Advance Program

(Please note that times and dates of presentations may be subject to change in advance of release of the Final Program.)

Twenty-Third Annual Computer Security Applications Conference (ACSAC)

Practical Solutions To Real World Security Problems

December 10-14, 2007

Miami Beach Resort and Spa
Miami Beach, FL, USA

Presented by

ACSA

Applied Computer Security Associates

Conference and Registration Information	Invitation to ACSAC 23	Important Dates to Remember	Welcome from the Program Chairs	Conference Registration Form	Special Instructions for Foreign Visitors
Conference Location	Hotel Information	Reservations	Transportation to Miami Beach	Directions to the Conference Hotel	Meals and Special Diet Requests

Conference At-A-Glance

Monday 10 December	8:30-12:00	Tutorials		
	13:30-17:00	Tutorials		
Tuesday 11 December	8:30-17:00	Workshop: Software Assurance		
	8:30-12:00	Tutorials		
	13:30-17:00	Tutorials		
	18:00-20:00	Welcome Reception		
Wednesday 12 December	8:30-10:00	Distinguished Practitioner: *Richard Kemmerer*		
		Track 1	*Track 2*	*Track 3*
	10:30-12:00	Operating Systems Security and Trusted Computing	Malware and Intrusion Detection	Case Studies
	13:30-15:00	Database Security	New Security Paradigms	Case Studies
	15:00-17:00	Applied Cryptography	Misuse Detection and Forensics	Case Studies
	18:00-21:00	Dinner by the Pool		
Thursday 13 December	8:30-10:00	Invited Essayist: *Daniel Weitzner* and Classic Paper: *John Rushby*		
		Track 1	*Track 2*	*Track 3*
	10:30-12:00	Access Control	Wireless and Mobile Systems Security	DNI-DOD C&A Transformation Initiative-Part I
	13:30-15:00	Security Engineering	Electronic Voting Options	DNI-DOD C&A Transformation Initiative - Part II
	15:30-17:00	Security in P2P Systems	Works in Progress	Vulnerability Management and Secure System Configurations
Friday 14 December		*Track 1*	*Track 2*	*Track 3*
	8:30-10:00	Software and Application Security	Malware	Virtualization Security
	10:15-11:45	Assurance	Software Security	Distributed Systems Security
	12:00-18:00	Optional Social Event		

Awards and Opportunities	Best Student Paper Award	Best Paper Award	ACSA Conferenceship Program	Works in Progress (WiP) Session
Conference Committee	Program Committee	ACSAC Steering Committee	About the Sponsor	ACSA

Conference and Registration Information

Invitation to ACSAC 23

Welcome to the 23rd Annual Computer Security Applications Conference (ACSAC), a premier security conference of outstanding tradition. The 2007 conference is held in beautiful Miami Beach at the Miami Beach Resort and Spa, a classic location in this exclusive part of Miami, Florida.

It is a joy and an honor to invite you to attend this year's conference. The conference organizers and all volunteers, passionate about security and its future, have worked hard throughout the year to plan and organize this conference, so we can bring to you the most recent advances in security and the very best as speakers and presenters.

ACSAC offers a remarkable forum for computer and network security experts from industry, academia and government to meet, present and exchange ideas on recent security threats, vulnerabilities, and the solutions we can use or build to counter them. The overall focus is on applied, rather than theoretical, security, with an emphasis on managing security during the lifecycle of systems, not just using point solutions.

We will have several invited speakers, presenting topics of special impact and reach. John Rushby will discuss how the Randell-Rushby concepts are used in today's separation kernels and virtual machine monitors. Daniel Weitzner, well-known Internet public policy expert from MIT and Director of the World Wide Web Consortium's Technology and Society activities, will touch on the interplay between policy and security and privacy technology. Finally, Dick Kemmerer is this year's Distinguished Practitioner.

The conference also presents a significant number of case studies, panels, and a Works in Progress session. The presentations for all these will be available after the conference from the ACSAC website.

Again, welcome to the conference and we hope you will find it most useful and challenging, and come back next year for the 24th ACSAC in Anaheim, California.

Cristina Serban, PhD, CISSP
2007 ACSAC Conference Chair

Conference Registration
(Online or PDF Forms)

Important Dates to Remember

November 19, 2007: Last day to reserve a room at the conference hotel at the conference rate.

November 19, 2007: Last day for early/reduced conference registration fee.

November 19, 2007: Last day to cancel your conference registration and obtain a refund less a service charge of $25.00. Cancellations must be in writing. See the Registration Form for complete details.

Return to Top

Welcome from the Program Chairs

We invite you to the 23rd Annual Computer Security Applications Conference, held December 10-14, 2007, in Miami (FL), USA.

In response to the call for papers, 191 papers were submitted to the conference. These papers were evaluated on the basis of their significance, novelty, technical quality, and practical impact. As in previous years, reviewing was "double-blind": the identities of reviewers were not revealed to the authors of the papers and author identities were not revealed to the reviewers. The program committee meeting was held electronically, yielding intensive discussion over a period of two weeks. Of the papers submitted, 42 were selected for presentation at the conference, giving an acceptance rate lower than 22%. Besides the technical program composed of the papers collated in this proceedings, the conference includes invited talks, panels, case studies, and work in progress presentations.

A conference like this just does not happen; it depends on the volunteer efforts of a host of individuals. There is a long list of people who volunteered their time and energy to put together the workshop and who deserve special thanks. Thanks to all the members of the program committee, and the external reviewers, for all their hard work in the paper evaluation. Due to the large number of submission program committee members were really required hard work in a short time frame, and we are very thankful to them for the commitment they showed with their active participation in the electronic discussion. We are also very grateful to all those people whose work ensured a smooth organization process: Cristina Serban, for her support, advices and overall organization as General Chair, Carrie Gates, for taking care of publicity, Robert Zakon for maintaining the web pages and for support and help with the Openconf system, Richard Parker for preparing this program. Thank you also to all those people who served in different capacities for organizing the conference: Daniel Faigin for the tutorials, Tom Haigh for the invited talks, Paul Jardetzky for the panels, Steven Rome for the case studies, and John McDermott for the works in progress.

Last but certainly not least our thanks go to all the authors who submitted papers and all the attendees. We hope you find the program stimulating and a source of inspiration for your future research and practical development.

Pierangela Samarati, Charlie Payne
2007 ACSAC Program Chairs

Special Instructions for Foreign Visitors

If you are traveling from outside the United States, you may need to obtain a visa. Details on requesting a letter of invitation from ACSAC can be found at visa request.

Conference Location

Hotel Information

The conference will be held at the Miami Beach Resort and Spa (http://www.miamibeachresortandspa.com). (However, do not make your reservation at this site. Use http://www.acsac.org/hotel to get the ACSAC group rate.)

Reservations

REGISTER EARLY! ACSAC has reserved a block of rooms at Group Room Rates until November 19. The Single/double price will be derived from the prevailing US Government per diem, plus tax.

All reservations must be made directly with Miami Beach Resort and Spa.

- For online reservations, go to http://www.acsac.org/hotel to be linked to the ACSAC group rate rooms.
- For reservations by telephone, call: +1-877-597-9696.

Please be sure to associate your reservation with ACSAC. This makes the special negotiated room rates available to you and gives the conference a credit which helps to lower the registration fees.

> ***Please Note:*** *In order to receive the $100 Early Registration Discount towards your conference registration, you will need the hotel confirmation code that you receive when you reserve your room. (Please note that this discount is available only for conference registrations submitted on or before November 19, 2007.)*

The room rate is available three days before and after the conference if you would like to stay over one or both weekends.

