ADVANCE
PROGRAM

18th Annual Computer Security Applications Conference

Presented by
Applied
Computer
Security
Associates

ACSA
Applied Computer Security Associates

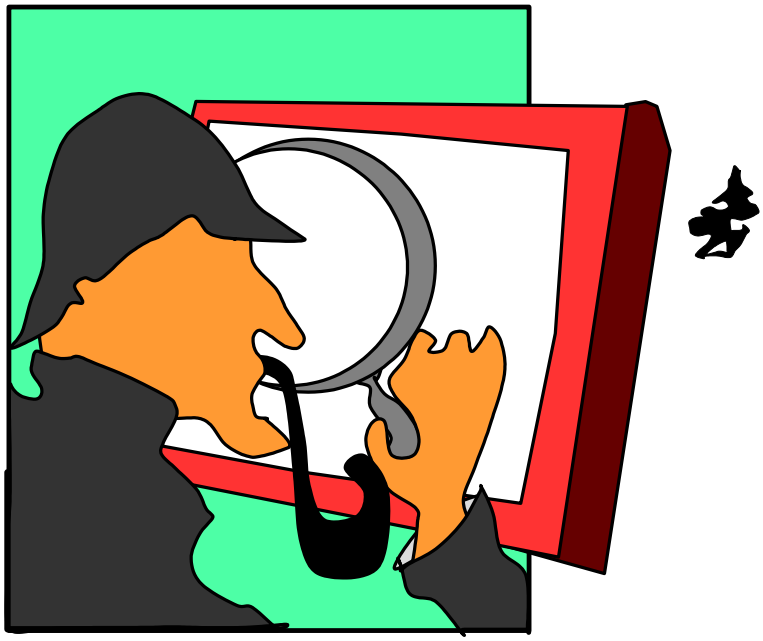
in cooperation with

ACM
Special Interest Group
on
Security, Audit and
Control

acm

Eighteenth Annual Computer Security Applications Conference (ACSAC)

Practical Solutions
To Real World Security Problems



December 9-13, 2002
Alexis Park Resort & Spa
Las Vegas, NV

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 17th Annual Conference (in 2001) went to Eric Montieth for his paper entitled ***"Genoa TIE, Advanced Boundary Controller Experiment."***

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 will address an important topic in Information Security not adequately covered by the existing literature.

The 2002 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 November 2002, ACSA is sponsoring the Workshop on the Application of Engineering Principles to System Security Design (www.acsac.org/waepssd); in 2001, ACSA sponsored the Workshop on Information-Security-System Rating and Ranking (www.acsac.org/measurement). In addition, ACSA has also begun an effort to encourage the use of Strong Access Control (www.sac-tac.org), and explored the creation of a lectureship program. ACSA is always interested in suggestions from interested professionals and computer security professional organizations on other ways to achieve its goals 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 ACSAC, 2906 Covington Rd, Silver Spring, MD 20910-1206, USA.

CONFERENCE AND REGISTRATION INFORMATION

WELCOME TO ACSAC 18

Our world has changed since September 11, 2001, and the role of Computer Security in our world has become increasingly important. 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 it 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 ensure its integrity. Achieving our security goal compels the application of maturing computer security technology to new and existing systems throughout its life cycle.

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 18th 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 in the registration area and staffed during the hours listed below. The information desk also provides the opportunity to purchase tutorial material, proceedings, and other conference items. It also serves as the conference "Lost and Found Center" and is the location of the conference message board.

	OPEN	CLOSE
Sunday, December 8th	6:00 PM	8:00 PM
Monday, December 9th	7:30 AM	11:30 AM
	12:30 PM	5:00 PM
Tuesday, December 10th	7:30 AM	11:30 AM
	12:30 PM	5:00 PM
Wednesday, December 11th	7:30 AM	12:30 PM
	1:30 PM	5:00 PM
Thursday, December 12th	7:30 AM	12:30 PM
	1:30 PM	5:00 PM
Friday, December 13th	7:30 AM	12:00 PM

CONFERENCE COMMITTEE

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

HOTEL INFORMATION

CONFERENCE LOCATION

ACSAC 18 will be held in Las Vegas, NV, USA, at the Alexis Park Resort & Spa (see next page). Las Vegas – "the meadows" – was named by Rafael Rivera, a scout for the Mexican trader Antonio Armijo, who discovered the valley oasis that Las Vegas once was while leading an expedition to Los Angeles in 1829. Las Vegas has a population of over 258, 000 and an elevation of over 2, 000 feet.

Although the city is famous for its gambling casinos, it now has theme hotels that the whole family can enjoy. In addition, it has spectacular natural attractions – such as the Red Rock Canyon National Conservation Area, the Valley of Fire State Park – and is near some man-made wonders like the Hoover Dam.

Visitors to Las Vegas can get their fill of golf, horseback riding, and walking – as well as sightsee via boat, bus, plane, or helicopter.

WEATHER

In the winter, days are mild and sunny in Las Vegas while the nights may have temperatures below freezing. Since Las Vegas' average annual rainfall is about 4 inches, ACSAC 18 attendants may be able to confidently leave their umbrellas at home. The average December has a high of 57 degrees and a low of 33 degrees. Throughout the year, most residents and visitors wear informal business attire but pack a sweater or jacket for the winter months. Sunglasses are encouraged all through the year.

TAXES

Nevada's state sales tax is 7.5 percent. An additional 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.

TRANSPORTATION

The McCarran International Airport is about 2 miles south of the conference hotel and it serves most major airlines.

The Greyhound Lines Inc. is the major bus company serving Las Vegas. The telephone numbers are (702) 384-8009 and (800) 231-2222.

AMTRAK trains also serve Las Vegas:

http://www.amtrak.com/destinations/west.html

1-800-USA-RAIL

LOCAL GROUND TRANSPORTATION

Taxi and limousine services are available from the airport to the "Strip" and other downtown hotels. Expect to pay about $10.00 one way to the conference hotel.

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 $2.20 for the first mile and $1.60 each additional mile. Trips to the airport incur a $1.20 surcharge.

LIMOUSINE: Three major limousine services are available and they also serve the airport:

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

Limousine service is about $35-$55 per hour.

PUBLIC TRANSPORTATION: City Area Transit (CAT)

Buses run every 10-15 minutes, 24 hours a day, 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. Schedule information can be obtained by calling CAT at (702) 228 –7433.

Air-conditioned trolleys also run on the "Strip" every 15 minutes for a charge of $1.50 (exact change). More information can be obtained by calling (702) 382-1404.

RENTAL CARS: The hotel provides free parking for its guests. Other hotel and commercial garages have ample parking at an average rate of $1-2 per hour.

SAFETY

Guests at the Alexis Park Resort & Spa are encouraged to use the free shuttle bus available at the nearby Hard Rock Café and Hard Rock Hotel to get to and from the "Strip." Once on the "Strip," additional shuttle buses, city buses, and trolleys can be taken to specific casino hotels. If you choose to walk to or from the "Strip" (about half a mile from the hotel), do so in a group. You can help by looking out for yourself and others while being street smart:

- As in any downtown area, you should always be aware of your surroundings and be alert for pickpockets or other suspicious individuals.
- As always, use common sense. Remember there is safety in numbers and avoid carrying large amounts of cash or wearing flashy jewelry.

