols*
  Sachin Joglekar, University of North Texas, Denton, USA
- *Counting Accesses in Content Distribution Networks*
  Radu Sion, CERIAS, Purdue University, USA
- *Enhancing Software Tamper-Resistance via Stealthy Address Computations*
  Cullen Linn, University of Arizona, Tucson, USA
- *Cardea: Providing Support for Dynamic Resource Access in a Distributed Computing Environment*
  Rebekah Lepro, NSA Ames, USA
- *Scalable Privilege Management for a Net-Centric World*
  Arnon Rosenthal, The MITRE Corporation, USA
- *Increasing Software Safety: Moving Test Support to the Runtime Image*
  Ronald Finkbine, Indiana University Southeast, USA
- *Intrusion Detection Using Attacker Profiles*
  Ram Dantu, University of North Texas, Denton, USA

Note that the Works In Progress Program is subject to last-minute changes.

Papers marked with a ♣ symbol were anonymously peer-reviewed by four or more reviewers before acceptance.

THURSDAY MORNING, DECEMBER 11TH, 2003

8:30 AM – 10:00 AM **INVITED ESSAYIST PLENARY**
Grand Ballroom 1
Honeypots: Catching the Insider Threat
Lance Spitzner, Honeypot Technologies, Inc.

10:00 AM – 10:30 AM **BREAK GRAND BALLROOM 1**

10:30 AM – 12:00 PM **SESSIONS**

TRACK A **Diamond 4**	**TRACK B** **Diamond 3**	**TRACK C: Case Studies** **Grand Ballroom 5**
Software Safety and Program Correctness **Chair: Meg Weinberg** **Mitretek Systems, Inc., USA** ♣ *Isolated Program Execution: An Application-Transparent Approach for Executing Untrusted Programs* Zhenkai Liang, VN Venkatakrishnan and R. Sekar, Stony Brook University, USA ♣ *How to Unwittingly Sign Non-repudiable Documents with Java Applications* Danilo Bruschi, Davide Fabris, Vincenzo Glave and Emilia Rosti, Universita Degli Studi di Milano, ITALY ♣ *Making Secure TCP Connections Resistant to Server Failures* Hailin Wu, Andrew Burt and Ramki Thurimella, University of Denver, USA	**Classic Papers** **Chair: Dan Thomsen** **Tresys Technology, USA** ♣ *PSOS Revisited* Peter Neumann, SRI, USA ♣ *A Failure to Learn From the Past* Eugene H. Spafford, Purdue University, USA	**Defensive Computer Environment** **Chair: Ray Potter** **CISCO, USA** • *Implementing Vaulting Technology* Alon Cohen, Cyber-Ark Software, Inc., USA • *Model of a Scalable and Secure Electronic Parabanking* Abhilasha Bhargav, CERIAS, Purdue University, USA • *An Approach to Employing Biometrics With No Hardware, No Software, No Training* Peter Tapling, Authentify, USA

12:00 PM – 1:30 PM **LUNCH GRAND BALLROOM 1**

SESSION ETIQUETTE

Please be courteous of others around you during the Tutorial and Conference sessions:

- Please try to enter and exit the session quietly.
- Please mute or reduce the volume of any beepers, cellular telephones, or other beeping devices.
- Please follow the directions of the session chair for asking questions.
- Please try to unwrap any hard candies before a session begins.

Papers marked with a ♣ symbol were anonymously peer-reviewed by four or more reviewers before acceptance.

THURSDAY AFTERNOON, DECEMBER 11TH, 2003

1:30 PM – 3:00 PM 🗣 SESSIONS

TRACK A **Diamond 4**	**TRACK B** **Diamond 3**	**TRACK C: Case Studies** **Grand Ballroom 5**
Event Correlation **Chair: Art Friedman** **National Security Agency, USA** ♣ *Collaborative Intrusion Detection System (CIDS): A Framework for Accurate and Efficient IDS* Yu-Sung Wu, Bingrui Foo, Yongguo Mei and Saurabh Bagchi, Purdue University, USA ♣ *Attack Signature Matching and Discovery in Systems Employing Heterogeneous IDS* Nathan Carey, George Mohay and Andrew Clark, Queensland University of Technology, AUSTRALIA ♣ *Log Correlation for Intrusion Detection: A Proof of Concept* Cristina Abad, Jed Taylor, Cigdem Sengul, William Yurcik and Yuanyuan Zhou, University of Illinois at Urbana-Champaign, and Ken Rowe, SAIC, USA	**Security Engineering and Management** **Chair: Marshall Abrams** **The MITRE Corporation, USA** ♣ *Protecting Personal Data: Can IT Security Management Standards Help?* Giovanni Iachello, Georgia Institute of Technology, USA ♣ *An Editor for Adaptive XML-Based Policy Management of IPSEC* Raj Mohan, Indian Army, INDIA; Timothy E. Levin and Cynthia E. Irvine, Naval Postgraduate School, USA ♣ *Security Design in Online Games* Jeff Yan, Cambridge University, UK	**Cryptography and Analysis** **Chair: Brian Hubbard** **Booz Allen Hamilton, USA, USA** • *Security Patterns* Ed Rodriguez, Booz Allen Hamilton, USA • *Keeping Today's Secrets Secure Tomorrow* Michael LaGasse, MagiQ Technologies, Inc., USA • *Modernization of "As Built" Legacy Cryptography* Bruce Harte, General Dynamics Decision Systems, USA

