Program

Twenty-Sixth Annual Computer Security Applications Conference (ACSAC)

Practical Solutions To Real World Security Problems

December 6-10, 2010
Four Seasons Hotel
Austin, Texas

Presented by

ACSA
Applied Computer Security Associates

Organizing Committee

Carrie Gates, CA Labs	Conference Chair
Michael Franz, University of California, Irvine	Program Chair
John McDermott, Naval Research Lab	Program Co-Chair
Christoph Schuba, Oracle Corporation	Multimedia/Proceedings
Daniel Faigin, Aerospace Corporation	Tutorials Chair
Steve Rome, Booz Allen Hamilton	Case Studies Chair
Ken Shotting, DoD	Case Studies Co-Chair
Hongxia Jin, IBM	Panels Chair
Art Friedman, NSA	Registration Chair
Benjamin Kuperman, Oberlin College	Poster Chair
James P. Early, State University of New York at Oswego	Poster Co-Chair
Kevin Butler, University of Oregon	Publicity Chair
Mike Collins, Redjack	Sponsorship Chair
Charles Payne, Adventium Labs	Works in Progress Chair
Harvey H. Rubinovitz, The MITRE Corporation	Workshop Chair
Marshall Abrams, MITRE	FISMA Coordination Chair
Jeremy Epstein, SRI International	Local Arrangements Chair
Kristin Steen, Sandia National Labs	Local Arrangements Co-Chair
Lillian Røstad, Norwegian Univ. of Science & Technology	Student Awards
Ben Cook, Sandia National Labs	Student Outreach Chair
Deb Frincke, Pacific Northwest Lab	Guest Speaker Liaison Chair
Kevin Butler, University of Oregon	Guest Speaker Liaison Co-Chair
Ed Schneider, Institute for Defense Analyses	Treasurer
Dan Thomsen, SIFT	Knowledge Coordinator
Jay Kahn, MITRE	ACSA Communications Chair
Cristina Serban, AT&T	Conference Chair Emerita
Robert H'obbes' Zakon, Zakon Group LLC	Web Advisor

Program Committee

Michael Franz, Univ. of California, Irvine (Chair)
John McDermott, Naval Research Lab (Co-Chair)
Vijay Atluri, Rutgers Univ.
Tuomas Aura, Microsoft Research
Lee Badger, NIST
Elisa Bertino, Purdue Univ.
Konstantin Beznosov, Univ. of British Columbia
Matt Bishop, Univ. of California, Davis
Sjdan Capcun, ETH Zurich
Fred Chong, Univ. of California, Santa Barbara
Christian Collberg, Univ. of Arizona
Marc Dacier, Symantec Corporation
Mary Denz, U.S. Air Force Research Laboratory
Sven Dietrich, Stevens Institute of Technology
Jeremy Epstein, SRI International
David Evans, Univ. of Virginia
Richard Ford, Florida Institute of Technology
Tyrone Grandison, IBM Almaden Research Center
Steven Greenwald, Independent Security Advisor
Cynthia Irvine, U.S. Naval Postgraduate School
Trent Jaeger, Pennsylvania State Univ.
Hongxia Jin, IBM Almaden Research Center
Michiharu Kudoh, IBM Tokyo Research Laboratory
Michael Locasto, Univ. of Calgary
Patrick McDaniel, Pennsylvania State Univ.
Peng Ning, North Carolina State Univ.
Charles Payne, Adventium Labs
Andreas Pfitzmann,Technische Universität Dresden
Christian Probst, Technical Univ. of Denmark
Lillian Røstad, Norwegian Univ. of Science & Technology
Reiner Sailer, IBM T.J. Watson Research Center
R. Sekar, Stony Brook Univ.
Pierangela Samarati, Univ. of Milan
Christoph Schuba, Oracle Corporation
Cristina Serban, AT&T
Frederick Sheldon, Oak Ridge National Laboratory
Brian Snow, Independent Security Advisor
Anil Somayaji, Carleton Univ.
Angelos Stavrou, George Mason Univ.
Bhavani Thuraisingham, Univ. of Texas, Dallas
Patrick Traynor, Georgia Institute of Technology
Venkat Venkatakrishnan, Univ. of Illinois at Chicago

This program is subject to change.