FOR MORE INFORMATION

The source of the information on this and the next page regarding travel to Las Vegas is the *AAA TourBook: Southern California & Las Vegas, 2002 Edition*. (http://www.aaa.com)

The Las Vegas Convention and Visitors Authority can be reached at:

- (702) 892-7575 or 1-877-VISITLV
- http://www.lasvegas24hours.com/index.asp

The Las Vegas Chamber of Commerce can be reached at (702) 735-1616 or http://www.lvchamber.com

HOTEL INFORMATION

CONFERENCE LOCATION

The Alexis Resort & Spa is located 2 miles from the McCarran International Airport at 375 East Harmon Avenue on the corner of Paradise Road and Harmon Avenue. This all-suites hotel is across from the Hard Rock Hotel and 2 blocks from the University of Nevada at Las Vegas. The hotel has 2 stories, 500 units, and exterior corridors; it offers a full-service health club, 3 swimming pools, and a 9-hole putting green. Both on-site and valet parking are available. Although the hotel does not have a casino, guests may board a free shuttle bus to and from the "Strip" from the Hard Rock Hotel or the Hard Rock Café (see map).

The conference takes place entirely in the hotel.

HOTEL REGISTRATION

REGISTER EARLY! Hotel reservations at the conference hotel can be made by contacting the Alexis Park Resort and Spa, 375 East Harmon Avenue, Las Vegas NV 89109.

You may also make reservations by telephone at **800-582-2228.** Although you can register through the Hotel's registration web site: https://reservations.alexispark.com this site does not provide the option to specify the conference rate or your association with the conference. (Note: you may need to use Internet Explorer to access the main hotel web site, although the registration site seems to work with Netscape).

The Conference rate per room for single or double occupancy is $79.00, plus 9 percent lodging tax, per night. Upgraded suites are available for an additional cost.

To get this rate, **you must identify yourself as attending the 18th Annual Computer Security Applications Conference and make your reservation by 14 November 2002**. The Conference rate is guaranteed only for reservations made by November 14. Be sure to obtain a reservation confirmation number.

The hotel requires a **deposit** equal to one night's stay to hold each reservation. The deposit confirms the reservation for the date(s) indicated. Upon check-in, the deposit is applied to the first night of the reserved stay. A personal check, money order, or major credit card may be used to secure your reservation. The deposit must be received no later than 14 days after the reservation was made.

If you must cancel a reservation, the deposit will be refunded in full – provided that you cancel at least 72 hours prior to the expected arrival date. Otherwise, a penalty charge for one (1) night's stay will be levied. Be sure to obtain a cancellation confirmation number. Note also the date and time of your call as well as the name of the person who handled the cancellation.

Hotel parking is free to hotel guests and visitors.

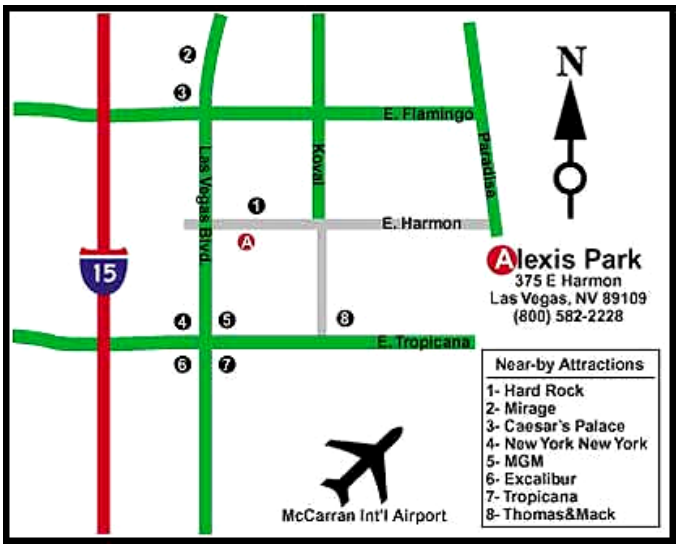
INTERNET ACCESS

The Alexis Park Resort & Spa provides a data port in each suite to which guests may connect their computers.

The hotel also has a Business Center at which guests may access the Internet ($10.00 per half hour) as well as print, fax, or copy documents. The Business Center can be reached by telephone at (702) 796-3340, by facsimile at (702) 796-3354, and by email at apconci@fiax.net. Be sure to confirm the latest rates for the services that the Center provides.

The following web site identifies the cybercafes in the Las Vegas area:

http://www.lasvegas.com/community/cybercafes.html



(ISC)2 SPONSORED EXAMS

For those interested in professional certification, the International Information Systems Security Certification Consortium, Inc., will be holding CISSP and SSCP Exams on Sunday, 8 December 2002, the day before the conference starts, also at the Alexis Park Resort & Spa.

Information about the exams is available at http://www.isc2.org

TUTORIAL PROGRAM

Monday, December 9, 2002	
M1	**Information System Security Basics** Dr. Steven J. Greenwald, *Independent Consultant* 8:30 AM to 5:00 PM
M2	**Understanding Biometric Technology and Its Implementation** Ms. Catherine J. Tilton, *SAFLINK Corp.* 8:30 AM to 5:00 PM
M3	**Denial of Service Attacks: Background, Diagnosis and Mitigation** Dr. Sven Detrich and Dr. John McHugh, *CERT/CC* 8:30 AM to 5:00 PM
M4	**XML Security** Mr. Christian Geuer-Pollmann, *University of Siegen* 8:30 AM to 5:00 PM

Tuesday, December 10, 2002			
T5	**Cryptography and PKI Basics** Dr. Steven J. Greenwald, *Independent Consultant* 8:30 AM to 5:00 PM		
T6	**Mobile and Wireless Security Issues, Threats and Countermeasures** Dr. Tasneem Brutch, *Hewlett-Packard* 8:30 AM to 5:00 PM		
T7	**How to Successfully Assess Business and Automation Risks** Ms. Marianne Emerson *Federal Reserve Board* 8:30 AM to 12:00 PM	**T8**	**Survivable Systems Analysis** Dr. Nancy Mead and Dr. Tom Longstaff *CERT/CC* 1:30 PM to 5:00 PM

TUTORIAL LUNCHES

Students enrolled in ACSAC Tutorials are provided lunch on the day of their tutorial.

TUTORIAL MATERIALS

Although all tutorial attendees 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 lunch is included in both the full-day and the half-day tutorial fee. See the registration form for more information. Please note the tutorial registration fees are for tutorials only; registration for the technical portion of the Conference is separate.

M 1
Monday, 12/9/2002
Full Day

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 our field. It is designed to bring the students up to speed on important basic issues, and otherwise fill fundamental gaps in their knowledge. Therefore, its emphasis will be mostly historical in nature, and not necessarily topical. However, it will contain 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 will be a high-speed low-drag course covering a very broad range of material. Since it is unrealistic to assume that the students can absorb all of this material in a one-day tutorial, each will be given, in addition to a textbook, an annotated bibliography of seminal papers and reports (most available on the web) that will be covered during the tutorial and which they may use 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.

Prerequisites

None.

High-Level Outline

I. Introduction. Overview/refresher of the necessary CS background, common definitions, and historical overview and perspectives.