CUTOFF DATE: *To qualify for the negotiated rates, hotel reservations by attendees must be received on or by Monday, November 19, 2007.*

Transportation to Miami Beach

Miami International Airport (http://www.miami-airport.com) is the closest airport (approximately 10 miles west of Miami Beach). For information on taxis and shuttle services: http://www.miami-airport.com/html/taxi_and_shuttle_service.html

Fort Lauderdale airport (http://www.broward.org/airport) is also convenient. It's approximately 30 minutes north of Miami Beach. Information on public transportation: http://www.miamidade.gov/transit/

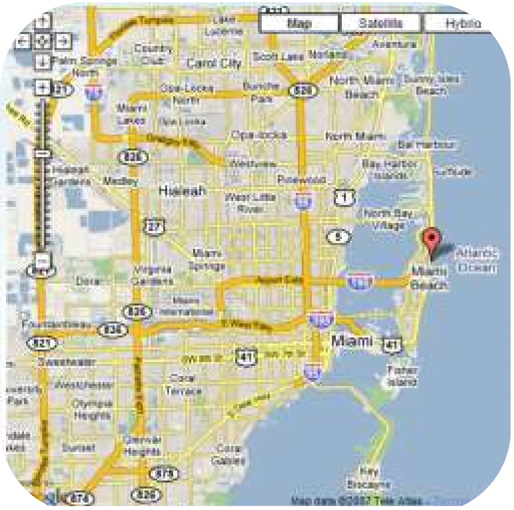
Official Miami Beach website: http://www.visitmiamibeach.us/

Return to Top

Directions to the Conference Hotel

- From Miami International Airport:
  - Exit Airport and follow the sign that says “Lejune Road North”
  - From Lejune Road North take the “112 East-Miami Beach” (second lane from right)
  - 112 East Miami Beach after the toll will become I-195 - Miami Beach
  - Once you are on I-195 go straight (always on the left lane) and after you pass the long bridge you will be on Arthur Godfrey Rd (also 41st Street)
  - Keep going until you see Indian Creek Drive, there you’ll make a left
  - Indian Creek will merge with Collins Avenue – proceed to 4833 Collins Avenue

- From Ft. Lauderdale / Hollywood International Airport:
  - Exit Airport to I-95 South
  - Take I-95 to I-195 Miami Beach
  - Once you are on I-195 go straight (always on the left lane) and after you pass the long bridge you will be on Arthur Godfrey Rd (also 41st Street)
  - Keep going until you see Indian Creek Drive, there you’ll make a left
  - Indian Creek will merge with Collins Avenue – proceed to 4833 Collins Avenue



4833 Collins Avenue, Miami Beach, Florida 33140

+1-877-597-9696

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.

Return to Top

Software Assurance Workshop

Chair: Harvey Rubinovitz, *The MITRE Corporation; Tuesday*, 11 December 2007, 8:30 a.m. - 4:30 p.m.

The disruption and economical loss due to software flaws, vulnerabilities, and malicious code is escalating. These flaws are exploited by attackers to compromise the enterprise's security. In many cases the same classes of flaws are exploitable in the same types of applications. For example, the Open Web Application Security Project (OWASP) has published the top ten security vulnerabilities in web applications.

Software assurance attempts to provide a metric to ensure that the software will consistently perform the same way it was intended, even when it comes under attack. These metrics/procedures can include tools used to build, assess, and test the software, and to fortify the environment where the software will be deployed.

This workshop will focus on Software Assurance, from how software developers can be better educated to the tools that are being used and further developed to improve the state of the art in software development. The workshop will also look at the need to facilitate the research and development of the next generation of Software Assurance standards and tools to assist in the creation of better assurance and more secure software.

Pre-registration is required. There is a registration fee to cover the cost of the workshop, lunch, and snack. Position papers are encouraged. To participate, contact Harvey Rubinovitz, Workshop Chair, The MITRE Corporation, M/S S145, 202 Burlington Road, Bedford, Massachusetts 01730; (781)-271-3076; hhr@mitre.org. If you are interested in attending please check off the appropriate box on the conference registration form and add in the workshop fee of $65 ($35 for students).

Tutorials

ACSAC is pleased to present nine tutorials this year on Monday, December 10, 2007 and Tuesday, December 11, 2007:

	Morning	Afternoon
Monday, December 10, 2007	**M1:** Web Services Security, Techniques and Challenges (Anoop Singhal, NIST & Gunnar Peterson, Arctec)	
	M2: Security Engineering (Steve Greenwald, Independent Consultant)	
	M3: Broadcast Encryption and Traitor Tracing for Content Protection (Hongxia Jin, IBM)	**M4:** Web Injection Attacks (V. N. Venkatakrishnan, University of Illinois at Chicago)
Tuesday, December 11, 2007	**T5:** Hands-on Web Application Security (Holger Peine, Fraunhofer-Institut Experimentelles Software-Engineering (IESE)	
	T6: ~~*Security Code Review for C and C++, High Assurance Applications*~~ - ***WITHDRAWN***	**T7:** Security Code Review for Java and J2EE Based Applications (Edward Tracy, Booz Allen Hamilton)
	T8: Botnets - Understanding and Defending (Bruce Potter, Booz Allen Hamilton)	**T9:** VoIP Security Analysis - Tools and Attacks (Siddhartha Gavirneni, Inter-Tel, Inc.)

If you are a CISSP, note that attendance at these tutorials can help you meet your continuing education requirements. See the descriptions that follow for more details about each tutorial, its instructor(s) and when it will be given Attendees enrolled in any of the tutorials are provided lunch on the day of their tutorial.

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.

Jump to Technical Program (skip detailed tutorial descriptions)

Tutorial M1

Web Services Security, Techniques and Challenges
Instructors: Dr. Anoop Singhal, *NIST* & Mr. Gunnar Peterson, *Arctec Group*
Time: Monday December 10, 2007 Full-Day Tutorial

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

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

Perimeter-based network security technologies (e.g., firewalls, intrusion detection) are inadequate to protect SOAs due to the following reasons:

- SOAs are dynamic, and can seldom be fully constrained to the physical boundaries of a single network
- SOAP protocol is transmitted over HTTP, which is allowed to flow without restriction through most firewalls. Moreover, TLS, which is used to authenticate and encrypt Web-based transactions, is unsuitable for protecting SOAP messages because it is designed to operate between two endpoints. TLS cannot accommodate Web services' inherent ability to forward messages to multiple other Web services simultaneously.

The SOA processing model requires the ability to secure SOAP messages and XML documents as they are forwarded along potentially long and complex chains of consumer, provider, and intermediary services. The nature of Web services processing makes those services subject to unique attacks, as well as variations on familiar attacks targeting Web servers.

Ensuring the security of Web services involves implementation of new security models based on use of authentication, authorization, confidentiality, and integrity mechanisms. This tutorial will discuss how to implement those security mechanisms in Web services. It also discusses how to make Web services and portal applications robust against the attacks to which they are subject. The following is a summary of some of the topics that will be discussed:

1. WS-Security
2. XML Security using XML Encryption and XML Signatures
3. Threats facing Web Services
4. Policy and Access control using WS-Policy, XACML and SAML
5. Security Management using WS-Trust
6. PKI for Web Services using XKMS
7. Secure Implementation Tools and Techniques
8. Recommendations for Web Services Security

Prerequisites: Participants should be familiar with concepts of network security and Web applications.

Return to Top

About the Instructors

Dr. Anoop Singhal is currently a Computer Scientist in the Computer Security Division at NIST. He has several years of Research experience at George Mason University, AT&T Labs and Bell Labs. As a Distinguished Member of Technical Staff at Bell Labs he has led several software projects in the area of Databases, Web Services and Network Management. He is a senior member of IEEE and he has published more than 20 papers in leading conferences and journals. He received his Ph.D. in Computer Science from Ohio State University, Columbus Ohio in 1985. He has given talks on Web Services Security in conferences such as ACSAC 2006 and RSA 2007.

Gunnar Peterson is a Managing Principal at Arctec Group. He is focused on distributed systems security for large mission critical financial, financial exchanges, healthcare, manufacturer, and insurance systems, as well as emerging start ups. Mr. Peterson is an internationally recognized software security expert, frequently published, an Associate Editor for IEEE Security & Privacy Journal on Building Security In, an Associate Editor for Information Security Bulletin, a contributor to the SEI and DHS Build Security In portal on software security, and an in-demand speaker at security conferences.

Tutorial M2

Security Engineering

Instructor: Dr. Steven J. Greenwald, *Independent Consultant*
Time: Monday December 10, 2007 Full-Day Tutorial

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

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

Prerequisites: None.

High Level Outline

1. A Quick Overview of Security Engineering Basics (1 hour).
2. Conventional Computer Security Issues (1 hour).
3. Hardware Engineering Aspects of Information Security (1 hour).
4. Attacks on Networks (1 hour).
5. Electronic Commerce (1 hour).
6. Policy, Management, and Assurance (1 hour)
7. Conclusions and General Q&A (½ hour).

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, and related areas. He also works with organizational security policy consulting, evaluation, training, and auditing.

