ADVANCE PROGRAM

21st Annual Computer Security Applications Conference

Presented by Applied Computer Security Associates

ACSAC
Application Computer Security Associates

Twenty-First Annual Computer Security Applications Conference (ACSAC)

Practical Solutions To Real World Security Problems

December 5-9, 2005
Tucson Marriott University Park
Tucson, AZ, USA
INVITATION TO ACSAC 21

I would personally like to invite you to attend the 21st Annual Computer Security Applications Conference (ACSAC). Having successfully completed twenty years of an international practical computer security conference, our only thought after last year's conference was "How do we make it better?"

Thanks to suggestions from attendees, we have several new features we are exploring this year. The first is that the refereed papers are going to be presented Tuesday through Thursday for three full days, instead of two and a half. The number of quality submissions has been steadily growing over the last several years and it was time to acknowledge that. In addition, ACSAC 21 adds a technology blitz session that will provide rapid-fire introductions to emerging and mature security technologies and their applications. Presentations are selected based on a 2000 word abstract.

This year the conference moves downtown near the University of Arizona campus. We hope this new venue will better serve our attendees by reducing the need for personal transportation while attending. This advance program should provide most of the details you will need to register, travel and attend, but please also visit www.acsac.org, where you can find many useful resources, including full archives of past ACSACs.

We hope to see you in Tucson this December!
Dan Thomsen, Conference Chair

WELCOME RECEPTION

Please join us on Monday evening at 6:00 PM for typical South-Western snacks, such as chips and salsa, fruit, and cheese and an opportunity to meet others in the security community. There will be a cash bar. This is a good opportunity for session chairs to meet face to face with their speakers, as well as a venue where all attendees can network prior to the technical tracks and sessions.

RECEPTION AND NISS AWARD

Please join us on Tuesday at 6:00 PM in the Canyon Room as Virgil Gligor, one of the country’s pioneering figures in computer security, will be presented with the 2006 National Information Systems Security Award by the National Institute of Standards and Technology and the National Security Agency in a brief ceremony. It will also be an excellent opportunity to network with all attendees and enjoy lite food and beverages until 9:00 PM.

IMPORTANT DATES TO REMEMBER

November 14, 2005: Last day to reserve a room at the Tucson Marriott University Park at the Conference rate.

November 16, 2005: Last day for early/reduced conference registration fee.

November 16, 2005: 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-21 (see Registration Form for the address and fax number).

CONFERENCE COMMITTEE

Conference Chair: Daniel Thomsen
Cyber Defense Agency LLC

Program Chair: Christoph Schuba
Sun Microsystems, Inc.

Program Co-Chair: Charles Payne
Adventium Labs.

Program Co-Chair: Pierangela Samarati
Università degli Studi di Milano

Registration: David Chizmadia
Promia, Inc.

Treasurer: Edward A. Schneider
Institute for Defense Analyses

Hot Topics Chair/ACSA Chair & Treasurer: Marshall Abrams
The MITRE Corporation

Tutorial Chair/ACSA Secretary: Daniel Faigin
The Aerospace Corporation

Student Awards Chair: Andre Luiz Moura dos Santos
The University of Puerto Rico, Mayaguez

Case Studies Chair/ACSA President: Steve Rome
Booz Allen Hamilton

Technology Blitz Chair: Paul Jardetzky
Independent Consultant

WIP Chair: Mary Ellen Zurko
IBM Corporation

Site Arrangements: Maria Collier
Internet Resources

Guest Speaker Liaison/ACSA Invited Essay Program: Steven J. Greenwald
Independent Consultant

Web Advisor: Robert H’ obbes’ Zakon
Zakon Group LLC.

Workshops Chair: Harvey H. Rubinvitz
The MITRE Corporation

Recording Secretary: Noelle Hardy
Aspect Security

Marketing Co-Chairs: Rama Moorthy, Rebecca Nelson
Booz Allen Hamilton

ACSA Vice-Chair: Jeremy Epstein
webMethods

ACSA Communications: Jay J. Kahn
The MITRE Corporation

Conference Chair Emerita: Ann Marmor-Squires
Northrop Grumman

ACSA Communications: Ann Marmor-Squires
Northrop Grumman

Conference Chair Emerita: Dee Akers
The MITRE Corporation

ADVANCE PROGRAM 21st Annual Computer Security Applications Conference
LOCAL INFORMATION

LOCATION
ACSAC 21 will be held in Tucson, Arizona, USA, at the Tucson Marriott University Park.

The city of Tucson is 2,389 feet above sea level and covers nearly 500 square miles. The landscape mixes flowering desert, rolling hills, winding dry riverbeds, rugged canyons, and pine-topped peaks – all beneath an expansive clear blue sky.

The whole state of Arizona is in the Mountain Standard Time Zone (MST).

WEATHER
The weather in Tucson is superb! Tucson enjoys more sunshine than any other city in the US, about 350 days a year. In December, the average high temperature is 65°F/18°C, while the average low temperature is 39°F/4°C. Throughout the year, most residents and visitors wear informal business attire. However, in the winter, a lightweight coat or jacket will usually suffice unless you plan to visit higher mountain areas where colder temperatures and snow are possible. Sunglasses and sun block are encouraged all through the year.

TAXES
Arizona’s state sales tax is 5%; an additional 2% is levied in Tucson. There is also a downtown tax of 5.6%. The tax on a hotel room in Tucson is 9.5%, plus $1.00 per room per night; the tax is 7.5% elsewhere in Pima County. The rental car tax is 10%, plus a concession fee of 10% if the car is picked up at the airport; the tax is 12% if the car is picked up off airport property, but within the Tucson city limits. Pima County imposes a car rental fee of $3.50. Note that cars can be rented at the Conference hotel.

TRANSPORTATION TO TUCSON
The Tucson International Airport is located about 12 miles south of Tucson – about 10 miles from the center of town and 8 miles from the conference hotel. Fourteen different airlines serve Tucson with nonstop service to 18 cities and connections to more than 121 destinations.

The distance between Phoenix Sky Harbor Airport and the conference hotel is approximately 100 miles. The estimated taxi fare is $100 one-way.

Arizona Stagecoach operates shared-ride van service. Fare $29 one-way, $56 round-trip. For more information, visit www.azstagecoach.com/ or call (520) 889-1000. Mention Group ID # ACSA120405. The AZ Stagecoach desk is located between carousels 4 & 5 at the baggage claim area.

To drive to the hotel from the airport, take Tucson Blvd to King Parkway; turn right on King to Broadway; turn left on Broadway to Euclid; turn right on Euclid to 2nd Street. The hotel is on the right.

PHOENIX– Information on the Phoenix Airport may be found at http://phoenix.gov/AVIATION/. The distance from the airport to the hotel is approximately 6 miles. The estimated taxi fare is $20 one-way, $33 round-trip. For more information, visit www.arizonashuttle.com/ or call (800) 888-2749 or (520) 795-6711 x168.

To drive to the hotel from the Phoenix Airport, take I-10 Southbound to Tucson; take Speedway exit east. Turn right on Park Avenue to Second Street. Turn right on Second Street. Hotel is at corner of Tyndal and Second.

Note- Renting a car is discouraged. The hotel is located downtown with several restaurants, coffee shops, ice cream stores, etc. within walking distance.

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 serves as the conference “Lost and Found Center” and is the location of the conference message board.

Sunday, December 4 6:00 – 8:00 PM
Monday, December 5 7:30 – 11:30 AM
1:00 – 4:30 PM
6:00 – 8:00 PM
Tuesday, December 6 through Thursday, December 8 7:30 – 11:30 AM
1:00 – 5:00 PM
Friday, December 9 7:30 AM– 10:30 AM

LOCAL GROUND TRANSPORTATION
Tucson – Information on the Tucson Airport may be found at www.tucsonairport.org/. The distance from the airport to the hotel is approximately 8 miles. The estimated taxi fare is $22 one-way.