Meeting Locations

Monday tutorials will be in the Little Colony, Stone's Crossing, and Waterloo rooms on the Lobby level, with lunch in Ballroom CD on the Lake level. Tuesday tutorials will be in the Little Colony and Waterloo rooms on the Lobby level and Boardroom 516 on the 5th floor, with lunch in Ballroom CD on the Lake level. The Tuesday GTIP workshop will be in Stone's Crossing on the Lobby level with lunch in Ballroom CD on the Lake level.

The Layered Assurance Workshop will be in Ballroom A on the Lake level on Monday and Tuesday, with lunch in Ballroom CD, also on the Lake level.

The Tuesday evening reception will be held on the Lawn (outdoors Lake level) if weather permits, otherwise in the Ballroom Foyer (Lake level).

All Wednesday through Friday activities are on the Lake level, with the exception of the FISMA training session which is on the Lobby level. Plenaries will be in Ballroom AB with breakouts in Ballroom AB, San Jacinto East, and San Jacinto West. FISMA training will be in Waterloo. Breakfasts will be in the Ballroom Foyer and lunches in Ballroom CD. Exhibits will be in the Ballroom Foyer.

The Wednesday dinner will be held on the Lawn (outdoors Lake level) if weather permits, otherwise in Ballroom CD (Lake level). The Thursday works in progress, posters, career fair, exhibits, and reception will be in the Ballroom Foyer (Lake level).

Registration and Information Desk Hours

Desk hours during the Conference are: Sunday, 17:00-19:00; Monday, 7:30-12:00 and 17:00-19:00; Tuesday, 7:30-12:00 and 16:00-19:00; Wednesday, 7:30-12:00 and 13:00-16:30; Thursday, 7:30-12:00 and 13:00-16:30; and Friday, 7:30-10:00. The Registration and Information Desk also serves as the conference "Lost and Found Center" and is the location of the conference message board.

Meals

The conference provides a continental breakfast, a mid-morning coffee break and a mid-afternoon snack and lunch for ACSAC conference (tutorial/workshop) attendees on the days of the conference (tutorial/workshop). Lunch will be provided on Friday only for those attendees registered for the outing to Stubbs Barbecue. A reception with light snacks and cash bar will be offered on Tuesday evening, dinner and entertainment on Wednesday evening (don't forget your drink tickets!), and a light reception with soft drinks at the WIP/Posters/Career Fair session on Thursday.

Internet Access

WiFi service for personal rooms is available for $5.50/day. Please see the instructions from the hotel on how to connect. WiFi service in meeting rooms is provided by our A/V company at no charge to you. The SSID is "CSA Conf" and password is "2011ACSAC". If you're paying for WiFi service in your room, you can also use that in the meeting rooms at no additional charge. ACSAC cannot guarantee the reliability or security of either of these WiFi options.

Session Etiquette

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

PROGRAM SCHEDULE

Monday, 6 December 2010

8:30-12:00 **Technology Tutorials & Workshops**

Workshop Ballroom A **Layered Assurance Workshop (LAW)** Chair: Rance J. DeLong, Lynuxworks, Santa Clara Univ. For details, please see page 17.	**Tutorial** Little Colony *M1. Educating Computer Security Professionals with the CyberCIEGE Video Game* Instructor(s): Mr. Michael Thompson, Naval Postgraduate School For details, please see page 18.	**Tutorial** Stone's Crossing *M3. Algorithms for Software Protection* Instructor(s): Dr. Christian Collberg, Univ. of Arizona; Dr. Jasvir Nagra, Google, Inc. For details, please see page 20	**Tutorial** Waterloo *M4. System Life Cycle Security Engineering* Instructor(s): Ms. Thuy D. Nguyen and Dr. Cynthia E. Irvine, Naval Postgraduate School For details, please see page 21