II. Fundamentals. Covers Identification & Authentication, Access Control, Security Kernels, and Security Models.

III. Practice. Provides a brief overview of Unix and Windows NT Security, as well as common errors (*e.g.*, buffer overflows) and security software.

IV. Cryptography. A brief overview of cryptography, PKI and standards.

V. Distributed Systems. Covers Web security and other aspects of network and distributed system security.

VI. Database Systems. Explores DBMS models and problems.

VII. Conclusions and Questions. Seeing the forest for the trees, professional development options, and if time permits any topical or other areas that may be of particular interest.

About the Instructor:

Dr. Steven J. Greenwald is an Independent Consultant in the field of Information Systems Security specializing in distributed security, formal methods, security policy modeling, resource based security and related areas. He also works with organizational security policy consulting, evaluation, training, and auditing. He is a Research Fellow at Virginia's Commonwealth Information Security Center (CISC) and on the adjunct faculty at James Madison University's Computer Science department teaching in their graduate INFOSEC program (a National Security Agency designated Center Of Academic Excellence in Information Security Assurance). Dr. Greenwald was formerly employed as a computer scientist in the Formal Methods Section of the U.S. Naval Research Laboratory, and is also 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, 12/9/2002
Full Day

Understanding Biometric Technology and Its Implementation

Ms. Catherine J. Tilton
SAFLINK Corp.

This tutorial provides a technical overview of biometric technologies - what they are, how they work, what kinds there are and the characteristics of each, how accuracy is measured - as well as an overview of the considerations for selection and deployment. It also covers the current technical and market trends in terms of applications for the technology, privacy and ethics, biometric standards, and testing/certification.

The role of biometrics in IT security is addressed as is the integration of biometrics with smart cards and PKI. References and sources of further information are provided.

Prerequisites

None. Technical background suggested, but not required.

High-Level Outline

I. Biometrics Overview. The What and How of Biometrics. Accuracy issues. Technology types. Markets and applications. Standards. Privacy and ethics issues.

II. Planning and Engineering a Biometric System. Requirements, alternatives, and design.

III. Summary and References.

About the Instructor:

Ms. Catherine J. Tilton is the Director of Special Projects at SAFLINK Corp., a multi-biometric computer security software company. She also chairs the steering committee of the BioAPI Consortium, and is active in the US Biometric Consortium, the International Biometric Industry Association (IBIA), ANSI X9F4, the Intel/Open Group CDSA Human Recognition Services (HRS) working group, the INCITS M1 committee. She formerly served as technical editor of the Human Authentication API. She has a BS in nuclear engineering from Mississippi State and an MS in systems engineering from Virginia Tech.

M3
Monday, 12/9/2002
Full Day

Denial of Service Attacks: Background, Diagnosis and Mitigation

Dr. Sven Detrich and Dr. John McHugh
CERT/CC

In the beginning, security was equated to confidentiality and it was considered better for a system to fail (or be forced into failure) than to leak protected information. As the field matured, the emphasis changed and concepts such as "Security-*" giving equal weight to integrity and assured service became acceptable. Concurrently, adversaries realized that attacks that reduced the utility of computing systems to authorized users could be as effective as attacks that compromised sensitive information. In the past year, brute force denial of service attacks based on the exhaustion of the victim's processing or communication resources have become commonplace.

The tutorial will trace the development of denial of service attacks from early, machine crashing exploits to attacks that based on the exploitation of server vulnerabilities or protocol pathologies to consume excessive computing resources 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 will also be considered. A substantial portion of the tutorial will be devoted to understanding DDoS attacks and developing appropriate responses. Among the issues to be addressed are preparing for a DDoS attack, recognizing the attack type and probable attack pattern, designing appropriate filter rules to mitigate the attack, and working with upstream providers. We will also survey current research that may lead to ways of thwarting such attacks in the future.

Prerequisites

A basic understanding of IP networking, network protocols, and routing as well as an understanding of computer security fundamentals is required. The tutorial is intended to be useful to system administrators, network administrators and computer security practitioners.

High-Level Outline

I. Fundamentals. Basic networking and routing protocols.

II. Denial of Service. Basic concepts. Vulnerabilities and pathologies. OS support. The jump from DoS to DDoS. Evolution of attack tools.

III. Classes of DDoS tools. What they do. Choices in the attack space. How they work. Currently available tools.

IV. Diagnosis of the problem. How do you know you are under attack. Symptoms in your own operational and system monitoring data. Differentiating between flash crowds and attacks. Advances in research. Inspecting a compromised system. Building a monitoring/traffic capture facility.

V. Mitigation. Recognition of the attack. Attack signatures and attack tool identification. DoS vs. DDoS. Indications of single and multiple sources. Creating countermeasures. Techniques for limiting the damage. Characterizing the attacked resources. Infrastructure changes. Traceback. Filtering. Active response. Strikeback.

VI. Political hurdles. Dealing with your ISP. Dealing with management.

VII. The bright road ahead. DDoS and beyond. Prospects for future advances in attacker tools, Technical, legal, and political mitigation strategies.

About the Instructors:

Dr. Sven Dietrich is a member of the technical staff at the CERT® Coordination 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, but are not limited to, computer security, cryptographic protocols, and quantum cryptography, and he randomly gives presentations and talks on the subject. Dr. Dietrich has a Doctor of Arts degree in Mathematics, a MS degree in Mathematics, and a BS degree in Computer Science and Mathematics from Adelphi University in Garden City, New York.

Dr. John McHugh is a senior member of the technical staff at the CERT® Coordination 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 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.

M4
Monday, 12/9/2002
Full Day

XML Security

Mr. Christian Geuer-Pollmann
University of Siegen

The tutorial will give a short introduction into XML and will explain the W3C standards, "XML Signature" and "XML Encryption," in great detail. It will cover introductions into the "XML Key Management Specification" (XKMS), the "Security Assertion Markup Language" (SAML) and describe how these security mechanisms can be integrated into SOAP to create secure web services.

The "eXtensible Markup Language" (XML) is a standard that describes a syntax for structuring data and documents. In early 1999, W3C and IETF officially launched the XML Signature Working Group to develop an XML compliant syntax used for representing the signature of Web resources and portions of protocol messages. All major vendors of cryptographic software have integrated support for the new XML digital signature format into their products. XML Signatures can sign parts of a document, allowing parties to sign only the relevant portions of a contract. XML Signatures help bring confidence into web transactions. IBM, HP, Microsoft, SUN and the Apache Foundation integrated XML Signatures into their respective SOAP based web service architectures.

In 2001, the W3C started the "XML Encryption" task. The mission of this working group is to develop a process for encrypting/decrypting digital content and to develop an XML syntax used to represent the encrypted content and the information that enables an intended recipient to decrypt it. Encryption enables selective-field-confidentiality for XML data. Together with its twin, XML Signatures, they enable system architects to design applications that provide real end-to-end-security on the application layer.

The "XML Key Management Specification" (XKMS) serves as an XML'ized application protocol to access PKIs and related structures. XKMS enables constrained clients like mobile devices and embedded hardware to outsource security related tasks like certificate validation to trusted hosts, and much more. The "Security Assertion Markup Language" (SAML) is an XML-based tool for exchanging authentication and authorization information in distributed systems, e.g. used by the Liberty Alliance.