Arizona Stagecoach operates shared-ride van service. Fare $20 one-way, $33 round-trip. For more information, visit www.azstagecoach.com/ or call (520) 889-1000. Mention Group ID # ACSA120405. The AZ Stagecoach desk is located between carousels 4 & 5 at the baggage claim area.

To drive to the hotel from the airport, take Tucson Blvd to King Parkway; turn right on King to Broadway; turn left on Broadway to Euclid; turn right on Euclid to 2nd Street. The hotel is on the right.

Packing Tips
The US Transportation Security Administration’s web page provides the latest packing tips for carry-on and checked baggage and lists of which items are permitted and prohibited: www.tsa.gov/public/index.jsp
The Tucson Marriott University Park is located downtown at 880 E Second Street, Tucson, AZ. Phone: (520) 792-4100, Fax: (520) 882-4100. More information may be found at marriott.com/property/factsheet/tusup. On-site parking is available for a fee of $10/day; Valet parking is $13/day.

Situated at the main gate of The University of Arizona, the Tucson Marriott University Park central location provides easy access to all Tucson has to offer. Tucson. Guest rooms and suites beautifully reflect Tucson's southwestern heritage. All rooms are furnished with cable TV, two phone lines with high speed Internet access, in-room coffee, iron and ironing board and hair dryer. This nine story atrium hotel offers tastefully appointed guest rooms and suites as well as an exercise room, full service business center and outdoor swimming pool. Downtown Tucson is two miles southwest of the hotel and the Fourth Avenue Arts District is just one mile away.

REGISTER EARLY! ACSAC has reserved a block of rooms

**Group Room Rates**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Single</td>
<td>$ 88.00</td>
</tr>
<tr>
<td>Double</td>
<td>$ 91.00</td>
</tr>
<tr>
<td>Additional Person</td>
<td>$ 15.00</td>
</tr>
</tbody>
</table>

**Reservations**

All reservations are to be made directly with Marriott reservations at (520) 792-4100 Extension 2020. Mention the Annual Computer Security Applications Conference (ACSAC or ACSAC 21) for the special rates. To book rooms outside of the conference dates, call (520) 792-4100 and accommodations will made upon space availability basis only.

Check-in time is 3:00 PM and Check-out time is 12:00 noon.

**Guarantee Reservation Policy**

All reservations must be accompanied by a first night room deposit or guaranteed with a major credit card. The hotel will not hold any reservation unless secured by one of the above methods.

**Cutoff Date**

Reservations by attendees must be received on or before Monday, November 14, 2005.
TUTOTIAL PROGRAM

TUTORIALS AT-A-GLANCE

ACSAC is pleased to host six all-day tutorials this year on Monday, December 5 and Friday, December 10, 2005. Check the pages that follow for more details about the tutorials and their instructors.

Monday, December 5, 2005

<table>
<thead>
<tr>
<th>M1</th>
<th>Web Application Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mr. David Wichers, <em>Aspect Security</em></td>
</tr>
<tr>
<td></td>
<td>8:30 AM to 5:00 PM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M2</th>
<th>Common Criteria Version 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mr. Ron Bottomly, <em>NIAP/CCEVS</em> and Dr. Dirk Jan-Out, <em>TNO-ITSEF</em></td>
</tr>
<tr>
<td></td>
<td>8:30 AM to 5:00 PM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M3</th>
<th>Trust Management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dr. Scott D. Stoller, <em>State University of New York at Stony Brook</em></td>
</tr>
<tr>
<td></td>
<td>8:30 AM to 12:30 PM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M4</th>
<th>Defenses Against Viruses, Worms, and Malicious Software</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dr. Tom Chen, <em>SMU Dept. of Electrical Engineering</em></td>
</tr>
<tr>
<td></td>
<td>8:30 AM to 12:30 PM</td>
</tr>
</tbody>
</table>

Friday, December 9, 2005

<table>
<thead>
<tr>
<th>F5</th>
<th>Acquisition and Analysis of Large Scale Network Data V.2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dr. John McHugh, <em>Dalhousie University</em></td>
</tr>
<tr>
<td></td>
<td>8:30 AM to 5:00 PM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>F6</th>
<th>Practical Security Policy Modeling</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dr. Steven J. Greenwald, <em>Independent Consultant</em></td>
</tr>
<tr>
<td></td>
<td>8:30 AM to 5:00 PM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>F7</th>
<th>Securing Enterprise &amp; Government Web Service Applications: A Lifecycle Perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mr. Steve Orrin, <em>Sarvega</em></td>
</tr>
<tr>
<td></td>
<td>8:30 AM to 12:30 PM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>F8</th>
<th>Identifying and Addressing Mobile Security Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mr. Norm Laudermilch and Mr. Bill Supernor, <em>Trust Digital</em></td>
</tr>
<tr>
<td></td>
<td>8:30 AM to 12:30 PM</td>
</tr>
</tbody>
</table>

TUTORIAL LUNCHES

Attendees enrolled in any of the ACSAC Tutorials listed above are provided lunch on the day of their tutorial.

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. 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.
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 applications may be the most important IT security issue 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. Security is just not a part of many computer science curricula today. This powerful one day course focuses on the most common application security problems facing web applications today. It describes the most common vulnerabilities present in today’s web applications, including the OWASP Top Ten, and practical techniques for avoiding, or identifying and removing such vulnerabilities from web applications.

**Prerequisites**
None. Technical background suggested, but not required.

**High-Level Outline**
This course starts with a module designed to raise awareness of just how insecure most web applications are. We demonstrate how hackers are able to attack web applications, and what some of the common vulnerabilities are. The next module presents the technological fundamentals of HTTP, the language of web applications. The basics of developing a good security policy for a custom application are then described. The course then covers the following application security vulnerability areas:

- Authentication
- Access Control
- Parameter Use
- Command/SQL Injection
- Cross Site Scripting
- Buffer Overflows
- Error Handling
- Cryptography
- System Administration
- Server Configuration
- Unnecessary and Malicious Code
- Thread Safety
- Denial of Service
- Privacy and Legislative Compliance
- Accountability and Logging
- Integrity
- Caching, Pooling, and Reuse
- Code Quality
- and more…

For each area, we cover the following:
- Theoretical foundations
- Common pitfalls when implementing
- Details on historical exploits
- Suggested security policies
- Best practices for implementation
- Pseudo code examples

The course then concludes with recommendations on how to improve security in your application development lifecycle so your teams can produce more secure code in the first place.

**About the Instructor:**
**Mr. David Wichers** is the Chief Operating Officer (COO) of Aspect Security, a company that specializes in application security services. Mr. Wichers has over seventeen years of experience in the information security field, in areas such as application security, security architectures, secure designs, security policies, models, database security, multilevel security, system and software development, and security testing. He has supported the design and development of enterprise web applications, trusted operating systems, trusted databases, secure routers, secure guards, and large integrated systems for a wide variety of Commercial and Government customers. He previously ran the Application Security Services Group at Exodus Communications. Mr. Wichers has a BSE in Computer Systems Engineering from Arizona State University and a Masters degree in Computer Science from the University of California at Davis. Mr. Wichers is a CISSP and a CISM, is currently the OWASP Conferences Chair (www.owasp.org), and is a coauthor of the OWASP Top Ten.
This tutorial introduces the Common Criteria version 3 and its associated methodology, in terms of its philosophy, structure, principles, and requirements. The tutorial will be useful for developers, in order to understand the requirements against which their products will be measured; for evaluators, who will use the criteria to perform security evaluations; and for consumers, who need to understand the meaning of results of CC evaluations.