12:00-13:30 **Lunch** Ballroom CD

13:30-17:00 **Technology Tutorials & Workshops**

Workshop Ballroom A **LAW (continued)**	**Tutorial** Little Colony *M2. State of the Practice: Intrusion Detection* Instructor(s): Dr. Michael Collins and Dr. John McHugh, Redjack, LLC For details, please see page 19	**Tutorial** Stone's Crossing *M3 (continued)*	**Tutorial** Waterloo *M4 (continued)*

Tuesday, 7 December 2010

7:30-8:30 **Breakfast** Ballroom CD

8:30-12:00 **Technology Tutorials & Workshops**

Workshop Ballroom A **LAW (continued)**	**Workshop** Stone's Crossing **Workshop on Governance of Technology, Information, and Policies (GTIP)** Chair: Dr. Harvey Rubinovitz, MITRE Corporation For details, please see page 17.	**Tutorial** Little Colony *T5. Visualization and Security* Instructor(s): Mr. Zed Abbadi, Public Company Accounting Oversight Board (PCAOB) For details, please see page 22	**Tutorial** Boardroom 516 *T7. State of the Practice: Secure Coding* Instructor(s): Mr. Robert C. Seacord, CERT Software Engineering Institute For details, please see page 23.	**Tutorial** Waterloo *T8. An Introduction to Usable Security* Instructor(s): Dr. Jeff Yan, Newcastle Univ.; Mary Ellen Zurko, IBM For details, please see page 24.

12:00-13:30 **Lunch** Ballroom CD

13:30-17:00 **Technology Tutorials & Workshops**

Workshop Ballroom A **LAW (continued)**	**Workshop** Stone's Crossing **GTIP (continued)**	**Tutorial** Little Colony *T6. Keeping Your Web Apps Secure: The OWASP Top 10 & Beyond* Instructor(s): Mr. Robert H'obbes' Zakon, Zakon Group LLC For details, please see page 22.	**Tutorial** Boardroom 516 *T7 (continued)*	**Tutorial** Waterloo *T8 (continued)*

18:00-20:00 **Welcome Reception** Lawn

In the event of bad weather, this event will be held in Ballroom CD.

Please visit our exhibitors tonight through Thursday evening!

Wednesday, 8 December 2010

7:30-8:30 **Continental Breakfast** Ballroom CD

8:30-8:45 **Welcome** Ballroom AB

Dr. Carrie Gates, Conference Chair
Dr. Michael Franz, Program Chair

8:45-10:00 **Distinguished Practitioner** Ballroom AB

Putting Basic Research To Work
Douglas Maughan, DHS Science & Technology Directorate

While many agencies struggle with how to move basic research across the 'valley of death', there are many success stories. For instance, IronKey was initially funded by DHS S&T as a two employee organization in 2005. IronKey is now a growing company — well over 100 employees, and probably the best USB (storage) in the marketplace and it's now the standard-issue at DHS. This talk provides a view from the trenches of what works — and what doesn't — when transitioning basic research into practice.

About the Speaker: Dr. Douglas Maughan is the Director of the Cyber Security Division in the Homeland Security Advanced Research Projects Agency (HSARPA) within the Science and Technology (S&T) Directorate of the Department of Homeland Security (DHS). Dr. Maughan has been at DHS since October 2003 and is directing and managing the Cyber Security Research and Development activities and staff at DHS S&T. His research interests and related programs are in the areas of networking and information assurance.

Prior to his appointment at DHS, Dr. Maughan was a Program Manager at the Defense Advanced Research Projects Agency (DARPA) in Arlington, Virginia. Prior to his appointment at DARPA, Dr. Maughan worked for the National Security Agency (NSA) as a senior computer scientist and led several research teams performing network security research. Dr. Maughan received Bachelor's Degrees in Computer Science and Applied Statistics from Utah State University, a Masters degree in Computer Science from Johns Hopkins University, and a PhD in Computer Science from the University of Maryland, Baltimore County (UMBC).