Dr. Greenwald is also a Research Fellow of Virginia's Commonwealth Information Security Center (CISC) and an adjunct professor at James Madison University (an NSA Designated Center of Academic Excellence in Information Security Assurance) where he teaches several graduate courses for their M.S. degree in Computer `Science concentrating in INFOSEC.

Dr. Greenwald served as the 2001 General Chair of the New Security Paradigms Workshop (NSPW), has been past Program Chair for NSPW, and also serves on the program committees of other conferences. He is a member of the Association for Computer Machinery and the IEEE Computer Society. More information about him, including his publications, can be found at his web site at http://www.gate.net/~sjg6.

Return to Top

Tutorial M3

Broadcast Encryption and Traitor Tracing for Content Protection
Instructor: Dr. Hongxia Jin, *IBM Almaden Research Center*
Time: Monday Morning, December 10, 2007 Half-Day Tutorial

Today we live in a digital world. The advent of digital technologies has made the creation and manipulation of multimedia content simpler. It offers higher quality and a lot more convenience to consumers. For example, it allows one to make perfect copies. Furthermore, the rapid advance of network technologies, cheaper storage and larger bandwidth have enabled new business models on electronically distributing and delivering multimedia content. However, unauthorized music and movie copying are eating a big bite of the profit of the record industry and the movie studios. The success of these emerging business models hinges on the ability to only deliver the content to authorized customers. It is highly desirable to develop techniques to protect the copyrighted material and defend against piracy.

Broadcast encryption and traitor tracing are two technologies that have received extensive studies in cryptography literatures. Of course bringing them to practice is a different question. There are many issues that the theoretical community has overlooked in order to bring the solution to practice. Based on the author's firsthand experience on design, implementation and deployment of solutions for content protection, this introductory tutorial teaches security researchers and practitioners the basic key management and forensic techniques to protect copyright and defend against piracy in real world. The focus of this tutorial is on multimedia content. We cover from broadcast encryption, revocation, tracing traitors, emerging standards, state-of-the-art and state-of-the-practice key management and forensic approaches. The tutorial will cover the gap between state-of-art and practice and show our experience on how to bring a theoretical solution to practice.

The attendees will walk away with an understanding of the primary technologies that can be used for content protection, different types of potential pirate attacks and challenges associated with defending against each attack. Intermediate students will have the opportunity to get summary of existing key management and forensic techniques against different types of pirate attacks. Academic researchers will walk away with an understanding of challenges arising to bring a theoretical solution to practice as well as potential new research directions that have been largely overlooked from academia in this area. Industrial practitioners will walk away with an understanding of real world forensic systems, from design, legal issues, to adoption.

The tutorial handouts will include slides, an annotated bibliography consisting of leading references and landmark papers, and relevant URLs to standards.

Prerequisites: This tutorial is targeted at a beginner to intermediate audience; only basic background on cryptography is assumed.

High Level Outline

1. **Introduction**
   History of content protection systems, DRM, CCS system, New industry standards: 4C and AACS, Key Management Approaches
2. **Broadcast Encryption**
   Current State of the art; current state of practice, Matrix-based: CPRM, Tree-based: NNL, Potential attacks
3. **Forensic Technologies**
   Tracing Traitors for pirate decoder attack, Traitor tracing for anonymous attack, Emerging models
4. **Future of Content Protection**
   Research directions

About the Instructor

Dr. Hongxia Jin brings expertise in mainstream content protection technologies and first-hand design, implementation and deployment of key generation, management and forensic systems in real world.

Hongxia Jin obtained her Ph.D. degree in computer science from the Johns Hopkins University in 1999 and worked as a Research Staff Member for IBM research ever since.

Return to Top

She is currently at the IBM Almaden Research Center, where she is the leading researcher working on key management, broadcast encryption and traitor tracing technologies. The key management and forensic technologies she developed have been chosen as the core technologies by AACS, a new content protection industry standards for managing content stored on the next generation of pre-recorded and recorded optical media for consumer use with PCs and consumer electronic devices. She has filed a dozen patents in this area. She also published numerous papers and couple invited book chapters.

Tutorial M4

Web Injection Attacks
Instructor: Dr. V. N. Venkatakrishnan, *University of Illinois at Chicago*
Time: Monday Afternoon, December 10, 2007 Half-Day Tutorial

In September 2006, MITRE Corp., a corporation that runs three federally funded research and development centers, reported that Cross-Site Scripting and SQL Injection Attacks (SQLIA) are the two most common forms of web injection attacks in 2006. MITRE Corp. came to this conclusion after studying a list of more than 20,000 common vulnerability and exposures (CVE) for the year.

This tutorial will focus on Web injection attacks and defense strategies. We will focus on Cross Site Scripting (XSS) attacks and SQL injection attacks, while briefly discussing other forms of injection attacks.

Our discussion of web injection attack defense will include both vulnerability identification approaches and m attack prevention approaches. The former category consists of techniques that identify vulnerable locations in a web application that may lead to injection attacks. We will discuss several techniques (such as static analysis) for identifying vulnerable locations in a web application. We will then discuss numerous attack prevention mechanisms around a deployed application (such as taint based defenses) to prevent injection attacks.

This tutorial will cover both the state-of-art in research in these topics, as well as cover common industrial practices to address injection attacks. The tutorial will be addressed at a level that will engage both researchers and practitioners in system security.

Prerequisites: Some basic introduction in computer security is required.

High Level Outline

1. Introduction
2. Vulnerability identification mechanisms
3. Attack Detection Mechanisms
4. More advanced attacks
5. Q & A

About the Instructor

Dr. V. N. Venkatakrishnan is an Assistant Professor of Computer Science at the University of Illinois at Chicago. He is currently co-director of the Center for Research and Instruction in Technologies for Electronic Security at UIC. His main research area is in using programming language based techniques for systems security. Specific research topics include web security, mobile code security, techniques for enforcing confidentiality and integrity policies in applications. He received his PhD degree from Stony Brook University in 2004. He has won numerous awards including the best paper award at ACSAC 2003.

Return to Top

Tutorial T5

Hands-on Web Application Security
Instructor: Dr. Holger Peine, *Fraunhofer-Institut Experimentelles Software-Engineering (IESE)*
Time: Tuesday December 11, 2007 Full-Day Tutorial

Security breaches are discovered on a day-to-day basis in well-known and less well-known software, often covered in the media, and software vendors need to apply patching measures again and again that are both personnel-intensive and hurting their reputation. Since 2006, typical web application vulnerabilities like cross-site scripting and SQL injection occupy the top ranks of the security bug charts. Many of these problems could be avoided if application developers were better informed regarding the possible vulnerabilities and respective prevention measures for applications.

The goals of this tutorial are to:

- Get a feel for the numerous ways how security vulnerabilities can emerge in web applications
- Get to know the most important measures to prevent security vulnerabilities in web applications

This class introduces the most important security vulnerabilities of web applications and gives concrete advice how to avoid them. Vulnerabilities in the configuration of web servers (e.g. Apache, IIS) are not covered, nor are platform-specific vulnerabilities (e.g. J2EE, .NET). The class is performed in the form of frequently alternating between presentation by the instructor and hands-on implementation by the participants who will perform attacks on a live web application with about 20 known vulnerabilities by means of their web browser and a simple web proxy tool. Topics to be covered (see outline below) include recent trends like web services, Ajax, and CSRF.

Prerequisites: Participants should have a basic understanding of web technology (HTML, HTTP; will be reviewed shortly). **To participate actively in the hands-on exercises, participants should bring a computer with WLAN interface, install a web proxy ("WebScarab") on their computer, and familiarize themselves with some of its basic functions (software and instruction leaflet will be provided in advance).** Participants without their own computer can watch the instructor present the exercise's solution at the end of each exercise, or work with their seat neighbor. Instructor will bring server computer and wireless access point.

The web proxy software is implemented in Java and runs on virtually any computer. Installation requires no decisions from the user and does not require administrative rights; an uninstaller is included. The software does not, to our best knowledge, change any settings of the computer. Note, however, that ACSAC disclaims any liability for software installed as part of this course.