Prerequisites

Basic knowledge on cryptography. This tutorial is intended for security people who want to come in touch with XML and the related security specifications.

High-Level Outline

I. Introduction to XML. XML 1.0. DTDs and Schema. Namespaces and Infoset. XSL Transforms. Structured data.

II. Related Security. Network layer vs. application layer security. Why SSL is no help. WYSIWYS problems - "What you see is what you sign"

III. XML Security Standards. . Canonical XML, XML Signature: Forms, Generation, Verification, Multiple Signatures, Syntax, Algorithms, and Security Considerations. XML Signature and SOAP Security. XML Encryption. XML Advanced Electronic Signatures (XAdES). Security Assertions Markup Language – SAML.

IV. Application Scenarios for XML Security. Document Workflow with XML Signature and XML Encryption. Contract Signing with XML Signature. Single-Sign-On with SAML and XML Signature. Credential transfers with SAML.

V. Products for XML Security. An overview to implementations and available products.

VI. Future directions in standardization.

About the Instructor:

Mr. Christian Geuer-Pollmann has a degree in electrical engineering from the University of Wuppertal/Germany, and is currently working on his Ph.D. thesis at the University of Siegen. He created the XML Signature implementation which is now available as part of the Apache XML Project. His main research interest is in encrypting XML. He's maintainer of the "XML Security page" <http://www.nue.et-inf.uni-siegen.de/~geuer-pollmann/xml_security.html>, and has presented a similar tutorial at BSI/GISA. Currently, he's writing a book on XML Security for Morgan Kaufmann Publishers. He actively participated in standardization since 1999, especially in the area of W3C for the standards "XML-Signature Syntax and Processing", "Exclusive XML Canonicalization", "XML-Signature XPath Filter 2.0" and "XML Encryption Syntax and Processing". He's in the program committee for the "2002 ACM Workshop on XML Security", held in conjunction with the Ninth ACM Conference on Computer and Communications Security (CCS-9).

T5
Tuesday, 12/10/2002
Full Day

Cryptography and PKI Basics

Dr. Steven J. Greenwald
Independent consultant

This tutorial is designed for the person who is new to the area of cryptography and Public Key Infrastructure (PKI). It is an intensive one-day survey of the most important areas of cryptography and PKI, designed to bring the students up to speed on important basic issues, and otherwise fill fundamental gaps in their knowledge. It will contain material that every effective practitioner in our field who deals with cryptographic applications needs to know.

The ideal student is someone who knows nothing (or next to nothing) about cryptography and PKI, or needs a refresher regarding the basics. This will be a high-speed low-drag course covering a very broad range of complex material. Since it is unrealistic to assume that the students can absorb all of this material in a one-day tutorial, each will be given, in addition to a textbook, an annotated bibliography of seminal papers and reports (most available on the web) that will be covered during the tutorial and which they may use 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.

Prerequisites

None.

High Level Outline

I. Introduction and Basic Concepts.

II. Conventional Cryptography. Explores classic and modern techniques, common algorithms, and approaches to confidentiality.

III. Public Key Cryptography and Hash Functions. Explores public key cryptography, message authentication and hash functions, algorithms, digital signatures, and authentication protocols.

IV. Public Key Infrastructure (PKI) and Network Cryptography Practice. Explores applications of cryptography such as authentication and email, as well as Internet protocols and web security.

V. Conclusions and Questions.

About the Instructor:

Dr. Steven J. Greenwald is an Independent Consultant in the field of Information Systems Security specializing in distributed security, formal methods, security policy modeling, resource based security and related areas. He also works with organizational security policy consulting, evaluation, training, and auditing. He is a Research Fellow at Virginia's Commonwealth Information Security Center (CISC) and on the adjunct faculty at James Madison University's Computer Science department teaching in their graduate INFOSEC program (a National Security Agency designated Center Of Academic Excellence in Information Security Assurance). Dr. Greenwald was formerly employed as a computer scientist in the Formal Methods Section of the U.S. Naval Research Laboratory, and is also 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).

T6
Tuesday, 12/10/2002
Full Day

Mobile and Wireless Security Issues, Threats and Countermeasures

Dr. Tasneem G. Brutch
Hewlett-Packard

The broadcast nature of the communication medium, and the absence of a fixed topology make communication in mobile/wireless networks vulnerable to illegal access, eavesdropping, and both passive and active intrusions. This includes disclosure of information to unauthorized individuals, modification of previously communicated messages, and falsely claiming the identity of a legitimate user. In order to provide adequate protection against these threats, a good understanding of security issues with various mobile and wireless technologies is needed for the provision of a secure environment. However, with the diversity of mobile and wireless standards and technologies available today, it is difficult to gain a complete understanding of the various mobile/wireless technologies, their limitations.

This tutorial is intended to provide an overview of some of the mobile and wireless technologies available today, the security provisions provided by each of these technologies, their limitations and vulnerabilities, and the available mechanisms, which can be used to protect against attacks and intrusions. Main topics discussed will include the Bluetooth standard, 802.11b (or Wi-Fi), and the Wireless Application Protocol (WAP).

Prerequisites

A general understanding of wireless computer security concepts.

High Level Outline

I. Bluetooth. Overview of the Standard. Security Architecture. Connection Setup. Access Profiles. Device Security. Service Security. Link Level Security. Key management. Encryption. Authentication. Security Limitations. Security Issues.

II. Wireless LANs. The 802.11b (Wi-Fi) Standard. Wireless LAN architecture. Wi-Fi Security Provisions. Open System Authentication. Shared Key Authentication. Access Lists. Service Set Identifier (SSID). Security Limitations and Issues. Security Solutions.

III. Wireless Application Protocol. Specification. Architecture. Wireless Transport Layer Security (WTLS). Security Features. Link Level Security. Connection Management. Cryptographic Attributes and Protocols. WAP Identity Module. WAP Security Issues.

About the Instructor:

Dr. Tasneem G. Brutch received her B.S. in Computer Science and Engineering, and an M.S. in Computer Science, from Texas A&M University. She has a Ph.D. from Texas A&M University in Computer Engineering in the area of wireless communication security. She is currently working for Hewlett-Packard as Security Software Design Engineer on the IDS/9000 intrusion detection product.

T 7
Tuesday, 12/10/2002
Morning

How to Successfully Assess Business and Automation Risks

Ms. Marianne Emerson
Federal Reserve Board

Although risk assessments are essential to information security, there is little guidance on how to do them. This course uses case studies and the methodology in place in the Federal Reserve System1 for more than ten years and to explain in detail how to analyze and measure risks to information and automation resources. The course starts with a study of the loss of two pieces of automation equipment and asks students to identify what was lost and the size of the loss. The study illustrates the difficulty of identifying which safeguards should be implemented when risks have not been assessed. The results of the case study are used as a frame of reference for introducing the elements of the risk assessment model, which are opportunities, threats, potential losses and offsetting safeguards. After walking through the elements hierarchically from less detail to more, the course returns to the case study to apply the model. Practical application of the model lets the students evaluate their level of understanding of it. Through this exercise and the questions it raises, they strengthen their knowledge of the concepts. This knowledge is reinforced through a final case study, whether or not the senior management of a major hotel chain should allow employees to telecommute from regional telework centers.