10:00-10:30 **Break** Ballroom Foyer

10:30-12:00 **Technical Tracks**

A. Papers Ballroom AB
Social Networks
Chair: Arthur R. Friedman

Detecting Spammers On Social Networks
Gianluca Stringhini, Christopher Kruegel, Giovanni Vigna, Univ. of California, Santa Barbara

Towards Worm Detection in Online Social Networks
Wei Xu, Fangfang Zhang, Sencun Zhu, Pennsylvania State Univ.

Who Is Tweeting On Twitter: Human, Bot, Or Cyborg?
Zi Chu, Steven Gianvecchio, Haining Wang, The College of William and Mary; Sushil Jajodia, George Mason Univ.

B. Case Studies San Jacinto West

Managing Security Information and PCI compliance at The Univ. of Dayton
Rick Wagner, Novell, Inc.

A Taxonomy of Vulnerability in the Supply Chain
Chris Romeo and Patrick Hunter, CISCO

The Security Threats To and From the Intelligent Electronics Devices
Baris Coskun, AT&T

C. Panel San Jacinto East
Risks in the Clouds - Between Silver Linings and Oncoming Storms
Dr. Peter Neumann, SRI (Chair); Earl Crane, Department of Homeland Security; Ahmad-Reza Sadeghi, Technical Univ. Darmstadt and Fraunhofer Institute for Secure Information Systems, Darmstadt; Matt Blaze, Professor of Computer Science, Univ. of Pennsylvania, USA; Lee Tien, Electronic Frontier Foundation, USA

D. Training Waterloo
TR1. Cyber Security Controls: NIST SP 800-53 Rev 3 & CNSSI 1253
Instructor: Dr. Marshall D. Abrams, The MITRE Corporation

See details on page 26.

12:00-13:30 **Lunch** Ballroom CD

13:30-15:00 **Technical Tracks**

A. Papers Ballroom AB
Software Defenses
Chair: Lillian Røstad

Cujo: Efficient Detection And Prevention Of Drive-by-download Attacks
Konrad Rieck, Berlin Institute of Technology; Tammo Krueger, Fraunhofer Institute FIRST; Andreas Dewald, Univ. of Mannheim

Fast And Practical Instruction-set Randomization For Commodity Systems
Georgios Portokalidis, Angelos D. Keromytis, Columbia Univ.

G-free: Defeating Return-oriented Programming Through Gadget-less Binaries
Kaan Onarlioglu, Bilkent Univ.; Leyla Bilge, Andrea Lanzi, Davide Balzarotti, Engin Kirda, Eurecom

B. Case Studies San Jacinto West

Global Automaker's North American Operations Deploys Managed Hardware Encryption for Protecting Sensitive Data on Employee Laptops
Steven Sprague, Wave Systems

ISO Cyber Security and ICT SCRM Standards
Nadya Bartol, Booz Allen Hamilton

EMC's Product Security Evolution
Dan Reddy, EMC

C. Panel San Jacinto East
Security Economics
Daniel Arista, SRC, Inc. (chair); Douglas Maughan, DHS; Tim Clancy, CIPHS; Marcus Sachs, Verizon; Sasha Romanosky, CMU

D. Training Waterloo
TR1. Cyber Security Controls: NIST SP 800-53 Rev 3 & CNSSI 1253
Instructor: Dr. Marshall D. Abrams, The MITRE Corporation

See details on page 26

15:00-15:30 **Break** Ballroom Foyer

15:30-17:00 **Technical Tracks**

A. Papers San Jacinto West
Authentication
Chair: Kevin Butler

Towards Practical Anonymous Password Authentication
Yanjiang Yang, Jianying Zhou, Jun Wen Wong, Feng Bao, Institute for Infocomm Research

Securing Interactive Sessions Using Mobile Device Through Visual Channel And Visual Inspection
Chengfang Fang, Ee-Chien Chang, National Univ. of Singapore

Usability Effects Of Increasing Security In Click-based Graphical Passwords
Elizabeth Stobert, Alain Forget, Sonia Chiasson, Paul van Oorschot, Robert Biddle, Carleton Univ.

B. Papers San Jacinto East
Vulnerability Assessment of Embedded Devices
Chair: Jeremy Epstein

Security Analysis Of A Fingerprint-protected USB Drive
Benjamin Rodes, Xunhua Wang, James Madison Univ.