- WebScarab Instructions (PDF)
- WebScarab Installer (JAR)

High Level Outline

- Threats to web applications
- The demonstration application WebGoat
- User authentication: Why and how
- Protection of user sessions
- Page access restrictions
- Attacks by means of manipulated input data (SQL injection, cross-site scripting, and other injection attacks)
- Giving away sensitive information (error messages, HTML comments)
- Insecure error handling
- False trust in the browser
- Security implications of Ajax
- Cross-Site Request Forgery (CSRF)
- Interplay with web services
- Further reading

About the Instructor
Dr. Holger Peine works at the Fraunhofer-Institut Experimentelles Software-Engineering (IESE) in Kaiserslautern (Germany) in the security department, developing and evaluating security concepts and tools for software, systems, and processes. He leads a research task force on techniques and tools for measurably secure and safe software. Dr. Peine has taught this tutorial repeatedly, and has taught numerous classes to English-speaking audiences, including at ACSAC.

Return to Top

Tutorial T6

Security Code Review for Java and J2EE Based Applications

WITHDRAWN

Tutorial T7

Security Code Review for Java and J2EE Based Applications
Instructor: Edward Tracy, *Booz Allen Hamilton*
Time: Tuesday Afternoon December 11, 2007 Half-Day Tutorial

As Java is one of the predominant technologies for web applications, web services, and traditional desktop applications, many enterprises rely on it for application development. Yet, as with any custom code, Java developers are likely to make security errors largely due to ignorance and development processes that have not historically focused on security. Java source code review provides assurance about the security posture of your mission-critical applications.

This tutorial will provide a brief business case for code review, a technical overview of performing the code review, and a presentation on tools that can be used to conduct the review. Target audience is a technical lead for a code review team. However, entry-level reviewers will benefit from the specific technology guidance. And, CSOs and other management will benefit from the market discussion, process guidance, and takeaways.

Participants will walk away with specific guidance and checklists that cover low-level usage of Java, high-level Java and J2EE security libraries and tools, and usage of the popular application frameworks, Jakarta Struts and Acegi.

Prerequisites: Familiarity with Java technologies, be able to read code, know common frameworks.

High Level Outline

1. Business Case for Code Review & Market Discussion
2. Code Review of the Low-level Java Language
3. Code Review of Java / J2EE Security Packages
4. Code Review of High-level Security Mechanisms
5. Reviewing Struts and Acegi for Security
6. Process Outline for an Internal Review & 3rd-Party Review
7. Reporting Results, Risk, and Remediation
8. Overview of Tools to Augment Code Review

About the Instructor

Edward Tracy is a CISSP whose career has focused on the problem of application security, primarily with web applications. Edward began his career with the National Security Agency. He went on to co-found Aspect Security, Inc., a consulting firm that focuses on application security. Edward is now at Booz Allen Hamilton, where he is continuing to provide software security services and teach software security.

Edward is actively involved in industry efforts related to software security, including the Open Web Application Security Project (OWASP) and is the lead Java editor for the GIAC Secure Software Programmer certification.

Tutorial T8

Botnets - Understanding and Defending
Instructor: Bruce Potter, *Booz Allen Hamilton*
Time: Tuesday Morning, December 11, 2007 Half-Day Tutorial

Described by some as the largest threat to the global Internet, Botnets are largely hidden from the average Internet user. Botnets have a long legacy, and initially were not used for malicious purposes. However, as bots have evolved, they have taken on sinister uses. Using thousands of compromised machines, botnets can be used for a variety of tasks including sending mountains of spam, launching crushing Denial of Service attacks, or harvesting massive amounts of personal information. One of the unfortunate aspects of Botnets is that many individuals are active participants in botnets and do not even know it. Bots have become very sophisticated at hiding themselves from anti-virus and security programs. Also, many bots have even become resilient to large scale network security systems and represent problems to not just home users but to large enterprises as well.

This tutorial will provide the attendee with a broad view of the current Botnet problem and ways to defend systems from bot infections. We will initially focus on the history of botnets in order to understand the lineage of the problem we're dealing with today. Next, we will examine all ways in which this zombie networks are used including sending spam, harvesting personal data, and holding online organizations hostage. The tutorial will provide an analysis of the scope of the botnet problem and will examine some of the larger networks in existence today. Then, we will break down the internal structure of several common bots such as SDBot and GTBot in order to understand the inner workings of these programs. Finally, we will discuss both host-based and network-based defense techniques that will help keep your network bot free.

Prerequisites: Basic understanding of networking and operating systems.

High Level Outline

1. History of Botnets
2. Botnet Uses
3. Scope of Current Botnet Problem
4. Common Botnet structure
5. Host-based Botnet Defenses
6. Networked-based Botnet Defenses
7. Future of Botnets

About the Instructor

Bruce Potter is the founder of the Shmoo Group of security professionals, a group dedicated to working with the community on security, privacy, and crypto issues. His areas of expertise include wireless security, software assurance, pirate songs, and restoring hopeless vehicles. Mr. Potter has co-authored several books including "802.11 Security" and "Mastering FreeBSD and OpenBSD Security" published by O'Reilly and "Mac OS X Security" by New Riders. Mr. Potter was trained in computer science at the University of Alaska, Fairbanks. Bruce Potter is a Senior Associate with Booz Allen Hamilton.

Return to Top

Tutorial T9

VoIP Security Analysis - Tools and Attacks
Instructor: Siddhartha Gavirneni, *Inter-Tel, Inc.*
Time: Tuesday Afternoon December 11, 2007 Half-Day Tutorial

With the convergence of voice and data, an organization's telecom infrastructure and communications are at a higher risk than ever before. Before deploying VoIP, the organization needs to be aware of the security risks. As administrators, and security experts, how can we help protect an organization's VoIP infrastructure? This tutorial will help you understand some basic threats to SIP based VoIP. We will look at some tools that would help you analyze a VoIP product, and help you take steps to secure your VoIP network and infrastructure.

Prerequisites: Participants should be familiar with Networking and have a basic knowledge of VoIP (preferably SIP).

High Level Outline

1. Introduction
2. Some threats to VoIP - Overview and Examples
3. Brief overview of SIP
4. Some VoIP attack scenarios
5. System setup
6. VoIP Security Tools
7. Recommendations
8. Q and A Session

About the Instructor

Siddhartha Gavirneni is a software applications/systems engineer at Inter-Tel, Inc. He graduated from the University of Kansas with a Master of Science degree in Computer Engineering, with a focus on networking and security. He has been working on SIP based products at Inter-Tel for more than three years. Inter-Tel, Incorporated is a leading provider of voice and converged communications for businesses.

He has extensive experience teaching Information Security to grad students at the University of Kansas, and training network administrators in SIP and Inter-Tel products. He is Security+ certified, and is currently leading the security initiative for Inter-Tel products.

Tuesday, December 11, 2007, 18:00-20:00

Welcome Reception

Please drop by to meet your fellow attendees on Tuesday evening in the Regency Ballroom. Light appetizers will be provided and a cash bar will be available. We hope to see you there! Speakers and Session Chairs are particularly encouraged to take this opportunity to meet and chat.

Technical Program

Wednesday, December 12, 2007, 7:30-8:30

Registration and Continental Breakfast

Wednesday, December 12, 2007, 8:30-10:00

Opening Plenary

Introductory Remarks:

Cristina Serban*, AT&T,* Conference Chair
Pierangela Samarati, *Università degli Studi di Milano*, Program Chair

Distinguished Practitioner:

So You Think You Can Dance? Dr. Richard Kemmerer, University of California, Santa Barbara

This paper discusses the importance of keeping practitioners in mind when determining what research to pursue and when making design and implementation decisions as part of a research program. I will discuss how my 30 plus years of security research have been driven by the desire to provide products, tools, and techniques that are useful by practitioners. I will also discuss my view of what new security challenges the future has in store for us.

About the Speaker:
Richard A. Kemmerer is the Computer Science Leadership Professor and a past Department Chair of the Department of Computer Science at the University of California, Santa Barbara. Dr. Kemmerer received the B.S. degree in Mathematics from the Pennsylvania State University in 1966, and the M.S. and Ph.D. degrees in Computer Science from the University of California, Los Angeles, in 1976 and 1979, respectively. His research interests include formal specification and verification of systems, computer system security and reliability, programming and specification language design, and software engineering. He is author of the book Formal Specification and Verification of an Operating System Security Kernel and a co-author of Computers at Risk: Safe Computing in the Information Age, For the Record: Protecting Electronic Health Information, and Realizing the Potential of C4I: Fundamental Challenges.