**Prerequisites**
Basic knowledge of the Common Criteria is strongly recommended.

**High Level Outline**

1. **Background**
   a. Source Criteria, development of CC, ISO standard
   b. Why a new CC version?

2. **Overview of the structure of the CC (.5 hrs)**
   a. Explanation of the different Parts, the CEM.
   b. Class/family/component structure
   c. Dependencies; hierarchy
   d. Explanation of special terms

3. **Protection Profiles and Security Targets (1hr)**
   a. Purpose
   b. Overview and structure of PPs/STs
   c. Purpose and content of the different sections

4. **CC Part 2: Security Functionality Requirements (2.5 hrs)**
   a. The Part 2 Model
   b. The Part 2 classes
   c. Modeling security with CC Part 2

5. **CC Part 3: Security Assurance Requirements and Methodology**
   a. High-level philosophy/approach
   b. The Part 3 classes (3 hrs)

**About the Instructors:**

**Mr. Ron Bottomly** is a chief validator of the Common Criteria Evaluation and Validation Scheme. He was an early reviewer of the Common Criteria, and the US scheme representative to the Common Evaluation Methodology Editorial Board, where he was a co-author of the CEM v1.0. He has also served as a member of the NATO CC working group. He is the US scheme representative to the Common Criteria Interpretations Management Board, where he co-authored the CC/CEM v3.0.

**Dr. Dirk-Jan Out** is the general manager of TNO-ITSEF, the Dutch Security Evaluation Facility, accredited under both the BSI (Germany) and the NSCIB (Netherlands) CC Certification Bodies. He was an early reviewer of the Common Criteria and the Dutch representative to the Common Evaluation Methodology Editorial Board, where he co-authored the CEM v1.0. He is currently a Dutch representative to the Common Criteria Interpretations Management Board, where he was a co-author of the CC/CEM v3.0.
As computer systems become increasingly inter-connected, there is a growing need to establish and enforce security policies in the information systems of large enterprises, coalitions, and other organizations that lack globally trusted security administrators. Trust management offers flexible solutions for decentralized management of security policies in such systems.

Trust management has three characteristic features: (1) each policy statement is associated with a principal, called its source or issuer; (2) each principal's policy specifies which sources it trusts for which kinds of statements, thereby delegating some authority to those sources; and (3) policies may refer to domain-specific attributes of and relationships between principals, resources, and other objects. Thus, in the trust management approach, the overall security policy is formed from decent rally managed policies interacting through delegation.

**Prerequisites**

None.

**High-Level Outline**

1. Introduction to and Motivation for Trust Management
2. Design Issues and Features in Trust Management
3. Overview of Existing Trust Management Frameworks
4. Two Representative Trust Management Frameworks in Detail
5. Sample Application Domains
6. Current Research Directions

**About the Instructor:**

**Dr. Scott D. Stoller** is an Associate Professor in the Computer Science Department at the State University of New York at Stony Brook. His primary research interests are computer security, distributed systems, concurrency, and software analysis, testing, and verification. He received his Bachelor's degree in Physics, summa cum laude, from Princeton University in 1990 and his Ph.D. degree in Computer Science from Cornell University in 1997. He received an NSF CAREER Award in 1999 and an Office of Naval Research Young Investigator Award 2002. He is a member of the team that won the NASA Turning Goals Into Reality Award for Engineering Innovation in 2003. He is the author or co-author of over 50 refereed research publications and has given over 50 presentations at conferences, workshops, universities, and research labs.
The Internet has created a fertile environment for viruses and worms since virtually every computer now interconnected into a global community. About every PC user has an experience with a virus or worm at some time or another. Unlike many types of security attacks directed at compromising a specific target, the self-replicating nature of viruses and worms creates a large-scale attack on the general community. The Internet itself is also affected by the resulting congestion.

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

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

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

Prerequisites
None.

High-Level Outline
1. Introduction
2. Malware Basics
3. Current Defenses
4. Early Detection and Warning
5. Dynamic Quarantining
6. References and Further Reading

About the Instructor:
Dr. Thomas M. Chen is an associate professor in the Department of Electrical Engineering at Southern Methodist University in Dallas, Texas. He received the BS and MS degrees in electrical engineering from the Massachusetts Institute of Technology in 1984, and the PhD in electrical engineering from the University of California, Berkeley, in 1990. He is currently the associate editor-in-chief of IEEE Communications Magazine, a senior technical editor for IEEE Network, an associate editor for ACM Transactions on Internet Technology, and past founding editor of IEEE Communications Surveys. He serves as the treasurer for the IEEE Technical Committee on Security and Privacy. He is a member of the Technical Advisory Board for the Voice over IP Security Alliance. Prior to joining SMU, he was a senior member of the technical staff at GTE Laboratories (now Verizon Labs) working on ATM research. He is the co-author of ATM Switching Systems (Artech House, 1995). He was the recipient of the IEEE Communications Society’s Fred W. Ellersick best paper award in 1996. His research interests include network security, traffic modeling, network performance, and network management.
Detecting malicious activity in network traffic is greatly complicated by the large amounts of noise, junk, and other questionable traffic that can serve as cover for these activities. With the advent of low cost mass storage devices and inexpensive computer memory, it has become possible to collect and analyze large amounts of network data covering periods of weeks, months, or even years. This tutorial will present techniques for collecting and analyzing such data, both from network flow data that can be obtained from many routers or derived from packet header data and directly from packet data such as that collected by TCPDump, Ethereal, and Network Observer.

Because of the quantity of the data involved, we develop techniques, based on filtering of the recorded data stream, for identifying groups of source or destination addresses of interest and extracting the raw data associated with them. The address groups can be represented as sets or multisets (bags) and used to refine the analysis. For example, the set of addresses within a local network that appear as source addresses for outgoing traffic in a given time interval approximates the currently active population of the local network. These can be used to partition incoming traffic into that which might be legitimate and that which is probably not since it is not addressed to active systems. Further analysis of the questionable traffic develops smaller partitions that can be identified as scanners, DDoS backscatter, etc. based on flag combinations and packet statistics. Traffic to and from hosts whose sources appear in both partitions can be examined for evidence that its destinations in the active set have been compromised. The analysis can also be used to characterize normal traffic for a customer network and to serve as a basis for identifying anomalous traffic that may warrant further examination.

Prerequisites
General familiarity with IP network protocols. Elementary familiarity with simple statistical measures.

High Level Outline
1. Introduction (60 Minutes)
2. Data Collection (30 Minutes)
3. The SiLKtools Analysis Suite (90 Minutes)
4. Advanced Analysis (90 Minutes)
5. Case studies (60 Minutes)
6. General Questions and Discussion (30 minutes)

About the Instructor:
Dr. John McHugh holds a Canada Research Chair in Privacy and Security at Dalhousie University in Halifax, NS where he leads the Privacy and Security Laboratory. Prior to joining Dalhousie, he was a senior member of the technical staff with the CERT Situational Awareness Team, where he did research in survivability, network security, and intrusion detection. Recently, he has been involved in the analysis of large scale network flow data. He was a professor and former chairman of the Computer Science Department at Portland State University in Portland, Oregon. His research interests include computer security, software engineering, and programming languages. He has previously taught at The University of North Carolina and at Duke University. He was the architect of the Gypsy code optimizer and the Gypsy Covert Channel Analysis tool. Dr. McHugh received his PhD degree in computer science from the University of Texas at Austin. He has a MS degree in computer science from the University of Maryland, and a BS degree in physics from Duke University.
Security Policies are the basis for the design and implementation of security mechanisms, among other things. This tutorial starts with a definition of “policy” and the important top-level policy properties for the INFOSEC field. Notions of security policies are examined, as well as some sample policy objectives in the context of enterprise/organizational and automated security policies. The differences between formal and informal security policy models will be examined, and some of the most influential policy models in the field will be presented (in the areas of access control, confidentiality, integrity, and organization). An example of the security policy modeling process will be given with an actual example model. Security policy modeling guidelines will then be presented.