3:00 PM – 3:30 PM ☕ BREAK GRAND BALLROOM 1

ATTENTION STUDENTS! Did you know…

ACSA offers a **Conferenceship Program** for selected students who need assistance to attend the Annual Computer Security Applications Conference. The Conferenceship Program pays for the conference and tutorial expenses for selected students who would need assistance to attend the conference. Applicants must be undergraduate or graduate students and must be nominated by a faculty member at an accredited university or school.

Four students were awarded conferenceships for ACSAC 19! For ACSAC 20, check the ACSAC web site or contact the Student Awards Chair, Dr. Andre Dos Santos, by email at student_chair@acsac.org for eligibility information.

ACSA also awards a **Best Paper by a Student Award** at each conference. The award includes an honorarium and all conference expenses. The winning paper may have multiple authors but the primary content of the paper must have been developed by students; students must provide written confirmation to the Student Awards Chair that they meet this policy. A student is defined as anyone who has a current course load of at least 9 credit hours or equivalent as explained by the student or who is enrolled in a degree-granting program and is not employed in a professional capacity outside of the university more than 20 hours per week. Check the ACSAC web site's Call For Papers in Spring 2004.

Papers marked with a ♣ symbol were anonymously peer-reviewed by four or more reviewers before acceptance.

THURSDAY AFTERNOON, DECEMBER 11TH, 2003

3:30 PM – 5:00 PM SESSIONS

TRACK A Diamond 4	TRACK B Diamond 3	TRACK C: Case Studies Grand Ballroom 5
Enterprise Security **Chair: Harold Podell** **General Accounting Office, USA**	**PANEL** **Themes and Highlights of the New Security Paradigms Workshop 2003** **Chairs: O. Sami Saydjari, Cyber Defense Agency, USA, and** **Carla Marceau, ATC-NY, USA**	**Professionalization** **Chair: Ken Heist** **General Dynamics Decision Systems, USA**
♣ *Security Analysis of the SAML Single Sign-on Browser/Artifact Profile* Thomas Gross, IBM Research, SWITZERLAND ♣ *Scalable and Efficient PKI for Inter-Organizational Communication* Arne Ansper, Ahto Buldas, Margus Freudenthal and Jan Willemson, Cybernetica, ESTONIA ♣ *A Policy Validation Framework for Enterprise Authorization Specification* Ramaswamy Chandramouli, National Institute of Standards and Technology, USA	♣ *Bringing Security Home: A Process for Developing Secure and Usable Systems* Ivan Flechais, University College London, United Kingdom ♣ *Locality: A New Paradigm for Thinking About Normal Behavior and Outsider Threat* John McHugh, SEI/CERT, USA ♣ *Securing WiFi Nomads: The Case for Quarantine, Examination, and Decontamination* Kevin Eustace, University of California Los Angeles, USA ♣ *Merging Paradigms of Survivability and Security: Stochastic Faults and Designed Faults* John McDermott, US Naval Research Laboratory, USA	• *ISSEP Government Perspective for Certification* Janet Oren, National Security Agency, USA • *ISSEP – The Practitioner View* Christopher Pohl, Booz Allen Hamilton, USA • *ISSEP – New Credentials Support Career-Enhancement Strategies* Dow Williamson, (ISC)^2, USA

5:30 PM – 6:30 PM CONFERENCE RECEPTION
6:30 PM – 8:00 PM CONFERENCE DINNER
} **GRAND BALLROOM 1**

CONFERENCE SURVEYS

During the conference, you will be provided with a conference survey. Please complete this survey and to return it to the Conference Registration Desk or mail it to: Mr. Daniel Faigin, ACSAC Conference Chair, The Aerospace Corporation MS M1/055, P. O. Box 92957, Los Angeles CA 90009-2957 USA

Note: We are looking for constructive criticism. Unfortunately, there is little we can do about speakers. Sometimes someone has a bad day or doesn't resonate with you. We have some discretion concerning invited speakers and tutorial presenters but none concerning authors.