Dr. Kemmerer is a Fellow of the IEEE Computer Society, a Fellow of the Association for Computing Machinery, a member of the IFIP Working Group 11.3 on Database Security, and a member of the International Association for Cryptologic Research. He is a past Editor-in-Chief of IEEE Transactions on Software Engineering and has served on the editorial boards of the ACM Computing Surveys and IEEE Security and Privacy. He currently serves on the Board of Governors of the IEEE Computer Society and on Microsoft's Trustworthy Computing Academic Advisory Board.

Return to Top

Wednesday, December 12, 2007, 10:30-12:00

Track 1: Technical Papers

Operating Systems Security and Trusted Computing

Establishing and Sustaining System Integrity via Root of Trust Installation
Luke St. Clair, Joshua Schiffman, Trent Jaeger, Patrick McDaniel; *Pennsylvania State University*

Tampering with Special Purpose Trusted Computing Devices: A Case Study in Optical Scan E-Voting
Aggelos Kiayias, Laurent Michel, Alexander Russel, Narasimha Sashidar, Andrew See; *University of Connecticut*

Toward a Medium-Robustness Separation Kernel Protection Profile
Rance DeLong; *Santa Clara University*
Thuy Nguyen, Cynthia Irvine, Timothy Levin; *Naval Postgraduate School*

Track 2: Technical Papers

Malware and Intrusion Detection

Improving Signature Testing Through Dynamic Data Flow Analysis
Christopher Kruegel; *Technical University Vienna*
Davide Balzarotti, William Robertson, Giovanni Vigna; *UC Santa Barbara*

HoneyIM: Fast Detection and Suppression of Instant Messaging Malware in Enterprise-like Networks
Mengjun Xie, Zhenyu Wu, Haining Wang; *College of William and Mary*

Feature Omission Vulnerabilities: Thwarting Signature Generation for Polymorphic Worms
Matthew Van Gundy, Hao Chen, Zhendong Su; *University of California, Davis*
Giovanni Vigna; *University of California, Santa Barbara*

Track 3: Case Studies

Protecting data privacy from the power of the database administrator
Barbara Banks; *SYBASE*

Coalition Warrior Interoperability Demonstration (CWID) 2007: A Case Study in International Cross-Domain Network Communications secured by strategic deployment of one-way data transfer systems
Jeffrey Menoher; *Owl Computing Technologies, Inc.*

A Case-Study of a Control System Cyber Security Event
Marshall Abrams; *The MITRE Corporation*

Wednesday, December 12, 2007, 12:00-13:30

Lunch

Wednesday, December 12, 2007, 13:30-15:00

Track 1: Technical Papers

Database Security

Toward Realistic and Artifact-Free Insider-Threat Data
Kevin Killourhy, Roy Maxion; *Carnegie Mellon University*

Database Isolation and Filtering against Data Corruption Attack
Meng Yu, Wanyu Zang; *Western Illinois University*
Peng Liu; *The Pennsylvania State University*

Sania: Syntactic and Semantic Analysis for Automated Testing Against SQL Injection
Yuji Kosuga, Kenji Kono, Miyuki Hanaoka; *Keio University*
Miho Hishiyama; Yu Takahama, *IX Knowledge Inc.*

Track 2: Panel

New Security Paradigms

Chair: Matt Bishop; *UC Davis*

This panel presents a selection of the best, most interesting, and most provocative work from the New Security Paradigms Workshop 2007. For fifteen years, the New Security Paradigms Workshop (NSPW) has provided a productive and highly interactive forum for innovative new approaches to computer security.

The panel presentations and discussions are intended to capture the lively interaction and debate that occurs between audience and panel members during an NSPW presentation. Each panelist will be given just five minutes of uninterrupted `formal' presentation time. The formal presentation of each panelist is deliberately short; it is intended to ensure that their paradigm thesis will be immediately accessible to the audience and thus encourage interaction from the audience.

Track 3: Case Studies

Wireless Intrusion Detection System (WIDS) Technology Transfer Case Study
Patrick Vescio; *Dolphin Technology*

Knowing what you don't know - X-Raying enterprise networks for malware
Samantha Madrid; *CISCO*

Emerging IT Trends and their Implications to the C&A Process
Ed Rodriguez; *Booz Allen Hamilton*

Return to Top

Wednesday, December 12, 2007, 15:30-17:00

Track 1: Technical Papers

Applied Cryptography

Closed-Circuit Unobservable Voice over IP
Carlos Aguilar Melchor; *XLIM, Université de Limoges*
Yves Deswarte; *LAAS-CNRS, Université de Toulouse*
Julien Igutchi-Cartigny; *XLIM, Université de Limoges*

SSARES: Secure Searchable Automated Remote Email Storage
Adam J. Aviv, Michael E. Locasto, Shaya Potter, Angelos D. Keromytis; *Columbia University*

Track 2: Technical Papers

Misuse Detection and Forensics

The Design and Development of an Undercover Multipurpose Anti-Spoofing Kit (UnMask)
Sudhir Aggarwal, Jasbinder Bali, Zhenhai Duan, Leo Kermes, Wayne Liu; *Florida State University*

Efficiency Issues of Rete-based Expert Systems for Misuse Detection
Michael Meier, Ulrich Flegel; *University of Dortmund*
Sebastian Schmerl; *Brandenburg University of Technology Cottbus*

Tracking Darkports for Network Defense
David Whyte, Paul van Oorschot,
Evangelos Kranakis; *Carleton University*

Track 3: Case Studies

DETER Testbed for Security Experimentation
Jelena Mirkovic; *USC*

Anatomy of Denial of Service Attack and Defense in a Lab Environment
Dongqing Yuan, Jinling Zhong; *Fairmont State University*

Secure Integration of Military and Civilian C2
John A. Sturm; *NuParadigm Government Systems*

Wednesday, December 12, 2007, 18:00-21:00

Dinner at the Pool

Weather permitting, please plan to join us for a buffet dinner poolside (we will dine in the Starlight Ballroom in case of rain.)

Return to Top

Thursday, December 13, 2007, 7:30-8:30

Registration and Continental Breakfast

Thursday, December 13, 2007, 8:30-10:00

Invited Essayist and Classic Paper Plenary

Invited Essayist:

Daniel J. Weitzner, *CSAIL Decentralized Information Group, Massachusetts Institute of Technology*

Personal privacy without computational obscurity: Rethinking privacy protection strategies for open information networks

Throughout the history of computer and network security research, privacy has been treated as synonymous with confidentiality, with the presumed high water mark of privacy being mathematically-provable anonymity. Despite the fact that technical innovation in cryptography and network security has enabled all manner of confidentiality control over the exposure of identity in information systems, the vast majority of Internet users remain deeply worried about their privacy rights and correctly believe that they are far more exposed today than they might have been a generation earlier. Have we just failed to deploy the proper security technology to protect privacy, are our laws inadequate to meet present day privacy threats, or have business practices and social conventions simply rendered privacy dead? While there is some truth to each possibility, the central failure to achieve robust privacy in the information age can be traced to an a long-standing mis-association of privacy with confidentiality and access control. In order to revitalize privacy protection, we should shift our legal attention away from rules limiting disclosure of personal information toward policies governing how personal information can be used. And technical efforts currently focused on access control and anonymization should be redirected toward technical measures that make information usage more transparent and accountable to clearly stated policies that address proper and improper uses of personal information.

About the Speaker:

Daniel Weitzner is Co-Director of the MIT CSAIL Decentralized Information Group, teaches Internet public policy in the Electrical Engineering and Computer Science Department, and is Policy Director of the World Wide Web Consortium's Technology and Society activities. At DIG he leads research on the development of new technology and public policy models for addressing legal challenges raised by the Web, including privacy, intellectual property, identity management and new regulatory models for the Web. At W3C he is responsible for Web standards needed to address public policy requirements, including the Platform for Privacy Preference (P3P) and XML Security technologies. He was the first to advocate user control technologies such as content filtering to protect children and avoid government censorship. These arguments played a critical role in the landmark Internet freedom of expression case in the United States Supreme Court, Reno v. ACLU (1997). In 1994, his advocacy work won legal protections for email and web logs in the US Electronic Communications Privacy Act.

Weitzner was co-founder and Deputy Director of the Center for Democracy and Technology, and Deputy Policy Director of the Electronic Frontier Foundation. He serves on the Boards of Directors of the Center for Democracy and Technology, the Software Freedom Law Center, and the Internet Education Foundation.