Prerequisites

A general familiarity with automation such as one would gain by using a PC for word processing and email.

High Level Outline

I. Overview. What good information security requires. Why risk assessments. How to do a risk assessment.

II. Stolen PC and lost PDA case study. Lessons from the case study. Scarcity of risk assessment methodologies.

III. Federal Reserve System Risk Assessment Model. Overview and details. Application of model.

IV. Doing a risk assessment. Challenges. Threat checklists.

V. Application of Model to large hotel chain telecommuting decision.

VI. Wrap-up

About the Instructor:

Ms. Marianne Emerson is the deputy director in the Federal Reserve Board's Division of Information Technology. The division provides automation, statistical, and telecommunications services to the Board and to the Federal Financial Institutions Examination Council. Ms. Emerson spent two years on loan to the Board's Division of Banking Supervision and Regulation as an advisor to the supervisory information technology function and ten years as the Board's information security officer. She has e-banking review experience, having led the first information services review of the firm responsible for automating Security First Network Bank, now the e-banking part of the Royal Bank of Canada. She has also participated in a number of operations reviews of information technology at Reserve Banks. She teaches graduate courses in information security at the R. H. Smith Business School of the University of Maryland. Ms. Emerson holds a Bachelor of Arts from Bryn Mawr College and a Master of Business Administration in finance and a Master of Science in Computer Science from the University of Maryland.

T8
Tuesday, 12/10/2002
Afternoon

Survivable Systems Analysis

Dr. Nancy Mead and Dr. Tom Longstaff
CERT/CC

Increasing societal dependence on large-scale, distributed information systems amplifies the consequences of intrusions and compromises. It is vital that these critical systems survive to provide essential functions even when operating under adverse circumstances. The tutorial objective is to describe practical techniques for survivability analysis and design that attendees can apply in their own environments. In particular, the tutorial introduces the Survivable Systems Analysis (SSA) method developed by the SEI's CERT/CC, as a means to assess and improve survivability and security characteristics of planned or existing information systems. The tutorial will present a case study and more detailed examples of survivability analysis.

Prerequisites

No special prerequisites, general understanding of information security desirable. The tutorial is aimed at analysis of abstract system architectures prior to implementation.

High Level Outline

I. Trends in information security and system survivability concepts. Trends in information security. Formal definition of survivability. Survivability concepts of resistance, recognition, and recovery.

II. The Survivable Systems Analysis Method.The 4-step SSA method, including system definition, essential capability definition, compromisable capability definition, and survivability analysis.

III. SSA Case Study and Examples. How to apply the SSA method. Examination of a prior SSA case study. Detailed examples.

About the Instructors:

Dr. Nancy Mead is the team leader for the Survivable Systems Analysis (SSA) team as well as a senior member of the technical staff in the Networked Systems Survivability Program at the Software Engineering Institute (SEI). She is also a faculty member in the Master of Software Engineering and Master of Information Systems Management programs at Carnegie Mellon University. She is currently involved in the study of survivable systems architectures and the development of professional infrastructure for software engineers. Her research interests are in the areas of software requirements engineering, software architectures, software metrics, and real-time systems. Dr. Mead received her PhD in mathematics from the Polytechnic Institute of New York, and received a BA and an MS in mathematics from New York University.

Dr. Tom Longstaff is a senior member of the technical staff in the Networked Systems Survivability (NSS) Program at the Software Engineering Institute (SEI), where he manages research and development in network security. Publication areas include information survivability, insider threat, intruder modeling, and intrusion detection. Since 1997, Tom has been investigating topics related to information survivability and critical national infrastructure protection. Prior to coming to the Software Engineering Institute, he was the technical director at the Computer Incident Advisory Capability (CIAC) at Lawrence Livermore National Laboratory in Livermore, California. He completed a PhD in 1991 at the University of California, Davis in software environments.

ISSUES 2002: COMPUTER FORENSICS COLLECTING, EXAMINING, PRESERVING, AND ACTING ACM SPECIAL INTEREST GROUP WORKSHOP

Chair: Dr. Harvey H. Rubinovitz

Tuesday, 10 December 2002
8:30 AM - 4:30 PM

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.

In recent years, the number of computer-related crimes has increased. Even if the crime itself has not taken place on the computer, the computer may contain evidence about a crime that has occurred or is about to occur. As the number of people using computers has increased, so has the number of criminals using computer and computer networks. Unfortunately, few investigators are well trained in identifying, investigating, capturing, analyzing, preserving, and processing computer-based evidence.

The security community has taken a great interest in computer forensics technology as the amount of criminal activity has increased in 'cyberspace'. The increasing challenge for investigators is that a physical presence is no longer needed when committing criminal acts nor may there be any physical evidence as there is in a conventional crime. Computer forensics is viewed by the security community as a method of examining, preserving, and acting on computer and network evidence. A number of tools have been developed and are being utilized today.

This year's SIGSAC Workshop will focus on the relationship between computer forensics and security, how the technology is being utilized to obtain meaningful information from data obtained from computer and computer networks today, and the need to facilitate the research and development of a new generation of computer forensic tools and procedures. Forensics data must be located, collected, and analyzed properly. The emphasis will be placed on the information-gathering process and the tools used to collect and analyze forensics data – with any remaining time used to discuss future trends in forensics along with issues from the legal communities.

Given wide interest today in digital forensics, this Workshop provides an excellent opportunity to learn about the field of computer forensics and standards developers' concerns about the topic, and to express your concerns and/or opinions. Send your presentation or discussion proposals to Harvey Rubinovitz, Workshop Chairman (contact information below).

Although there is no charge for attending the workshop, pre-registration is requested. To do so, use the Registration Form or 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.

Please note that registration for this Workshop does not include registration for any ACSAC sessions. Workshop participants can continue their discussions at the ACSAC Tutorial lunch for $25.00. See the Registration Form for details.

ACSAC INVITED SPEAKERS

2002 DISTINGUISHED PRACTITIONER

EARL BOEBERT
SENIOR SCIENTIST
SANDIA NATIONAL LABORATORIES

Earl Boebert is a Senior Scientist at Sandia National Laboratories. He has 44 years of experience in computers – 30 of those years in communications and computer security. He is the holder or co-holder of 13 patents and has participated in four National Research Council studies on security matters.

Prior to joining Sandia, he was the technical founder and Chief Scientist of Secure Computing Corporation where he developed the Sidewinder Security Server, a system that currently protects several thousand sites. Before that, he worked at Honeywell where he rose to the position of Senior Research Fellow. At Honeywell, he worked on secure systems, cryptographic devices, flight software and a variety of real-time simulation and control systems, and won Honeywell's highest award for technical achievement.

2002 INVITED ESSAYIST

DR. DANIEL GEER
CHIEF TECHNOLOGY OFFICER
@STAKE, INC

Dr. Daniel Geer oversees the strategy and direction of @stake's approach to digital security. Over the last 25 years, he has researched, developed, and instructed on the use of technology in medical computing, distributed systems management, and digital security. Dr. Geer has an extensive background in medical computing, culminating in a systems manager role for the Health Sciences Computer Facility at Harvard University. He went on to manage systems development for MIT's Project Athena, the first large distributed computing plant. Project Athena introduced much of the general organization of enterprise computing we now take for granted, including the X Windows System and Kerberos.