Papers marked with a ♣ symbol were anonymously peer-reviewed by four or more reviewers before acceptance.

FRIDAY, DECEMBER 12th, 2003

8:30 AM – 10:00 AM 🗣 SESSIONS

TRACK A Diamond 4	TRACK B Diamond 3
OS Security **Chair: Dirk Balfanz** **Palo Alto Research Center, USA** ♣ *Goalkeeper: Close-In Interface Protection* Stephen D Wolthusen, Fraunhofer-IGD, GERMANY ♣ *Poly2 Paradigm: A Secure Network Service Architecture* Eric Bryant, James Early, Rajeev Gopalakrishna, Gregory Roth, Paul Williams, Keith Watson, Scott Yost and Eugene Spafford, Purdue University, USA ♣ *Defending Embedded Systems Against Buffer Overflow via Hardware/Software* Zili Shao, Qingfeng Zhuge, Yi He and Edwin Sha, University of Texas at Dallas, USA	**Intrusion Detection II** **Chair: David Chizmadia** **Promia, Inc., USA** ♣ *Experimenting a Policy-Based HIDS Based on an Information Flow Control Model* Jacob Zimmermann, Ludovic Me and Christophe Bidan, Supelec, FRANCE ♣ *An Experience Developing an IDS Stimulator for the Black-Box Testing of Network Intrusion Detection Systems* Darren Mutz, Giovanni Vigna and Richard Kemmerer, University of California, Santa Barbara, USA ♣ *Synthesizing Test Data for Fraud Detection Systems* Emilie Lundin and Erland Jonsson, Chalmers University of Technology, SWEDEN, Hakan Kvarnstrom, Telia Research AB, SWEDEN

10:00 AM – 10:30 AM ☕ BREAK GRAND BALLROOM 1

10:30 AM – 12:00 PM 🗣 SESSIONS

Access Control **Chair: Ed Schneider** **Institute for Defense Analyses, USA** ♣ *Differential Data Protection for Dynamic Distributed Applications* Patrick Widener, Karsten Schwan and Fabian E. Bustamante, Georgia Institute of Technology, USA ♣ *Usable Access Control for the World Wide Web* Dirk Balfanz, Palo Alto Research Center, USA ♣ *Modeling Contexts in the Or-BAC Model* Frederic Cuppens and Alexandre Miege, ENSTB, FRANCE	**PANEL** **Miracle Cures and Toner Cartridges: Finding Solutions to the Spam Problem** **Chair: Michael Clifford** **The Aerospace Corporation** ● Daniel Faigin, The Aerospace Corporation, USA ● Matthew Bishop, University of California, Davis, USA ● Tasneem Brutch, Kaiser Permanente, USA

12:00 PM ADJOURN

12:00 – 6:00 PM (OPTIONAL) VALLEY OF FIRE STATE PARK TOUR

12:15 PM Depart the Aladdin Lobby via chartered bus. A box lunch (sub, chips, cookie, and soda) will be provided.

1:30 – 2:30 PM Stop at the Lost City Museum of Archeology.

At the State Park, we will visit the Visitor's Center, Elephant Rock, Mouse Tank, and Atlatl Rock.

If time permits, we will stop at Ethel Ann's Chocolate Factory before returning to the Aladdin Resort & Casino at 6:00pm.

The cost of the trip is $35.00 per person. Registration is required. Check the Registration and Information Desk for any openings.

Papers marked with a ♣ symbol were anonymously peer-reviewed by four or more reviewers before acceptance.

ACSAC 20

6-10 December 2004
Tucson, AZ, USA

Hilton Tucson El Conquistador
Golf & Tennis Resort

Call for Participation

The 20th ACSAC will be held the week of December 6-10, 2004, in Tucson, Arizona, USA. If you are developing, researching, or implementing practical solutions to problems relating to protecting your commercial enterprise or your country's information infrastructure, consider sharing your experience and expertise at this conference.

We are looking for papers, panels, tutorials, and case studies that address technologies, concerns, and issues like the following:

- Access control models and policies
- Certification and accreditation/product evaluation
- Cryptographic protocols and applied cryptography
- Database security
- Electronic commerce security
- Firewalls and other boundary control devices
- Forensics
- Middleware and distributed systems security
- Modeling and simulation
- Network security
- Operating systems security
- PKI and certificate management
- Risk/vulnerability assessment
- Intrusion detection and security management
- Survivability and denial of service protection
- Security engineering
- Security against malicious mobile code

Specific information on how to submit a paper or idea will be available on the ACSAC web page (below) in early March 2004. Actual paper submissions are typically due by June 1. Direct your questions to the Program Chair at program_chair@acsac.org.

www.acsac.org