Weitzner has law degree from Buffalo Law School, and a B.A. in Philosophy from Swarthmore College. His writings have appeared in Science magazine, the Yale Law Review, Communications of the ACM, Computerworld, Wired Magazine, Social Research, Electronic Networking: Research, Applications & Policy, and The Whole Earth Review.

Return to Top

Thursday, December 13, 2007, 8:30-10:00

Invited Essayist and Classic Paper Plenary

Classic Paper

Distributed Secure Systems: Then and Now

John Rushby, *Computer Science Laboratory, SRI International*

The early 1980s saw the development of some rather sophisticated distributed systems. These were not merely networked file systems: rather, using remote procedure calls, hierarchical naming, and what would now be called middleware, they allowed a collection of systems to operate as a coherent whole. One such system in particular was developed at Newcastle which allowed pre-existing applications and (Unix) systems to be used, completely unchanged, as components of an apparently standard large (multi-processor) Unix system.

The Distributed Secure System (DSS) described in our 1983 paper proposed a new way to construct secure systems by exploiting the design freedom created by this form of distributed computing. The DSS separated the security concerns of policy enforcement from those due to resource sharing and used a variety of mechanisms (dedicated components, cryptography, periods processing, separation kernels) to manage resource sharing in ways that were simpler than before.

In this retrospective, we provide the full original text of our DSS paper, prefaced by an introductory discussion of the DSS in the context of its time, and followed by an account of the subsequent implementation and deployment of an industrial prototype of DSS, and a description of its modern interpretation in the form of the MILS architecture. We conclude by outlining current opportunities and challenges presented by this approach to security.

About the Speaker:

John Rushby received B.Sc. and Ph.D. degrees in computing science from the University of Newcastle upon Tyne in 1971 and 1977, respectively. He joined the Computer Science Laboratory of SRI International in 1983, and served as its director from 1986 to 1990; he currently manages its research program in formal methods and dependable systems, which develops the highly regarded and widely used PVS verification system, the SAL suite of model checkers, and the Yices SMT solver. Prior to joining SRI, he held academic positions at the Universities of Manchester and Newcastle upon Tyne in England. His research interests center on the use of formal methods for problems in the design and assurance of secure and dependable systems.

Dr. Rushby is a former associate editor for Communications of the ACM, IEEE Transactions on Software engineering, and Formal Aspects of Computing. He is the author of the (now rather outdated) chapter on formal methods for the FAA Certification Handbook, and a member of a National Research Council study that recently delivered its report "Software for Dependable Systems: Sufficient Evidence?". His publications are available online at http://www.csl.sri.com/users/rushby/biblio.html

Return to Top

Thursday, December 13, 2007, 10:30-12:00

Track 1: Technical Papers

Access Control

Extensible Pre-Authentication Kerberos
Phillip Hellewell, Tim van der Horst, Kent Seamons; *Brigham Young University*

Quarantining Untrusted Entities: Dynamic Sandboxing using Mandatory Access Controls
Manigandan Radhakrishnan, Jon Solworth; *University of Illinois at Chicago*

Retrofitting the IBM POWER Hypervisor to Support Mandatory Access Control
Enriquillo Valdez, Reiner Sailer, Ronald Perez; *IBM T. J. Watson Research Center*

Track 2: Technical Papers

Wireless and Mobile Systems Security

Extending the Java Virtual Machine to Enforce Fine-Grained Security Policies in Mobile Devices
Iulia Ion, Boris Dragovic; *CREATE-NET*
Bruno Crispo; *University of Trento*

Countering False Accusations and Collusion in the Detection of In-Band Wormholes
Daniel Sterne; *SPARTA*
Richard Gopaul; *U.S. Army Research Laboratory*
Geoffrey Lawler, Peter Kruus; *SPARTA*

Localized Multicast: Efficient Distributed Detection of Node Replication Attacks in Sensor Networks
Bo Zhu, Gopal Addada, Sanjeev Setia, Sushil Jajodia, Sankardas Roy; *George Mason University*

Track 3: Case Studies

DNI-DOD C&A Transformation Initiative-Part I
Building a Common Information Security Foundation

Sharon Ehlers (ODNI); Gary Stoneburner (Johns Hopkins APL); DOD Representative (Invited)

The Chief Information Officers from the Office of the Director of National Intelligence (ODNI) and the Department of Defense launched a Certification and Accreditation (C&A) Transformation Initiative in June 2006. The transformation goals focused on developing a unified approach to information security for the Intelligence Community and the Defense Department and included plans to develop a common risk management framework, common security categorization approach, common security controls, and a common lexicon of terminology. The unified framework for information security will form the basis for significant improvements to the current C&A process. This session will report on the latest results of the transformation initiative in all key areas of the project.

Thursday, December 13, 2007, 12:00-13:30

Lunch

Return to Top

Thursday, December 13, 2007, 13:30-15:00

Track 1: Technical Papers

Security Engineering

Exploring Design Principles for Usable Security

Audun Josang; *Queensland University of Technology*
Tyrone Grandison; *IBM Almaden Research*
Bander Alfayyadh, Mohammed Alzomai, Judith McNamara; *Queensland University of Technology*

Breaking Visual CAPTCHAs with Naïve Pattern Recognition Algorithms

Jeff Yan, Ahmad Salah El Ahmad, *Newcastle University*

Combining Static and Dynamic Analysis for Automatic Identification of Precise Access-Control Policies

Paolina Centonze; *IBM T. J. Watson Research Center*
Robert J. Flynn; *Polytechnic University*
Marco Pistoia; *IBM T. J. Watson Research Center*

Track 2: Panel

Electronic Voting Options

Chair: Jeremy Epstein, *Software AG*

Electronic voting is a perennial hot topic. In this forum, speakers from several points of view will address key areas including:

- A review of the different categories and models of voting machines currently available in the US and a quick overview of the related security risks.
- Relative difficulties of auditing and security breaches in human vs. semiautomated vs. automated systems at granularities for coercion, auditing, retail vs. wholesale fraud etc.
- Challenges to conducting election recounts, as typified by the phrase "hanging chad", from the recount process in 2000
- Language access issues in electronic voting systems, an especially critical issue in Florida and other states with large immigrant populations.

Panelists:

Dr. Barbara Simons; *ACM*

Dr. Alec Yasinsac; *Florida State University*

Linda Rodriguez-Tassef; *Duane Morris LLP*

Track 3: Case Studies

DNI-DOD C&A Transformation Initiative - Part II

Transition Strategies and Implementation Issues

Anthony Cornish (CNSS); Mark Morrison (DIA); Dennis Heretick (DOJ)

The DNI-DOD Certification and Accreditation (C&A) Transformation Initiative has completed its initial development work in building a unified framework for information security for the Intelligence Community and the Department of Defense. This session focuses on how organizations that will be affected by the transformation initiative plan to develop transition strategies to adopt the new policies when implemented, including common approaches for managing enterprise risk, categorizing information systems based on mission/business function impact, developing security plans using common security controls, and employing common assessment methodologies to determine control effectiveness. Significant implementation issues will also be addressed and proposed solutions discussed.

Return to Top

Thursday, December 13, 2007, 15:30-17:00

Track 1: Technical Papers

Security in P2P Systems

Routing in the Dark: Pitch Black
Nathan Evans, Christian Grothoff, Chris Gauthier Dickey; *University of Denver*

Centralized Security Labels in Decentralized P2P Networks
Nathalie Tsybulnik, Kevin W. Hamlen, Bhavani Thuraisingham; *University of Texas at Dallas*

A Taxonomy of Botnet Structures
David Dagon`, Guofei Gu, Christopher P. Lee, Wenke Lee; *Georgia Institute of Technology*

Track 2: Works in Progress Session

Chair: John McDermott; *NRL*

Works in progress to be presented include the following:

A methodology to build secure systems using patterns - Eduardo B. Fernandez

Development of a cyber incident mission impact assessment methodology - Michael Grimaila

Towards securing inter-device communication: applying inter-device authentication and authorization framework to home appliances - Manabu Hirano, Takeshi Okuda, and Suguru Yamaguchi

EXAMIN: Tools for malware incubation - Steve Brueckner, Greg Durrett, and Hajime Inoue

Design and implementation of a portable educational network to teach cyber security curricula and digital forensics at a community college - Donna Kaputa

Towards a high assurance multi-level secure off-the-shelf PC - David Kleidermacher

Reducing vulnerabilities in software: a European approach - Per Håkon Meland, Jostein Jensen and Lillian Røstad

The Secflow source code security checker: current problems and solution alternatives - Holger Peine and Stefan Mandela

Dynamic, intelligent and adaptable access control - Lillian Røstad, Gunnar René Øie, Øystein Nytrø

Network security analysis using attack graphs - Anoop Singhal, Lingyu Wang, and Sushil Jajodia

Correlating packet timing with memory content detects IP covert timing channels - Richard Stillman

Secure biometric network protocol - Bobby L. Tait and S.H. Von Solms

fakePointer: a user authentication scheme that makes peeping attack with a video camera hard - Tetsuji Takada

Security analysis of the native code in Sun's JDK - Jason Croft and Gang Tan

Social engineering: where's the research? - Carol Taylor

Track 3: Case Studies

Vulnerability Management and Secure System Configurations

Current Activities of the National Vulnerability Database and Information Security Automation Program

Peter Mell, NIST; Daniel Schmidt, NSA

The National Vulnerability Database (NVD) is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). SCAP is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). The NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics and also supports the Information Security Automation Program (ISAP). ISAP is a U.S. government multi-agency initiative to enable automation and standardization of technical security operations. This session will provide information on the latest activities of the NVD, ISAP, and SCAP.