In the private sector, Dr. Geer served as a Director of Engineering at Open Market, Inc. and as Chief Scientist and Vice President of OpenVision Technologies (now Veritas). Prior to joining @stake, he was Vice President and Senior Strategist at CertCo, the leading on-line risk assurance authority.

An expert in modern security protocols and network solutions, Dr. Geer has been called to testify before the House Science Committee and the Subcommittee on Technology about public policy in the age of electronic commerce.

Dr. Geer speaks and publishes regularly on a range of issues in digital security. His November 1998 speech, "Risk Management is Where the Money Is," has been widely quoted, warranting both reprint as a special issue of the *RISKS Digest* and prompting editorial comment in *Wired Magazine*. With Avi Rubin of ATT Research and Marcus Ranum of Network Flight Recorder, he is co-author of *The WebSecurity Sourcebook*.

He holds a Sc.D. in biostatistics from the Harvard University School of Public Health as well as an S.B. in Electrical Engineering and Computer Science from MIT. He recently completed his term as President of USENIX, the advanced computing systems association.

WEDNESDAY MORNING, DECEMBER 11TH, 2002

8:30 AM – 10:00 AM 🗣 OPENING PLENARY

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**	*"The Common Sense of System Design"* Earl Boebert, Sandia National Laboratories, USA
9:50 AM	**Technical Program Introduction**	LouAnna Notargiacomo, Oracle Corporation, USA (Program Chair)

10:00 AM – 10:30 AM ☕ BREAK

10:30 AM – 12:00 PM 🗣 SESSIONS

TRACK A

Network Security I

Chair: Christoph Schuba
Sun Microsystems, Inc., Germany

- ♣ *GOSSIB vs. IP Traceback Rumors*
  Marcel Waldvogel, IBM Research, SWITZERLAND
- ♣ *Composable Tools For Network Discovery and Security Analysis*
  Giovanni Vigna, Fredrik Valeur, Jingyu Zhou and Richard Kemmerer, University of California Santa Barbara, USA
- ♣ *Representing TCP/IP Connectivity For Topological Analysis of Network Security*
  Ronald Ritchey, Booz Allen Hamilton, USA, Brian O'Berry and Steven Noel, George Mason University, USA

TRACK B

Electronic Commerce

Chair: Art Friedman
National Security Agency, USA

- ♣ *Regulating E-Commerce through Certified Contracts*
  Victoria Ungureanu, Rutgers University, USA
- ♣ *With Gaming Technology towards Secure User Interfaces*
  Hanno Langweg, University of Bonn, GERMANY
- ♣ *Protecting Web Usage of Credit Cards using One-Time Pad Cookie Encryption*
  Donghua Xu, Chenghuai Lu and Andre Luiz Moura dos Santos, Georgia Institute of Technology, USA

TRACK C: CASE STUDIES

Authentication

Chair: Vic Lindberg
Titan Systems Corp, USA

- *Investigating the Legacy System Challenge of Internet Connectivity*
  Martin Norman, Safestone Technologies, USA
- *Crossbeam X40S*
  Andrew Bagrin, Regal Entertainment Group, USA
- *Forging Digital Signatures*
  Albert Levi, Sabanci University, TURKEY

12:00 PM – 1:30 PM 🍽 LUNCH

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

WEDNESDAY AFTERNOON, DECEMBER 11TH, 2002

1:30 PM – 3:00 PM 🗣 SESSIONS

TRACK A

Mobile Security

Chair: Marshall Abrams
The MITRE Corporation, USA

- ♣ *Throttling Viruses: Restricting Propagation to Defeat Malicious Mobile Code*
  Matthew Williamson, Hewlett-Packard Labs, UK
- ♣ *Enforcing Resource Bound Safety for Mobile SNMP Agents*
  Weijiang Yu and Aloysius Mok, University of Texas at Austin, USA
- ♣ *Security of Internet Location Management*
  Tuomas Aura and Michael Roe, Microsoft Research, UK, Jari Arkko, Ericsson, FINLAND

TRACK B

FORUM
Wireless Security: Vulnerabilities and Solutions

Chair: Dale Johnson
The MITRE Corporation, USA

- Scott Paisley, Internet Security Systems, Inc., USA
- William Arbaugh, The University of Maryland, USA
- Steve Bellovin, AT&T Labs Research, USA
- Vipin Swarup, The MITRE Corporation, USA

TRACK C: CASE STUDIES

e-Commerce

Chair: Laura Montano
Booz Allen Hamilton, USA

- *The Key to Web Services Deployments: Security Standards Development,* Darran Rolls ,Waveset Technologies, Inc., USA
- *Long Term Storage for Electronically Signed Documents,*
  Georg Lindsberger, Xcript Technologies, AUSTRIA
- *Controlling Digital Multi-Signature with Attribute Certificate*
  Paul Axayacatl FRAUSTO BERNAL, LGI2P Research Center, Ecole de Mines d'Ales, FRANCE

3:00 PM – 3:30 PM ☕ BREAK

3:30 PM – 5:00 PM 🗣 SESSIONS

Classic Papers

Chair: Dan Thomsen
Secure Computing Corporation, USA

- ♣ *LOCK: A Historical Perspective*
  O. Sami Saydjari, SRI International, USA
- ♣ *A Practical Approach to Identifying Storage and Timing Channels: Twenty Years Later*
  Richard Kemmerer, University of California, Santa Barbara, USA
- ♣ *Thirty Years Later: Lessons from the Multics Security Evaluation*
  Paul Karger, IBM Corporation, T. J. Watson Research Center, USA and Roger Schell, Aesec Corporation, USA

Security Architecture

Chair: Jody Heaney
The MITRE Corporation, USA

- ♣ *Controlled Physical Random Functions*
  Blaise Gassend, Dwaine Clarke and Srinivas Devadas, Massachusetts Institute of Technology, USA, Marten van Dijk, Philips Research, THE NETHERLANDS
- ♣ *A Security Architecture for Object-Based Distributed Systems*
  Bogdan Popescu, Maarten van Steen and Andrew Tanenbaum, Vrije Universiteit, Amsterdam, THE Netherlands
- ♣ *A Secure Directory Service Based on Exclusive Encryption*
  John Douceur, Atul Adya, Josh Benaloh, William Bolosky, & Gideon Yuval, Microsoft Research, USA

Wireless

Chair: Rick Wilson
National Security Agency, USA

- *802.1X: Secure Network Access for Wired and Wireless Network*
  Jeff Hayes, Alcatel, USA
- *Wireless Case Study*
  Ruben Xing, Montclair State University, USA
- *Issues in Wireless Security,*
  Les Owens, Booz Allen Hamilton, USA

5:15 PM – 6:30 PM 🗣 Works In Progress

Chair: Chenxi Wang, Carnegie Mellon University, USA
(Room assignments will be posted at the Registration Desk)

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

THURSDAY MORNING, DECEMBER 12TH, 2002

8:30 AM – 10:00 AM 🗣 **INVITED ESSAYIST PLENARY**

Penetration Testing: The Science of Insecurity

Dan Geer, @stake, Inc., USA

10:00 AM – 10:30 AM ☕ **BREAK**

10:30 AM – 12:00 PM 🗣 **SESSIONS**

TRACK A

Protection Against Malicious Software

Chair: John McHugh
Carnegie Mellon University, USA

♣ *Protecting Data from Malicious Software*
Matthew Schmid and Frank Hill, Cigital, USA, Anup Ghosh, DARPA, USA