The ideal student is someone who knows nothing about Security Policy Modeling, or needs a refresher regarding the basics. Since it is unrealistic to assume that the students can absorb all of this material in a one-day tutorial, each will be given 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. Novice level.

**High-Level Outline**


4. Conclusions and General Q&A.

**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 is a member of 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 US 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). He has an M.S. degree in Computer Science and Information Systems from Barry University and a bachelor's degree in Chemistry from Emory University.
Securing Enterprise & Government Web Service Applications: A Lifecycle Perspective

Mr. Steve Orrin
Sarvega.

Organizations that are implementing Web Services are discovering that there are security challenges unique to Web Services that can surface throughout the various phases of Web Service lifecycle. Traditional network and application protection and infrastructure systems lack the functionality, performance, and operational efficiencies needed to provide a secure, cost effective solution.

Web Services and SOA provide significant benefits and efficiencies to organizations that implement them. However they also introduce new risk structure not seen in other applications or technology solutions before. Web services introduce a ‘Perfect Storm’ of security/risk requirements. These requirements for security, access control, business continuity and risk management can be divided into 3 categories or groupings: Trust services, Operationalization/Reliability, and Risk Mitigation.

This tutorial explores the process for securing Web Services as well as what is needed to address security through all phases of the Web Service lifecycle of Build, Publish, Deploy, and Run. The tutorial investigates the nature of XML Web Services threats, including threat models, threat types, attack vectors, and risk.

The tutorial covers what to expect from Web Service security standards and proposes practical approaches to secure Web Services and ensure the data integrity and confidentiality of Web Services transactions. The tutorial reviews an approach to XML Web Services security and threat prevention that provides a logical separation between XML Web Services trust enablement and XML Web Services threat prevention. The tutorial will cover what is needed to proactively protect Web Services data and communications. It will describe what can be implemented to protect against known and unknown XML network threats that could impact the availability and integrity of the Web Services application.

Prerequisites
None.

High-Level Outline
1. Web Services Adoption Curve
2. Web Services Drivers
3. The Web Services protocol stack
4. Standards & Web Services security:
5. Perfect Storm of Security Requirements
6. Relating Security to Phases of Implementing Web Services:
7. The Process for securing XML Web Services
8. Understanding the characteristics of XML Web Services flows (and their impact on network infrastructure)
10. Web Services Attack Threats:
11. Key components of effective XML Threat Prevention
12. Web Services Security Gateways
13. Q&A: 15 minutes Introduction and Motivation

About the Instructor:
Mr. Steve Orrin is CSO of Sarvega, Inc., and is responsible for the security products strategy and direction for the company. Steve was formerly Vice President of Security Solutions for Watchfire, Inc., and was responsible for the product strategy and direction of Watchfire’s web application security and privacy software product lines. Steve was CTO of Sanctum, a pioneer company in Web application security testing and firewall software prior to Watchfire’s acquisition of Sanctum.

Prior to Sanctum, Steve was CTO and co-founder of Lockstar Inc., which provided a secure XML Web Services environment that enabled legacy and enterprise applications for e-business. Steve joined Lockstar from SynData Technologies, Inc., where he was CTO and chief architect of its desktop email and file security products.

Steve Orrin is a well known speaker on Web Services, XML, and application security topics and has spoken on numerous occasions at CSI, RSA, ISACA, N+1, TEPR, Vanguard, and SANS conferences. Steve was named one of InfoWorld’s Top 25 CTO’s of 2004 and has developed several patent-pending technologies covering user authentication, secure data access, and steganography, with one patent issued to him in steganography. Steve is a member of the Network and Systems Professional Association (NaSPA), the Computer Security Institute (CSI), the Information Systems Security Association (ISSA), and the Software Engineering Institute (SEI). He participates in several working groups of OASIS and ITEF.
Identifying and Addressing Mobile Security Issues

Mr. Norm Laudermilch and Mr. Bill Supernor

Trust Digital

Is your Perimeter Security really protecting your perimeter? Are you sure that you understand where all of your access points are? Do you even know where the processing and storage of your company proprietary information starts and stops? If you have even one employee with a palm pilot, smart phone, pocket pc or other mobile device, chances are you answered that last question with a "no".

Do you know what your company is spending on mobility next year? Have you figured out what you need to do and how much its going to cost to extend your current security mechanisms to the mobile edge? As mobile devices become more a part of our daily work lives, and as more industries come to rely on the convenience of mobile data to achieve their goals, security at the mobile edge becomes critical. The mobile devices of today are far more advanced than just a few months ago, and their networking, processing, and storage capabilities are doubling every few months. Your employees (and non-employees) are buying and using them, and whether you like it or not they are in your corporate environment - connected. After this session you will know how to discover your mobile edge, understand how to protect your mobile edge, and feel confident with the security and trust at your mobile edge.

Prerequisites

Working knowledge of TCP/IP networking - both wired and wireless, basic knowledge of standard security components and practices (firewalls, IDS, policy definition, etc).

High-Level Outline

1. What perimeter security "used" to look like
2. Today's problem
3. Risk, and real-world examples
4. Evolutionary path
5. The necessary components
6. A model for mobile edge security
7. Conclusion

About the Instructors:

Mr. Norm Laudermilch is a security expert with sixteen years of technical and executive experience. Mr. Laudermilch has been involved in the design, development, and implementation of numerous security products and services and is a sought after speaker at global computer security conferences. His definitive writings and teaching range from TCP/IP to UNIX to numerous security topics including several research papers on firewall design. Mr. Laudermilch has held the highest national security clearances and has experience in numerous classified environments. Mr. Laudermilch is currently the Chief Security Officer at Trust Digital where he plays an active role in the evolution of their Mobile Edge Security Architecture. He recently served as Vice President of Managed Security Services at global infrastructure services provider, VeriSign. Prior to VeriSign, he served as Vice President of Managed Security Services at Riptech/Symantec from 2000-2002. Before joining Riptech/Symantec, Laudermilch co-founded the Internet Security Advisors Group as well as the Internet Service Provider Security Working Group (ISPSEC). Laudermilch was also Director of Global Security at UUNET.

Mr. Bill Supernor, CISSP, is the Trust Digital Vice President of Engineering. Mr. Supernor brings over 12 years of experience with enterprise application development, IT security, networking, and team management to the company. He has built a reputation of developing quality software for on-time releases against aggressive schedules. Prior to Trust Digital, Mr. Supernor directed software development at Cognio, building its wireless spectrum management prototype into an enterprise customer-ready product. Prior to Cognio, he worked at MountainWave/Symantec, at first directing the development of the CyberWolf security information management system, and then managing the evolution of CyberWolf into Symantec Incident Manager. Mr. Supernor also managed development at Network Associates/McAfee on the Gauntlet firewall, where he enhanced the firewall to perform gateway virus scanning over multiple protocols. Later, he was instrumental to the conversion of this function to the WebShield internet gateway appliances. Following the sale of Gantlet to Secure Computing, Mr. Supernor worked for a time as an Architect on the SideWinder G2 firewall. Mr. Supernor has also worked at a number of defense contracting and US military organizations.
MALICIOUS SOFTWARE (PREVENTION AND DEFENSE)

Chair:
Dr. Harvey H. Rubinovitz
Mitre Corporation

Monday, 5 December 2004
8:30 AM - 4:30 PM

In recent years, Internet infectious epidemics have become one of the major threats to service availability and information security. The infections caused by malicious software, which includes viruses, worms, Trojan horses, rootkits, spyware, malware, and adware, are costing corporations billions of dollars in time and resources, and show no signs of abating.