The final Works in Progress Program will be available in the Conference Registration Area as well as at the WiP Session location.

Return to Top

Friday, December 14, 2007, 7:30-8:30

Registration and Continental Breakfast

Friday, December 14, 2007, 8:30-10:00

Track 1: Technical Papers

Software and Application Security

Secure Input for Web Applications
Martin Szydlowski, Engin Kirda, Christopher Kruegel; *Vienna University of Technology*

Secure and Flexible Monitoring of Virtual Machines
Bryan Payne, Martim Carbone, Wenke Lee; *Georgia Institute of Technology*

Automated Format String Attack Prevention for Win32/X86 Binaries
Wei Li, Tzi-cker Chiueh; *Stony Brook University*

Track 2: Technical Papers

Malware

MetaAware: Identifying Metamorphic Malware
Qinghua Zhang, Douglas Reeves; *North Carolina State University*

Limits of Static Analysis for Malware Detection
Andreas Moser, Christopher Kruegel, Engin Kirda; *Vienna University of Technology*

OmniUnpack: Fast, Generic, and Safe Unpacking of Malware
Lorenzo Martignoni, *Università degli Studi di Milano*
Mihai Christodorescu; *IBM Research*
Somesh Jha; *University of Wisconsin, Madison*

Track 3: Panel

Virtualization Security

Chair: Christoph Schuba, Sun Microsystems, Inc.

On a virtualized platform, operating system instances are hosted within an execution environment that's controlled by a virtual machine monitor. Physical resources, such as memory, CPU, trusted platform modules, networking interfaces, etc. are no longer under the single control of an operating system, but are shared among the guest OS instances and primarily controlled by the virtual machine monitor.
While much work has been done in the past on topics such as separation kernels and secure hypervisor technologies, it is time to revisit the topic as a small number of OS virtualization technologies (Xen hypervisor, VMWare, Solaris containers) are becoming widely adopted in the industry.
This panel aims at understanding e.g., which security guarantees and features are provided by these popularity-gaining vm technologies. What is their current state of the art with respect to containment, secure migration, scalable administration, or hardware-rooted trust - and what can we expect in their roadmap.

Panelists:
Tal Garfinkel; *Stanford University and VMWare*
Reiner Sailer; *IBM Watson*
Andy Warfield; *University of British Columbia*
John McDermott; *Naval Research Laboratory*

Return to Top

Friday, December 14, 2007, 10:15-11:45

Track 1: Technical Papers

Assurance

Runtime System Infrastructure for Practical Application Development
Boniface Hicks, Tim Misiak, Patrick McDaniel; *Penn State*

Automated Security Debugging Using Program Structural Constraints
Chongkyung Kil, Emre Can Sezer, Peng Ning; *North Carolina State University*
Xiaolan Zhang, *IBM*

Static And Dynamic Information Flow In A Java Virtual Machine
Michael Franz, Deepak Chandra; *University of California, Irvine*

Track 2: Technical Papers

Software Security

Automated Vulnerability Analysis: Leveraging Control Flow for Evolutionary Input Crafting
Sherri Sparks, Shawn Embleton, Ryan Cunningham, Cliff Zou; *University of Central Florida*

The Age of Data: pinpointing guilty bytes in polymorphic buffer overflows on heap or stack
Asia Slowinska, Herbert Bos; *Vrije Universiteit, Amsterdam*

Spector: Automatically Analyzing Shell Code
Kevin Borders, Atul Prakash; *University of Michigan*
Mark Zielinski; *Arbor Networks*

Track 3: Technical Papers

Distributed Systems Security

An Overview of the Annex System
Duncan Grove, Toby Murray, Chris Owen, Chris North, Jeremy Jones; *DSTO*

Efficient Detection of Delay-Constrained Relay Nodes
Baris Coskun, Nasir Memon; *Polytechnic University*

Bonsai: Balanced Lineage Authentication
Ashish Gehani, Ulf Lindqvist; *SRI*

Conference Adjourns

Friday, December 14, 2007, 12:00-18:00

Optional Social Event: ACSAC Miami & Everglades Excursion

Please join us for a double dose of Miami culture and nature on Friday afternoon, December 14, 2007.

1. Lunch at the *Little Havana* landmark restaurant, **Versailles**. The food just doesn't get any more Cuban than at Versailles. Versailles has the best Cuban food and pastries in town with the most authentic Cuban flavor. It's a Miami institution and everyone who visits Miami should experience Versailles' food and ambience in order to really say they have truly visited Miami! Our menu includes Appetizers (fried yucca, plantain chips with Mojo sauce), your choice of either Roast Pork Cuban Style (marinated and slow roasted and served boneless with moros rice, fried plantains, and garlic bread) or the Cuban classic Chicken with Yellow Rice (*arroz con pollo*, served with fried plantains and garlic bread), Soft Drink or Coffee (try the Cuban espresso-style coffee for a jolt to your nervous system), and Dessert (flan, a type of Cuban custard).

2. Next, experience South Florida's delicate ecological system as we visit Everglades Safari Park (http://www.evsafaripark.com/) including an exhilarating airboat ride through the Everglades National Park to see a unique ecosystem and some of Mother Nature's most exotic wildlife! See alligators, birds, and other local wildlife in their natural habitat! Journey into the Everglades preserved wilderness made up of 1.2 million acres of grasslands and hardwood hammocks aboard an airboat. A professional tour guide will narrate your thrilling airboat ride as you glide through this wilderness: the legendary Everglades National Park. Our tour guide will lead us through this natural wonder where we will encounter breathtaking panoramic views, lush vegetation and tranquility. You will be amidst alligators, native flora and fauna and other exotic wildlife in their habitat as you thrust through this *River of Grass* most unique ecosystem.

Everglades Safari Park's Main Attractions:

- 30-40 minute Airboat Ride,
- Alligator Wildlife Nature Show,
- Jungle Trail, Observation Platform & Exhibits.

Price: $55.00 per person. Price includes bus transportation from and back to the *Miami Beach Resort & Spa*, a delicious Cuban lunch, and admission to the Everglades Safari Park. We leave at 12 noon sharp! Return by 6:00 pm.

Wear comfortable shoes since some light walking is required. Be sure to bring your camera and sunscreen.

Awards and Opportunities

Best 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, a set of best paper candidates is selected based on the recommendation of the Program Committee. 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.

Best 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. Conferenceships can be requested by any student and will be awarded to students that will get the most from ACSAC. However, conferenceship will be awarded first to students that are author of papers and that have a co-author also attending ACSAC. The conferenceship will cover registration, 4 nights at the conference hotel, and $400 (North America Student)/$700 (International Student). The amount above is to cover airline tickets and other expenses, and require a copy of the airline ticket receipt.

To be considered for the Conferenceship Program, please submit the following information to the Student Awards Chair at 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 15.

Works in Progress (WiP) 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.