♣ *Safe Virtual Execution Using Software Dynamic Translation*
Kevin Scott and Jack W. Davidson, University of Virginia, USA

♣ *Digging For Worms, Fishing For Answers*
CERIAS Intrusion Detection Research Group, Purdue University, USA

TRACK B

Access Control

Chair: Ravi Sandhu
SingleSignOn.Net, Inc. and George Mason University, USA

♣ *A Framework for Organisational Control Principles*
Andreas Schaad and Jonathan Moffett, University of York, UK

♣ *Reusable Components for Developing Security-Aware Applications*
Stefan Probst, Wolfgang Essmayr and Edgar Weippl, Software Competence Center Hagenberg, AUSTRIA

♣ *A Context-Aware Security Architecture for Emerging Applications*
Michael Covington, Prahlad Fogla, Zhiyuan Zhan and Mustaque Ahamad, Georgia Institute of Technology, USA

TRACK C: CASE STUDIES

Boundary Protection

Chair: Jean Schaffer
National Security Agency, USA

- *Port 25: Securing the Gaping Hole*
  Scott Petry, Postini, USA
- *Operationalizing Mutilevel Security aka: Guarding Solutions*
  Brian Hubbard, Booz Allen Hamilton, USA
- *Building a Next Generation Firewall*
  Dan Thomsen, Secure Computing, USA

12:00 PM – 1:30 PM 🍽 **LUNCH**

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

THURSDAY AFTERNOON, DECEMBER 12TH, 2002

1:30 PM – 3:00 PM SESSIONS

TRACK A

Network Security II

Chair: Germano Caronni, Sun Microsystems Laboratories, USA

♣ *Voice over IPsec: Analysis and Solutions*
Roberto Barbieri, Danilo Bruschi and Emilia Rosti, Universita degli Studi di Milano, ITALY

♣ *Networking in The Solar Trust Model: Determining Optimal Trust Paths in a Decentralized Trust Network*
Michael Clifford, The Aerospace Corporation, USA

♣ *Gender-Preferential Text Mining of E-mail Discourse*
Malcolm Corney and Alison Anderson, and George Mohay, Queensland University of Technology, AUSTRALIA, Olivier de Vel, Defence Science and Technology Organisation, AUSTRALIA

TRACK B

Forum

Enterprise Engineering and Security: Enterprise Frameworks and Architectures, and IA Patterns

Chair: Jody Heaney, The MITRE Corporation, USA

- Duane Hybertson, The MITRE Corporation, USA
- Ann Reedy, The MITRE Corporation, USA
- Susan Chapin, The MITRE Corporation, USA
- Malcolm Kirwan, The MITRE Corporation, USA

TRACK C: CASE STUDIES

Policy

Chair: Mike Hale, Tresys Technology, USA

- *PKI Implementation Challenges*
  Michelle Ruppel, Saffire Systems, USA
- *Compliance Online: How to Protect Customer Privacy and Meet Other Regulatory Guidelines*
  Ken Beer, Tumbleweed, USA
- *Protecting Executives from Liabilities: Assessments and Solutions*, Ulf Mattsson, Protegrity, USA

3:00 PM – 3:30 PM BREAK

3:30 PM – 5:00 PM SESSIONS

FORUM

Themes and Highlights of the New Security Paradigms Workshop 2002

Chairs: Christina Serban, AT&T Labs, USA, and O. Sami Saydjari, SRI International, USA

- TBA

Intrusion Detection

Chair: Sara Weinberg, Mitretek Systems, USA

♣ *Evaluating the Impact of Automated Intrusion Response Mechanisms*
Thomas Toth and Christopher Kruegel, Technical University Vienna, AUSTRIA

♣ *Architectures for Intrusion Tolerant Database Systems*
Peng Liu, The Pennsylvania State University, USA

♣ *Detecting and Defending against Web-Server Fingerprinting*
Dustin Lee, University of California, Davis, USA

Enterprise Security

Chair: Bill Bialick, Bialick, Lee & Assoc., USA

- *Computer Security Regulations*
  Ben Rothke, QinetiQ Trusted Information Management, Inc., USA
- *Host-Oriented Security Test Suite*
  Jim Finegan, MITRE, USA
- *The Big Five Challenges of Enterprise Network Security,* Rod Murchison, Ingrian Networks, USA

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

THURSDAY EVENING, DECEMBER 12TH, 2002

5:30 PM – 6:30 PM 🍽 **CONFERENCE DINNER RECEPTION**

6:30 PM – 8:00 PM 🍽 **CONFERENCE DINNER**

FRIDAY MORNING, DECEMBER 13TH, 2002

8:30 AM – 10:00 AM 🗣 **SESSIONS**

TRACK A

Role-Based Access Control

Chair: Jay Kahn
The MITRE Corporation, USA

- ♣ *Advanced Features for Enterprise-Wide Role-Based Access Control*
  Axel Kern, Systor Security Solutions, GERMANY
- ♣ *Access Control for Active Spaces*
  Geetanjali Sampemane, Prasad Naldurg, Roy Campbell, University of Illinois at Urbana-Champaign, USA
- ♣ *A Model for Attribute-Based User-Role Assignment*
  Mohammad Al-Kahtani, George Mason University, USA, Ravi Sandhu, SingleSignOn.net, Inc. and George Mason University, USA

TRACK B

FORUM
Intrusion Detection: How Good is it and Where is it Going?

Chair: Karl Levitt
University of California at Davis, USA

- Josh Haines, MIT Lincoln Laboratory, USA
- Jeff Rowe, Unversity of California at Davis, USA
- Stuart Stanifor, Silicon Defense, USA
- Johannes Ullrich, The SANS Institute, USA

10:00 AM – 10:30 AM ☕ **BREAK**

10:30 AM – 12:00 PM 🗣 **SESSIONS**

Experience Reports

Chair: Ken Eggers
Entrust, USA

- ♣ *Did You Ever Have To Make Up Your Mind? What Notes Users Do When Faced With A Security Decision*
  Mary Ellen Zurko, Charlie Kaufman and Katherine Spanbauer, IBM Software Group, USA
- ♣ *Evaluating the Proposed NIST RBAC Standard with Respect to a Financial Institution's Legacy Mainframe Access Control System*
  Andrew Marshall, TD Bank Financial Group, CANADA
- ♣ *Security Architecture of the Austrian Citizen Card Concept*
  Herbert Leitold, Center for Secure Information Technology, AUSTRIA, Arno Hollosi and Reinhard Posch, Federal Chief Information Office, AUSTRIA

Detection

Chair: Jeremy Epstein
webMethods, Inc., USA

- ♣ *Detection of Malicious Boot Firmware*
  Frank Adelstein and Matt Stillerman, ATC-NY, USA, Dexter Kozen, Cornell University, USA
- ♣ *Beyond the Perimeter: The Need for Early Detection of Denial of Service Attacks*
  John Haggerty, Qi Shi, Madjid Merabti, Liverpool John Moores University, UK
- ♣ *A Toolkit for Detecting and Analyzing Malicious Software*
  Michael Weber, Matthew Schmid, David Geyer and Michael Schatz, Cigital, Inc., USA

12:00 PM **ADJOURN**

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

ACSAC TECHNICAL PROGRAM

OUTSTANDING PAPER AWARD

An annual prize for the Outstanding Paper has been established for the Annual Computer Security Applications Conference. The award will be based on both the written paper and an oral presentation of the paper by the author at the conference. A plaque and honorarium will be presented to the winning author. The Final ACSAC Program will identify the Outstanding Paper candidates.