The security community has taken a great interest in malicious software due to the rise in the number of reported cases of attacks and is exploring methods to reduce damage caused by malicious software. In addition to the various applications that can detect and eradicate viruses, spyware, malware, and adware, security professionals are starting to incorporate the use of more advanced software development tools during the application design process. The end result of making security a key component of the design stage is a reduction in the number of security related bugs, for example buffer-overflow errors are one of the leading exploits. Configuration management applications are also helpful, as they insure that computer systems are kept up-to-date with the latest release of vendor software. Intrusion Detection Systems (IDS), along with network management systems, help isolate the affected systems that have been exploited.

This workshop will focus on the relationship between malicious software and security, specifically how technology is being implemented and utilized to identify, mitigate, and remediate the effects of malicious software. The workshop will also look at the need to facilitate the research and development of the next generation of anti-malicious software procedures to assist in the creation of more robust software.

WORKSHOP REGISTRATION

If you are interested in attending please check off the appropriate box on the conference registration form and add the nominal fee of $50 to cover the cost of the workshop, lunch and snack. Position papers are encouraged. To submit a paper, contact Harvey Rubinovitz, Workshop Chair, The MITRE Corporation, M/S S145, 202 Burlington Road, Bedford, Massachusetts 01730; (781) 271-3076; hhr@mitre.org.

Please note that registration for this Workshop does not include registration for any ACSAC sessions.
2005 DISTINGUISHED PRACTITIONER

BRIAN SNOW
NATIONAL SECURITY AGENCY

We Need Assurance!

When will I be secure? Nobody knows for sure – but it cannot happen before commercial security products and services possess not only enough functionality to satisfy customer’s stated needs, but also sufficient assurance of quality, reliability, safety, and appropriateness for use. Such assurances are lacking in most of today’s commercial security products and services. Paths to better assurance in Operating Systems, Applications, and Hardware through better development environments, requirements definition, systems engineering, quality certification, and legal constraints are discussed and examples given.

A mathematician/computer scientist, Brian helped found the computer science department at Ohio University in the 1960’s. He left university teaching in 1971 to join the U. S. National Security Agency where he became a cryptologic designer and security systems engineer. Brian spent much of his early NSA career in research – developing cryptographic components and systems. Many of his algorithms are used today in cryptographic systems serving the U.S. government and military. These systems provide capabilities not previously available, and span a range from nuclear command and control to tactical radios for the battlefield. He has garnered patents and many awards and honors attesting to his creativity. Mr. Snow’s later career has been the model for what it means to be a Technical Director at NSA (similar to a chief scientist or senior technical fellow in industry); he has served in that capacity in three major mission components – Research, Information Assurance, and currently the National Cryptologic School (NSA’s Corporate University). His mantra has been: “Managers are responsible for doing things right; Technical Directors are responsible for finding the right things to do.” Brian holds a B.A mathematics 1965, M.A. mathematics 1967, both from University of Colorado. Additional course work was completed at University of Ohio and University of Maryland.

2005 INVITED ESSAYIST

MARY ELLEN ZURKO
IBM CORPORATION

User Centered Security: Stepping Up to the Grand Challenges

User-centered security has been identified as a grand challenge in information security and assurance. It is on the brink of becoming an established subdomain of both security and human/computer interface (HCI) research, and an influence on the product development lifecycle. Both security and HCI rely on the reality of interactions with users to prove the utility and validity of their work.

As practitioners and researchers in those areas, we still face major issues when applying even the most foundational tools used in either of these fields across both of them. This essay discusses the systemic roadblocks at the social, technical, and pragmatic levels that user-centered security must overcome to make substantial breakthroughs. Expert evaluation and user testing are producing effective usable security today. Principles such as safe staging, enumerating usability failure risks, integrated security, transparent security and reliance on trustworthy authorities can also form the basis of improved systems.

Mary Ellen Zurko leads security architecture and strategy for Lotus Workplace, Portal, and Collaboration Software at IBM. She defined the field of User-Centered Security in 1996. She is on the steering committee for New Security Paradigms Workshop and the International World Wide Web Conference series. She has worked in security since 1986, at The Open Group Research Institute and Digital Equipment Corporation, as well as IBM. She is a contributor to the upcoming O’Reilly book, “Security and Usability: Designing Secure Systems that People Can Use.”
# ACSAC TECHNICAL PROGRAM

**TUESDAY MORNING, December 6, 2005**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30 AM – 10:00 AM</td>
<td>OPENING PLENARY</td>
</tr>
<tr>
<td>Opening Remarks</td>
<td>Dan Thomsen, Conference Chair, Cyber Defense Agency LLC, USA</td>
</tr>
<tr>
<td>Welcome to Tucson</td>
<td>Hotel Manager</td>
</tr>
<tr>
<td>Distinguished Practitioner</td>
<td>“We Need Assurance!”</td>
</tr>
<tr>
<td>Technical Program Introduction</td>
<td>Christoph Schuba, Program Chair, Sun Microsystems, Inc., USA</td>
</tr>
<tr>
<td>10:00 AM – 10:30 AM</td>
<td>BREAK</td>
</tr>
<tr>
<td>10:30 AM – 12:00 PM</td>
<td>SESSIONS</td>
</tr>
<tr>
<td><strong>TRACK A</strong></td>
<td><strong>SOFTWARE SECURITY</strong></td>
</tr>
<tr>
<td>Chair: Christoph Schuba</td>
<td>Sun Microsystems, Inc., USA</td>
</tr>
<tr>
<td>Model Checking an Entire Linux Distribution for Security Violations</td>
<td>Benjamin Schwarz, Hao Chen, David Wagner, Geoff Morrison, Jacob West, Jeremy Lin, and Wei Tu, University of California, Berkeley, USA</td>
</tr>
<tr>
<td>Strengthening Software Self-Checksumming via Self-Modifying Code</td>
<td>Jonathan Giffin, Mihai Christodorescu, and Louis Kruger, University of Wisconsin, Madison, USA</td>
</tr>
<tr>
<td>Countering Trusting Trust through Diverse Double-Compiling</td>
<td>David A. Wheeler, Institute for Defense Analysis, USA</td>
</tr>
<tr>
<td><strong>TRACK B</strong></td>
<td><strong>NETWORK INTRUSION DETECTION</strong></td>
</tr>
<tr>
<td>Chair: Peng Liu</td>
<td>Penn State Univ., USA</td>
</tr>
<tr>
<td>A Framework for Detecting Network-based Code Injection Attacks Targetting Windows and UNIX</td>
<td>Stig Andersson, Andrew Clark, George Mohay, Bradley Schatz, and Jakub Zimmermann, Queensland University of Technology, Australia</td>
</tr>
<tr>
<td>Exploiting Independent State for Network Intrusion Detection</td>
<td>Robin Sommer, Technische Universität München, Germany and Vern Paxson, ICSI and LBNL, USA</td>
</tr>
<tr>
<td>A Host-Based Approach to Network Attack Chaining Analysis</td>
<td>Paul Ammann, Joseph Pamula, and Julie Street, George Mason University, USA and Ronald Ritchey, Booz Allen Hamilton, USA</td>
</tr>
<tr>
<td><strong>TRACK C: Case Studies</strong></td>
<td><strong>SECURITY MANAGEMENT</strong></td>
</tr>
<tr>
<td>Chair: Tom Fuhrman</td>
<td>Booz Allen Hamilton, USA</td>
</tr>
<tr>
<td>iTSafe</td>
<td>Ian Bryant, iTSafe, England</td>
</tr>
<tr>
<td>Implementing Long-Term, Coarse Traffic Capture</td>
<td>Michael Collins, CERT, USA</td>
</tr>
<tr>
<td>PATCHLINK UPDATE: Patch &amp; Vulnerability Management Remedy for MidMichigan Medical Center</td>
<td>Jim Czyzewski and Don Leatham, MidMichigan Medical Center, USA</td>
</tr>
<tr>
<td>12:00 PM – 1:30 PM</td>
<td>LUNCH</td>
</tr>
</tbody>
</table>
## ACSAC TECHNICAL PROGRAM