Return to Top

Program Committee

- **Pierangela Samarati** (PC Chair), *Università degli Studi di Milano*
- **Charles Payne** (PC Co-Chair), *Adventium Labs*
- **Tuomas Aura**, *Microsoft Research, UK*
- **Lujo Bauer**, *Carnegie Mellon University*
- **David Elliott Bell**, *Selfless Security*
- **Terry Benzel**, *USC - ISI*
- **Konstantin Beznosov**, *University of British Columbia*
- **Rafae Bhatti**, *Florida International University*
- **Sabrina De Capitani di Vimercati**, *Università degli Studi di Milano*
- **Marc Dacier**, *Eurecom Institute*
- **Mary Denz**, *Air Force Research Laboratory*
- **Jan Eloff**, *University of Pretoria*
- **Philip Fong***, University of Regina*
- **Sara Foresti**, *Università degli Studi di Milano*
- **Michael Franz**, *University of California, Irvine*
- **Carrie Gates**, *CA Labs*
- **Dieter Gollmann**, *Hamburg University of Technology*
- **Steven J. Greenwald**, *Independent Consultant*
- **Tom Haigh**, *Adventium Labs*
- **Wesley Higaki**, *Symantec Corporation*
- **Thomas Hinke**, *NASA Ames Research Center*
- **Cynthia Irvine**, *Naval Postgraduate School*
- **Sushil Jajodia**, George *Mason University*
- **Jan Jürjens**, *TU München*
- **Myong Kang**, *Naval Research Laboratory*
- **Angelos Keromytis**, *Columbia University*
- **Wenke Lee**, *Georgia Tech*
- **Ulf Lindqvist**, *SRI International*
- **Peng Liu**, *Pennsylvania State University*
- **Javier Lopez**, *University of Malaga*
- **Bryan Lyles**, *Telcordia Technologies*
- **Patrick McDaniel**, *Pennsylvania State University*
- **John McDermott**, *Naval Research Laboratory*
- **Jelena Mirkovic**, *University of Delaware*
- **Peng Ning**, *North Carolina State University*
- **Paul Van Oorschot**, *Carleton University*
- **Stefano Paraboschi**, *Università di Bergamo*
- **Joon Park**, *Syracuse University*
- **Lillian Røstad**, *Norwegian University of Science and Technology*
- **Reiner Sailer**, *IBM T.J. Watson Research Center*
- **Andre Dos Santos**, *University of Puerto Rico at Mayagüez*
- **Christoph Schuba**, *Sun Microsystems, Inc.*
- **Kent Seamons**, *Brigham Young University*
- **Anoop Singhal**, *National Institute for Standards and Technology*
- **Carol Taylor**, *University of Idaho*
- **Dan Thomsen**, *Cyber Defense Agency*
- **Giovanni Vigna**, *University of California Santa Barbara*
- **Simon Wiseman**, *QinetiQ*
- **Diego Zamboni**, *IBM Zürich Research Laboratory*

Conference Committee

- **Cristina Serban**, *AT&T* (Conference Chair)
- **Marshall Abrams**, *The MITRE Corporation* (ACSA Chair)
- **Pierangela Samarati**, *Università degli Studi di Milano* (Program Chair)
- **Charlie Payne**, *Adventium Labs* (Program Co-Chair)
- **Laura Corriss**, *Barry University* (Site Arrangements)
- **Daniel P. Faigin**, *The Aerospace Corporation* (Tutorials Chair)
- **Arthur Friedman**, *NSA* (Registration Chair)
- **Christine Anderson**, *Booz Allen Hamilton, Inc.* (Registration Co-Chair)
- **Carrie Gates**, *CA Labs* (Publicity Chair)
- **Tom Haigh**, *Adventium Labs* (Guest Speaker Liaison)
- **Paul Jardetzky**, *Network Appliances, Inc.* (Panels Chair)
- **Jay Kahn**, *The MITRE Corporation* (Distribution Chair)
- **Steven Rome**, *Booz Allen Hamilton, Inc.* (Case Studies Chair)
- **Harvey H. Rubinovitz**, *The MITRE Corporation* (Workshop Chair)
- **Andre dos Santos**, *University of Puerto Rico at Mayagüez* (Student Awards Chair)
- **Ed Schneider**, *Institute for Defense Analyses* (Treasurer)
- **Dan Thomsen**, *Cyber Defense Agency* (Knowledge Coordinator)
- **John McDermott**, *Naval Research Laboratory* (Works in Progress Chair)
- **Rick Smith**, *University of St. Thomas*, *Minnesota* (Proceedings Chair)
- **Robert H'obbes' Zakon**, *Zakon Group LLC* (Web Advisor)

ACSAC Steering Committee

- **Marshall Abrams**, *The MITRE Corporation*
- **Jeremy Epstein**, *Software AG*
- **Daniel Faigin**, *The Aerospace Corporation*
- **Steve Rome**, *Booz Allen Hamilton*
- **Ron Ross**, *National Institute of Standards*
- **Christoph Schuba**, Sun Microsystems, Inc.
- **Ann Marmor-Squires**, *The Sq Group*
- **Dan Thomsen**, *Cyber Defense Agency, LLC*

Return to Top

About the Sponsor

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.

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

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 page on the website.

For more information on ACSA and its activities, please visit http://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 http://www.acsac.org

ACSA

- **Marshall Abrams**, *The MITRE Corporation* (ACSA Chair & Assistant Treasurer)
- **Jeremy Epstein**, *Software AG* (ACSA Vice President)
- **Daniel Faigin**, *The Aerospace Corporation* (ACSA Secretary)
- **Steven Greenwald**, *Independent Consultant*
- **Steve Rome**, *Booz Allen Hamilton* (ACSA President)
- **Harvey Rubinovitz**, *The MITRE Corporation* (ACSA Treasurer)
- **Ann Marmor-Squires**, *The Sq Group* (Chair Emerita)
- **Mary Ellen Zurko**, *IBM Corporation*

ACSAC-23

Miami Beach Resort & Spa (MBR&S)
December 10-14, 2007

Advance Registration Form

www.acsac.org

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:	**On or Before Nov. 19**		**After Nov. 19, 2007**	
	Regular	Student	Regular	Student
TECHNICAL PROGRAM *Circle applicable fee:*	**$750**	**$450**	**$850**	**$550**
TUTORIALS Full Day	**$550**	**$400**	**$650**	**$400**
(circle no more than one each day)	M1	M2	M3+M4	T5
			T7+T8	T8+T9
Half Day Only	**$325**	**$200**	**$375**	**$200**
	M3		M4	
		T7	T8	T9
TUESDAY WORKSHOP: Software Assurance Workshop	*Circle to register for the workshop and lunch*: $65 *Student Fee* $35			

PAYMENT COMPUTATION

Technical Program Registration: $ ________
$100 Discount [^] if staying at MBR&S reservation # ________ $ ________
Full-day Tutorials: ……………..________ x $ ________ $ ________
Half-day Tutorials: ………….....________ x $ ________ $ ________
Workshop registration: $ ________
Friday Afternoon Excursion: chicken (default) [ ] or pork [ ] x $65 $ ________

TOTAL COST: $ ________

FREE cell phone charger/flashlight with early registration or purchased for $25 at the conference

METHOD OF PAYMENT

[ ] Personal or Company Check enclosed. Make checks payable to ACSAC-23.
[ ] 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

Return to Top

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: Provide Code ________
[ ] Previous ACSAC Conference
[ ] ACSAC Website
[ ] Friend
[ ] Publication: ________
[ ] At Conference: ________
[ ] other: ________

HOTEL REGISTRATION

ACSAC has reserved a block of rooms at the Conference group rate. The hotel room rate is subject to state and local taxes (currently 13%), in effect at the time of check-in. (One night deposit will be required at the time of reservation. The per diem rate will be honored by the hotel for ACSAC guests for 3 days pre/post conference, based on room availability.)

You must make your hotel reservation first in order to receive the $100.00 discount [^] towards the conference. Registering for the Conference doesn't reserve a room, so please call the MBR&S Reservation Department at 1-877-597-9696 or use the following link: http://www.acsac.org/hotel

and identify yourself as an ACSAC attendee. Partial water view rates will be offered until Nov. 19, 2007

REGISTRATION:

Conference registration will not be accepted via telephone.

Register via the ACSAC web site at:
www.acsac.org/registration
or mail this form to:

ACSAC-23
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 19, 2007. Conference registrations may be canceled before that date for a service charge of $25. Cancellations must be in writing and sent to ACSAC-23 using the address or fax number provided above.

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

acs08v06-050916

Exhibit coordinator

FBC
Federal Business Council, Inc.

Registration Management

RSL
Registration Systems Lab

Online Registration

Return to Top