A Quantitative Analysis Of The Insecurity Of Embedded Network Devices: Results Of A Wide-area Scan
Ang Cui, Salvatore J. Stolfo, Columbia Univ.

Multi-vendor Penetration Testing In The Advanced Metering Infrastructure
Stephen McLaughlin, Dmitry Podkuiko, Adam Delozier, Sergei Miadzvezhanka, Patrick McDaniel, Pennsylvania State Univ.

C. Training Waterloo
TR2. Near Real-Time Risk Management Process: NIST SP 800-37
Instructor: Dr. Marshall D. Abrams, The MITRE Corporation

See details on page 26

17:00-17:45 **Classic Paper I** Ballroom AB

Network Intrusion Detection: Dead or Alive?
Giovanni Vigna, Univ. of California, Santa Barbara, USA

Research on network intrusion detection has produced a number of interesting results. In this paper, I look back to the NetSTAT system, which was presented at ACSAC in 1998. In addition to describing the original system, I discuss some historical context, with reference to well-known evaluation efforts and to the evolution of network intrusion detection into a broader field that includes malware detection and the analysis of malicious behavior.

About the Speaker: Giovanni Vigna is a Professor in the Department of Computer Science at the Univ. of California in Santa Barbara. His current research interests include malware analysis, web security, vulnerability assessment, and intrusion detection. He also edited a book on Security and Mobile Agents and authored one on Intrusion Correlation. He has been the Program Chair of the International Symposium on Recent Advances in Intrusion Detection (RAID 2003), of the ISOC Symposium on Network and Distributed Systems Security (NDSS 2009), and of the IEEE Symposium on Security and Privacy (S&P 2010 and 2011). He is known for organizing and running an inter-university Capture The Flag hacking contest, called iCTF, that every year involves dozens of institutions around the world. Giovanni Vigna received his M.S. with honors and Ph.D. from Politecnico di Milano, Italy, in 1994 and 1998, respectively. He is a member of IEEE and ACM.

17:45-18:00 **A Tribute to Paul Karger** Ballroom AB

19:00-22:00 **Conference Dinner** Lawn

Featuring music by blues guitarist Alan Haynes. In the event of bad weather, this event will be held in Ballroom CD.

Thursday, 9 December 2009

7:30-8:30	**Continental Breakfast**	Ballroom CD
8:30-8:45	**Opening Remarks & Announcements**	Ballroom AB
8:45-10:00	**Invited Essayist**	Ballroom AB

Barriers to Science in Security
Thomas Longstaff, Johns Hopkins Univ., Applied Physics Laboratory, USA

In the past year, there has been significant interest in promoting the idea of applying scientific principles to information security. The main point made by information security professionals who brief at conferences seems to be that our field of information security is finally mature enough to begin making significant strides towards applying the scientific approach. Audiences everywhere enthusiastically agree and thrash themselves for bypassing science all along, bemoaning the fact that we could be "so much further along" if we only did science. Of course, after the presentation is over, everyone goes back to the methods that have been used throughout our generation to generate prototypes and tools with no regard for the scientific principles involved. We explore the barriers to adopting a scientific approach to experimental information security projects, including:

- time to publish as a primary driver
- standard of peer reviews in conferences and journals
- expectation of a breakthrough in every publication

Based on these factors, we examine a way forward — how the scientific method can allow us to understand the underlying causality of information security and addressing the problem at its most fundamental level, and the changes in attitudes and processes necessary for this to happen.

About the Speaker: Dr. Tom Longstaff is the Chief Scientist for the Cyber Missions Branch of the Applied Physics Laboratory. APL is a Univ. Affiliated Research Center, a division of the Johns Hopkins Univ.. Tom joined APL in 2007 to work with a wide variety of infocentric operations projects on behalf of the US Government to include technology transition of cyber R&D, information assurance, intelligence, and global information networks.