### TUESDAY AFTERNOON, December 6, 2005

<table>
<thead>
<tr>
<th>1:30 PM – 3:00 PM</th>
<th>SESSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TRACK A</strong></td>
<td><strong>TRACK B</strong></td>
</tr>
<tr>
<td><strong>Security Designs</strong></td>
<td><strong>Protocol Analysis</strong></td>
</tr>
<tr>
<td>Chair: Art Friedman</td>
<td>Chair: Pierangela Samarati, Università degli Studi di Milano, Italy</td>
</tr>
<tr>
<td>NSA, USA</td>
<td></td>
</tr>
<tr>
<td>♣ A Nitpicker’s Guide to a Minimal-Complexity Secure GUI</td>
<td>♣ Verify Results of Network Intrusion Alerts Using Lightweight Protocol Analysis</td>
</tr>
<tr>
<td>Norman Feske and Christian Helmuth, Technische Universität Dresden, Germany</td>
<td>Jingmin Zhou, Adam Carlson, and Matt Bishop, University of California, Davis, USA</td>
</tr>
<tr>
<td>♣ A User-Level Framework for Auditing and Monitoring</td>
<td>♣ Improving the Security of TCG Specification</td>
</tr>
<tr>
<td>Yongzheng Wu and Roland Yap, National University of Singapore, Singapore</td>
<td>Danilo Bruschi, Lorenzo Cavallaro, Andrea Lanzi and Mattia Monga, Universita’ degli Studi di Milano, Italy</td>
</tr>
<tr>
<td>♣ TARP: Ticket-based Address Resolution Protocol</td>
<td>♣ Automated Code Security Analysis of a Biometric Authentication System</td>
</tr>
<tr>
<td>Wesam Lootah, William Enck, and Patrick McDaniel, Penn State University, USA</td>
<td>Jan Jürjens, Technische Universität München, Germany</td>
</tr>
</tbody>
</table>

| 3:00 PM – 3:30 PM | BREAK |

---

**ADVANCE PROGRAM** 21st Annual Computer Security Applications Conference 17
### 3:30 PM – 5:30 PM |  SESSIONS

<table>
<thead>
<tr>
<th>TRACK A</th>
<th>TRACK B: HOT TOPICS I</th>
<th>TRACK C: Case Studies</th>
</tr>
</thead>
</table>
| **Vulnerability Assessment**  
  Chair: Ronald Ritchey  
  Booz Allen Hamilton, USA | **How Does Information Assurance R&D Impact Information Assurance in Practice?**  
  Chair: Dr. Doug Maughan  
  Department of Homeland Security, USA | **Managing the Enterprise**  
  Chair: Jim Gerretson  
  DNovus, USA |
| ♣ Automated and Safe Vulnerability Assessment  
  Fanglu Guo, Yang Yu, and Tzi-cker Chiueh, Stony Brook University, USA | ♣ Dr. Steve King DoD/DDR&E  
 ♣ Mr. Mark Powell FAA  
 ♣ Mr. Michael Brown FAA  
 ♣ Mr. Art Friedman OSD(NII) | ♣ Aligning Roles for a Managed Security Environment  
 Joe Cupano, Solsoft, USA |
| ♣ Understanding Complex Network Attack Graphs through Clustered Adjacency Matrices  
 Steven Noel and Sushil Jajodia, George Mason University, USA | ♣ Security Methodology and Incident Response  
 Patrick Hanrion, Microsoft, USA |
| ♣ Intrusion Detection in RBAC-Administered Databases  
 Elisa Bertino and Ashish Kamra, Purdue University, USA, and Evimaria Terzi, University of Helsinki, Finland, and Athena Vakali, Aristotle University, Greece | ♣ Designing for Insecurity  
 Drew Simonis, Symantec Corp. USA |

**6:00 PM | NISS Award and Reception**
WEDNESDAY MORNING, December 7, 2005

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30 AM – 10:00 AM</td>
<td>INVITED ESSAYIST PLENARY</td>
</tr>
<tr>
<td></td>
<td><em>User Centered Security: Social, Technical and Practical Challenges</em></td>
</tr>
<tr>
<td></td>
<td><em>Mary Ellen Zurko</em></td>
</tr>
<tr>
<td></td>
<td>IBM Corporation</td>
</tr>
<tr>
<td>10:00 AM – 10:30 AM</td>
<td>BREAK</td>
</tr>
<tr>
<td>10:30 AM – 12:00 PM</td>
<td>SESSIONS</td>
</tr>
<tr>
<td>TRACK A</td>
<td>TRACK B</td>
</tr>
<tr>
<td>Automation</td>
<td>Security Analysis</td>
</tr>
<tr>
<td>Chair: Patrick McDaniel</td>
<td>Chair: Jarrellann Filsinger</td>
</tr>
<tr>
<td>Penn State University, USA</td>
<td>National Archives, USA</td>
</tr>
<tr>
<td>Corrado Leita, Ken Mermoud, and Marc Dacier, Eurecom Institute, France</td>
<td>Mourad Debbabi, Mohamed Saleh, Chamseddine Talhi, and Sami Zhioua, Concordia University, Canada</td>
</tr>
<tr>
<td>Zhenkai Liang and R. Sekar, Stony Brook University, USA</td>
<td>John Black, Martin Cochran, and Ryan Gardner, University of Colorado at Boulder, USA</td>
</tr>
<tr>
<td>♣ Evolving Successful Stack Overflow Attacks for Vulnerability Testing</td>
<td>♣ Building Evidence Graphs for Network Forensics Analysis</td>
</tr>
<tr>
<td>Gunes Kayacik, Malcolm Heywood, and Nur Zincir-Heywood, Dalhousie University, Canada</td>
<td>Wei Wang and Thomas E. Daniels, Iowa State University, USA</td>
</tr>
<tr>
<td>TRACK C: Case Studies</td>
<td>Internet Security Visualization</td>
</tr>
<tr>
<td>Chair: Marshall Abrams</td>
<td>Chair: Marshall Abrams</td>
</tr>
<tr>
<td>The MITRE Corporation, USA</td>
<td>The MITRE Corporation, USA</td>
</tr>
<tr>
<td>Bill Yurcik, National Center for Supercomputing Applications, Univ. of Illinois, USA</td>
<td>Carrie Gates, CERT, USA</td>
</tr>
<tr>
<td>♣ Creating Dynamic Baselines Visually</td>
<td>♣ Creating Dynamic Baselines Visually</td>
</tr>
<tr>
<td>Paul Sop, Intellitactics, CANADA</td>
<td>Paul Sop, Intellitactics, CANADA</td>
</tr>
<tr>
<td>12:00 PM – 1:30 PM</td>
<td>LUNCH</td>
</tr>
</tbody>
</table>
# WEDNESDAY AFTERNOON, December 7, 2005

## 1:30 PM – 3:00 PM  ●  PLENARY SESSION

### Technology Blitz

**Session Chair:** Jeremy Epstein, webMethods, Inc.

The Technology Blitz Session is a forum for participants that wish to disseminate practical research or operational results in an abbreviated format. This session is particularly well suited toward authors that do not have time to construct a full academic paper, yet still may provide useful insight into solutions for computer or networked computer security.