The process for selection of the Outstanding Paper is as follows: First, the program committee makes a preliminary selection of Outstanding Paper candidates, and presents this list to ACSA. ACSA forms a subcommittee to judge the Outstanding Paper candidates, and the members of this subcommittee attend the presentation of each candidate paper. After all candidate papers have been presented, the subcommittee meets to select the winning paper. If the timing of paper presentations permits, the award is announced at the next available opportunity during the conference.

STUDENT PAPER AWARD

The winner of the student paper award is selected by the Student Awards Committee in consultation with ACSA. 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.

WORK IN PROGRESS SESSION

The Work In Progress (WIP) Session is intended as a forum to introduce new ideas, report on ongoing work that may or may not be complete, and to state positions on controversial issues or open problems. Additional submissions may be given to the Program Chair, LouAnna Notargiacomo, or the WIP Chair, Chenxi Wang. Submitted topics will be announced at the Opening Plenary session, and will be posted near the Conference Registration Desk.

ACSA CONFERENCESHIP PROGRAM

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.

To be considered for the Conferenceship Program, please submit the following information to the 2002 Student Awards Chair, Dr. Andre Dos Santos, student_chair@acsac.org: your name, your address, and the name of the institution at which you are a student; a list of applicable course work that you have completed or are currently enrolled in; your current grade point average; a short narrative discussing why you are interested in the security field, relevant areas of interest, the type of career you plan on pursuing, and two letters of recommendation from faculty. This material is typically due by October 1, 2002.

MEALS AND SPECIAL DIET REQUESTS

The Conference Committee has selected lunch menus we hope everyone will enjoy. We realize that some individuals have special dietary needs. We have made arrangements to offer a vegetarian meal at lunch that will feature some combination of pasta, vegetables, and/or fruits. Please indicate your dietary request on the registration form and on your arrival, 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.

ACSAC SPECIAL EVENTS AND OTHER INFORMATION

HOOVER DAM TOUR

Join us Friday at noon for a tour of the Hoover Dam – recognized by the American Society of Civil Engineers as one of seven modern American civil engineering wonders! The Dam is located in Black Canyon on the Colorado River about 30 miles southeast of Las Vegas on the Nevada-Arizona border. The tour will take about 5 hours.

See the Conference Registration Form to register for the tour – which includes a box lunch and transportation.

Picture Credit: US Department of Interior, Bureau of Reclamation – Lower Colorado Region.

IMPORTANT DATES TO REMEMBER

November 13, 2002: Last day for early/reduced conference registration.

November 14, 2002: Last day to reserve a room at the Alexis Park Resort & Spa at the Conference rate.

November 14, 2002: Last day to cancel your Conference registration and obtain a refund less a service charge of $25.00. Cancellations must be in writing and sent to ACSAC-18 (see Registration Form for the address).

HANDY URLS

ACSAC: http://www.acsac.org

Alexis Park Resort & Spa: http://www.alexispark.com. Note that Internet Explorer may be needed to access this site.

(ISC)2: http://www.isc2.org

Las Vegas Cybercafes: http://www.lasvegas.com/community/cybercafes.html

Las Vegas Metropolitan Police Department: http://www.lvmpd.com

ACSAC-18

Registration Form

www.acsac.org

Alexis Park Resort, Las Vegas, Nevada

December 9-13, 2002

ATTENDEE INFORMATION *Please TYPE or PRINT carefully.*

First Name _____ Last Name _____ Nickname for Badge _____

Company/Organization _____

Address _____

City _____ State _____ Zip Code _____ Country _____

Phone _____ Fax _____

Email _____

FEES

	On or Before Nov 13, 2002			After Nov 13, 2002		
	ACM Member	Non-member	Student	ACM Member	Non-member	Student
TECHNICAL PROGRAM *Circle applicable fee*	$550	$600	$175	$600	$650	$200
TUTORIALS *Circle applicable fees and tutorial numbers*						
Monday Full-day:	$475	$525	$175	$525	$575	$200
Tuesday Full-day:	$475	$525	$175	$525	$575	$200
Tuesday T7 or T8:	$375	$425	$125	$400	$450	$150

M1 M2 M3 M4 T5 T6 T7 T8

SIGSAC ISSUES WORKSHOP ***Circle to register and optionally to reserve lunch***

Registration (no fee) Lunch ($25)

PAYMENT COMPUTATION

Technical Program Registration: …… $ _____

Tutorial Registrations: …….. $ _____

SIGSAC Issues Workshop lunch: …… $25 $ _____

Thursday Dinner for guests: …….. ___ ticket(s) x $50 $ _____

Friday event (Hoover Dam Tour w/Lunch): ___ ticket(s) x $35 $ _____

TOTAL COST: $ _____

METHOD OF PAYMENT

[ ] Personal or Company Check enclosed. Make checks payable to ACSAC-18.

[ ] VISA, MasterCard, American Express, or Discover, please provide the following information in full:

Card Number _____ Expiration Date _____

Name on card _____ Cardholder's Signature _____

Billing Address, if different from mailing address _____

*Your credit card statement will describe this charge as "**REGISTRATION SYSTEMS LAB**"*

For additional registration information, please call: 407-971-4451

Privacy Policy: Go to "www.acsac.org" to see the ACSAC privacy policy.

PREFERENCES *Check all that apply.*

[ ] Do NOT publish my registration information in the attendee list.

[ ] Do NOT include me on the ACSA mailing list for future conference announcements.

[ ] I require special accommodations (kosher or vegetarian meals, wheelchair access, etc.):

_____

SURVEY: How did you hear about ACSAC?

[ ] ACM

[ ] Mailing

[ ] Publication: _____

[ ] Previous ACSAC Conference

[ ] Friend

[ ] ACSAC Website

[ ] At Conference: _____

[ ] other: _____

MEMBERSHIP:

ACM Member number: _____

HOTEL REGISTRATION

ACSAC has reserved at block of rooms at a special conference rate of $79.00 + 9% tax guaranteed until 14 November 2002. However, registering for the conference does not guarantee a room. You MUST reserve your hotel room through the Alexis Park at (800)582-2228 or http://www.alexispark.com/.

REGISTRATION:

Conference registration will not be accepted via telephone.

Register via the ACSAC web site at:

www.acsac.org

or mail this form to:

ACSAC-18
c/o Registration Systems Lab
61 Alafaya Woods Blvd. PMB#199
Oviedo, FL 32765

or Fax it to: 407-366-4138

Refund Policy: No refunds will be provided after November 15, 2002. Conference registrations may be canceled before that date for a service charge of $25. Cancellations must be in writing and sent to ACSAC-18 using the address or fax number provided at the right.

acs.v6 1121201