### 3:00 PM – 3:30 PM  ●  BREAK

### 3:30 PM – 5:00 PM  ●  SESSIONS

<table>
<thead>
<tr>
<th>TRACK A</th>
<th>TRACK B</th>
<th>TRACK C: HOT TOPICS II</th>
</tr>
</thead>
</table>
| **OS Security Mechanisms**  
Chair: Ed Schneider  
Institute for Defense Analyses, USA  
♣ Multi-level Security Requirements for Hypervisors  
Paul Karger, IBM T.J. Watson Research Center, USA  
♣ Building a MAC-based Security Architecture for the Xen Opensource Hypervisor  
Reiner Sailer, Trent Jaeger, Enriquillo Valdez, Ramon Caceres, Ronald Perez, Stefan Berger, John Griffin, and Leendert van Doorn, IBM T.J. Watson Research Center, USA  
♣ E-NeXSh: Achieving an Effectively Non-Executable Stack and Heap via System-Call Policing  
Gaurav Kc and Angelos Keromytis, Columbia University, USA | **Data Integrity**  
Chair: Randy Simpson  
Institute for Defense Analyses, USA  
♣ Dynamic Taint Propagation for Java  
Vivek Haldar, Deepak Chandra, and Michael Franz, University of California, Irvine, USA  
♣ An Integrity Verification Scheme for DNS Zone File Based on Security Impact Analysis  
Ramaswamy Chandramouli and Scott Rose, National Institute of Standards and Technology, USA  
♣ A Global Secure File Access Control System  
Fareed Zaffar and Gershon Kedem, Duke University, USA and Ashish Gehani, University of Notre Dame, USA | **Thinking of a Career in Information Assurance?**  
Chair: Marla Collier  
Internet Resources, USA  
As industry begins to invest more in Information Assurance (IA), there are numerous aspects of a career in IA worth exploring: Are certifications a smart career move? What is industry looking for today and in the future? If I want to do R&D, what do I need to know and what are the pluses/minuses of going corporate, academic or federal/state? Okay, I got hired in IA --- what next?  
- Wes Higaki- Symantec  
- J.F. Mergen- Verizon  
- Brian Snow- NSA/Government  
- Tom Fuhrman - Booz Allen |

### 5:00 PM – 5:30 PM  ●  BREAK

### 5:30 PM – 7:00 PM  ●  PLENARY SESSION

### Works in Progress

**Session Chair:** Mary Ellen Zurko, IBM Corporation, USA

The Works 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, Christoph Schuba, or the WIP Chair. Submitted topics will be announced at the Opening Plenary session and posted near the Conference Registration Desk.
## TCASAC TECHNICAL PROGRAM

### THURSDAY MORNING, December 8, 2005

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30 AM – 10:00 AM</td>
<td><strong>PLENARY SESSION</strong></td>
</tr>
<tr>
<td></td>
<td>Classic Papers</td>
</tr>
<tr>
<td></td>
<td>Session Chair: Charles Payne, Adventium Labs, USA</td>
</tr>
<tr>
<td></td>
<td><em>Looking Back on the Bell-LaPadula Model</em></td>
</tr>
<tr>
<td></td>
<td>David Elliott Bell</td>
</tr>
<tr>
<td></td>
<td><em>The Pump: A Decade of Covert Fun</em></td>
</tr>
<tr>
<td></td>
<td>Myong H. Kang, Ira S. Moskowitz, and Stanley Chincheck</td>
</tr>
<tr>
<td></td>
<td>Naval Research Laboratory, USA</td>
</tr>
<tr>
<td>10:00 AM – 10:30 AM</td>
<td><strong>BREAK</strong></td>
</tr>
<tr>
<td>10:30 AM – 12:00 PM</td>
<td><strong>SESSIONS</strong></td>
</tr>
<tr>
<td><strong>TRACK A</strong></td>
<td><strong>TRACK B: PANEL</strong></td>
</tr>
<tr>
<td>Malware</td>
<td>Highlights of the 2005 New Security Paradigms Workshop</td>
</tr>
<tr>
<td>Chair: Desiree A. Beck</td>
<td>Chair: Abe Singer</td>
</tr>
<tr>
<td>The MITRE Corporation</td>
<td>San Diego Supercomputer Center, USA</td>
</tr>
<tr>
<td>♠ Design and Implementation of an Extrusion-based Break-in Detector for Personal Computers</td>
<td></td>
</tr>
<tr>
<td>Weidong Cui and Randy Katz</td>
<td>University of California, Berkeley, USA, and Wai-tian Tan, Hewlett-Packard Laboratories, USA</td>
</tr>
<tr>
<td>♠ Detecting Intra-Enterprise Scanning Worms based on Address Resolution</td>
<td></td>
</tr>
<tr>
<td>David Whyte, Paul C. van Oorschot and Evangelos Kranakis, Carleton University, Canada</td>
<td></td>
</tr>
<tr>
<td>♠ Stealth Breakpoints</td>
<td></td>
</tr>
<tr>
<td>Amit Vasudevan and Ramesh Yerraballi, University of Texas at Arlington, USA</td>
<td></td>
</tr>
<tr>
<td><strong>TRACK C: Case Studies</strong></td>
<td></td>
</tr>
<tr>
<td>Security in Health Care</td>
<td></td>
</tr>
<tr>
<td>Chair: Alexis Feringa Booz Allen Hamilton, USA</td>
<td></td>
</tr>
<tr>
<td>♦ The OneHealthPort Trusted Community: Simplifying Access to Information for Healthcare</td>
<td></td>
</tr>
<tr>
<td>Ravi Sandhu, TriCipher Inc., USA</td>
<td></td>
</tr>
<tr>
<td>♦ Curing Secure Remote Access Pains</td>
<td></td>
</tr>
<tr>
<td>Zachary Grant, Sun Healthcare, USA</td>
<td></td>
</tr>
<tr>
<td>♦ Enterprise Single Sign-On: How City Hospital Cured Its Password Pain</td>
<td></td>
</tr>
<tr>
<td>David Ting, Imprivata, USA</td>
<td></td>
</tr>
<tr>
<td>12:00 PM – 1:30 PM</td>
<td><strong>LUNCH</strong></td>
</tr>
</tbody>
</table>
### Thursday Afternoon, December 8, 2005

**1:30 PM – 3:00 PM**

<table>
<thead>
<tr>
<th>SESSIONS</th>
<th>TRACK A</th>
<th>TRACK B</th>
<th>TRACK C: Case Studies</th>
</tr>
</thead>
</table>
| **Distributed System Security** | Chair: Michah Lerner  
IPMetric, USA | &bullet; **mSSL: Extending SSL to Support Data Sharing Among Collaborative Clients**  
Juni Li and Xun Kang, University of Oregon, USA | &bullet; **IPMetric, USA** |
| | &bullet; **Layering a Public-Key Distribution Service over Secure DNS**  
John Jones, Daniel Berger, and Chinya Ravishankar, University of California, Riverside, USA | &bullet; **Making User PKI Safe on Machines of Heterogeneous Trustworthiness**  
Sara Sinclair and Sean W. Smith, Dartmouth College, USA | &bullet; **Common Criteria**  
Chair: Audrey Dale  
NSA, USA |
| | &bullet; **Making User PKI Safe on Machines of Heterogeneous Trustworthiness**  
Sara Sinclair and Sean W. Smith, Dartmouth College, USA | &bullet; **Uniform Application-level Access Control Enforcement of Organization-wide Policies**  
Tine Verhanneman, Frank Piessens, Bart De Win and Wouter Joosen, Katholieke Universiteit Leuven, Belgium | &bullet; **Writing a Protection Profile for a Security Service Package**  
Don Marks and John Hale, Univ. of Tulsa, USA |
| | | &bullet; **Using Continuous Biometric Verification to Protect Interactive Login Sessions**  
Sandeep Kumar, Terence Sim, Rajkumar Janakiraman, and Sheng Zhang, National University of Singapore, Singapore | **MILS, Multiple Independent Levels of Security**  
Carol Taylor and Jim Alves-Foss, Univ. of Idaho, USA |
| | | &bullet; **Better Port Knocking with Strong Authentication**  
Rennie deGraaf, John Aycock, and Michael Jacobson, University of Calgary, Canada | &bullet; **A Comprehensive Review of the National Information Assurance Partnership**  
Ed Schneider, Institute for Defense Analyses, USA |
# ACSAC TECHNICAL PROGRAM

**THURSDAY AFTERNOON, December 8, 2005**

<table>
<thead>
<tr>
<th>3:30 PM – 5:00 PM</th>
<th>SESSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TRACK A</strong></td>
<td><strong>TRACK B</strong></td>
</tr>
<tr>
<td>Passwords and Applied Crypto</td>
<td>Defense in Depth/Database Security</td>
</tr>
<tr>
<td>Chair: Richard Smith</td>
<td>Chair: J. Thomas Haigh Adventium Labs and Cyber Defense Agency LLC, USA</td>
</tr>
<tr>
<td>University of St. Thomas, USA</td>
<td></td>
</tr>
<tr>
<td>Xiaoyuan Suo and Ying Zhu, Georgia State University, USA</td>
<td>Jennifer Chong, Partha Pal, Michael Atigetchi, Paul Rubel, and Franklin Webber, BBN Technologies, USA</td>
</tr>
<tr>
<td>♦ Have the Cake and Eat It Too – Infusing Usability into Text-Password Based Authentication Systems</td>
<td>♦ Generating Policies for Defense in Depth</td>
</tr>
<tr>
<td>Sundararaman Jeyaraman and Umut Topkara, Purdue University, USA</td>
<td>Paul Rubel, BBN Technologies, USA, and Michael Ihde, University of Illinois at Urbana-Champaign, USA, and Steven Harp and Charles Payne, Adventium Labs, USA</td>
</tr>
<tr>
<td>♦ Fault Attacks on Dual-Rail Encoded Systems</td>
<td>♦ Defensive Execution of Transactional Processes Against Attacks</td>
</tr>
<tr>
<td>Jason Waddle and David Wagner, University of California, Berkeley, USA</td>
<td>Meng Yu, Monmouth University, USA, and Peng Liu, Penn State University, USA and Wanyu Zang</td>
</tr>
</tbody>
</table>

**5:00 PM**

**ADJOURN**
OUTSTANDING PAPER AWARD
An annual prize for the Outstanding Paper is based on both the written paper and the oral presentation at the conference. A plaque and honorarium will be presented to the winning author.

To determine the Outstanding Paper, the Program Committee makes a preliminary selection of Outstanding Paper candidates. A subcommittee then attends the presentation of each candidate paper and 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.

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 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.

WORKS IN PROGRESS SESSION
The Works 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, Christoph Schuba, or the WIP Chair. Submitted topics will be announced at the Opening Plenary session and posted near the Conference Registration Desk.

TECHNOLOGY BLITZ
The Technology Blitz Session is a forum for participants that wish to disseminate practical research or operational results in an abbreviated format. This session is particularly well suited toward authors that do not have time to construct a full academic paper, yet still may provide useful insight into solutions for computer or networked computer security.

MEALS AND SPECIAL DIET REQUESTS
The Conference Committee has selected lunch menus that 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 upon 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.
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 20th Annual Conference (in 2004) for both Outstanding Paper and Outstanding Student Paper went to Shai Rubin, Somesh, and Jha Barton Miller of University of Wisconsin, Madison, USA for their paper Automatic Generation and Analysis of NIDS Attacks.


This year’s 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).

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 objectives of encouraging and facilitating dialogue and technical interchange.

To learn more about the conference, visit the ACSAC web page at www.acsac.org
To be added to the Conference Mailing List, visit us on the World Wide Web at www.acsac.org/list/
For questions, contact the committee members using the following E-mail addresses:

General_chair@acsac.org  Publicity_chair@acsac.org
CaseStudies_chair@acsac.org  Student_chair@acsac.org
Panel_chair@acsac.org  Tutorial_chair@acsac.org
Program_chair@acsac.org

If electronic contact is not possible, please write to ACSAC, 2906 Covington Rd, Silver Spring, MD 20910-1206, USA.
AC SAC-21
Tucson Marriott University Park, Tucson, Arizona
December 5-9, 2005

ATTENDEE INFORMATION Please TYPE or PRINT carefully.

First Name    Last Name    Nickname for Badge

Company/Organization

Address

City   State/Province Zip/Postal Code Country

Phone    Fax

Email

[ ] Check if you are a first-time attendee

FEES in US Dollars:

<table>
<thead>
<tr>
<th></th>
<th>On or Before Nov 16</th>
<th>After Nov 16, 2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular</td>
<td>$625</td>
<td>$725</td>
</tr>
<tr>
<td>Student</td>
<td>$325</td>
<td>$425</td>
</tr>
</tbody>
</table>

TECHNICAL PROGRAM - Circle applicable fee: $625 $325

TUTORIALS - Circle applicable tutorial numbers and fees:

- Full-day (circle one only): M1 M2 $550 $400 $650 $400
- Full-day (circle one only): F5 F6 $550 $400 $650 $400
- Half-day each: $325 $200 $375 $200
- Two half-days on same day: $550 $400 $650 $400

MONDAY WORKSHOP:
MALICIOUS SOFTWARE (PREVENTION & DEFENSE)
Circle to register for the workshop and lunch: $50

PAYMENT COMPUTATION

Technical Program Registration: $ __________
Full-day Tutorials: x $ __________ = $ __________
Half-day Tutorials: x $ __________ = $ __________
Workshop registration: $ __________
TOTAL COST: $ __________

METHOD OF PAYMENT

[ ] Personal or Company Check enclosed. Make checks payable to ACSAC-21.
[ ] VISA, MasterCard, American Express, or Discover, please provide the following information:

Card Number    Code*    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”

*Required: last 3-digit code on back of Visa/Mastercard signature tape or 4-digit code on front of American Express above card number. See the URL below for visual examples of how to locate this code
https://www.secure-server-hosting.com/secutran/secureforms/sh200566/verification.htm

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

ACSAC-21
Advance Registration Form
www.acsac.org

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?

[ ] Mailing
[ ] Previous ACSAC Conference
[ ] ACSAC Website
[ ] Friend
[ ] IEEE Security & Privacy Ad
[ ] Information Security magazine Ad
[ ] Publication: _____________________________
[ ] At Conference: _________________________
[ ] other: ________________________________

HOTEL REGISTRATION

ACSAC has reserved a block of rooms at the US Government per diem rate of $88.00 + 10.5% tax for Sunday - Saturday that will be honored until 5:00pm PST on 14 Nov 2005. The hotel room rate is subject to state and local taxes (which currently is 11.5% plus a $1.00 city surcharge), in effect at the time of check-in.

Registering for the Conference doesn’t reserve a room, so please call the Hotel Reservation Department at 1-520-792-4100 ext 2020 and request the Applied Computer Security Applications Conference group rate.

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-21
c/o Registration Systems Lab
779 East Chapman Road
Oviedo, FL 32765

or Fax it to: 407-366-4138

Refund Policy: No refunds will be provided after November 16, 2005. Conference registrations may be canceled before that date for a service charge of $25. Cancellations must be in writing and sent to ACSAC-21 using the address or fax number provided above.

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

acs05v05-050916