Tom's academic publications span topics such as malware analysis, information survivability, insider threat, intruder modeling, and intrusion detection. Tom is Chair of the Computer Science, Information Assurance, and Information Systems Engineering Programs at The Johns Hopkins Univ. Whiting School of Engineering. Tom is also a fellow of the International Information Integrity Institute and editor of the IEEE Security & Privacy journal.

10:00-10:30	**Break**	Ballroom Foyer

10:30-12:00 **Technical Tracks**

A. Papers Ballroom AB

Botnets

Chair: Angelos Stavrou

Friends Of An Enemy: Identifying Local Members Of Peer-to-peer Botnets Using Mutual Contacts
Baris Coskun, Polytechnic Institute of NYU; Sven Dietrich, Stevens Institute of Technology; Nasir Memon, Polytechnic Institute of NYU

The Case For In-the-lab Botnet Experimentation: Creating And Taking Down A 3000-node Botnet
Joan Calvet, Carlton Davis, Jose M. Fernandez, Ecole Polytechnique de Montreal; Jean-Yves Marion, LORIA - Nancy Univ.; Pier-Luc St-Onge, Ecole Polytechnique de Montreal

Conficker And Beyond: A Large-scale Empirical Study
Seungwon Shin, Guofei Gu, Texas A&M Univ.

B. Panel San Jacinto East

Federal Cyber Security Research Agenda
Tomas Vagoun, NITRD (chair); Patricia Muoio, ODNI; Douglas Maughan, DHS S&T; Samuel Weber, NSF

C. Training Waterloo

TR2. Near Real-Time Risk Management Process: NIST SP 800-37
Instructor: Dr. Marshall D. Abrams, The MITRE Corporation

See details on page 26.

12:00-13:30 **Lunch** Ballroom CD

13:30-15:00 **Technical Tracks**

A. Papers Ballroom AB

Email, E-Commerce, and Web 2.0
Chair: Christoph Schuba

Spam Mitigation Using Spatio-temporal Reputations From Blacklist History
Andrew West, Adam Aviv, Jian Chang, Insup Lee, Univ. of Pennsylvania

Breaking E-banking Captchas
Shujun Li, Univ. of Konstanz; Syed Amier Haider Shah, Muhammad Asad Usman Khan, Syed Ali Khayam, National Univ. of Science and Technology (NUST); Ahmad-Reza Sadeghi, Ruhr-Univ. of Bochum

Firm: Capability-based Inline Mediation Of Flash Behaviors
Zhou Li, XiaoFeng Wang, Indiana Univ. at Bloomington

B. Papers San Jacinto West

Hardware-Assisted Security
Chair: Michael E. Locasto

T-dre: A Hardware Trusted Computing Base For Direct Recording Electronic Vote Machines
Roberto Gallo, Univ. of Campinas; Henrique Kawakami, KRYPTUS Cryptographic Engineering; Ricardo Dahab, Guido Arajo, Univ. of Campinas; Rafael Azavedo, Tribunal Superior Eleitoral

Hardware Assistance For Trustworthy Systems Through 3-d Integration
Jonathan Valamehr, Mohit Tiwari, Timothy Sherwood, UC Santa Barbara; Arash Arfaee, Ryan Kastner, UC San Diego

Sca-resistant Embedded Processors—the Next Generation
Stefan Tillich, Univ. of Bristol; Mario Kirschbaum, Alexander Szekely, Graz Univ. of Technology

C. Case Studies San Jacinto East

Supply Chain Risk Management
Nadya Bartol, Booz Allen Hamilton (chair); Don Davidson, DoD/Global Task Force; Marianne Swanson, NIST; Carol Woody, SEI CERT; Larry Wagoner, NSA; Dan Reddy, EMC/ SAFECode

D. Training Waterloo

TR3. Integrated Enterprise-Wide Risk Management Organization, Mission, and Information System View: NIST SP 800-39
Instructor: Dr. Marshall D. Abrams, The MITRE Corporation

See details on page 26.

15:00-15:30 **Break** Ballroom Foyer

15:30-17:00 **Technical Tracks**

A. Papers Ballroom AB
Security Protocols and Portable Storage
Chair: Baris Coskun

Porscha: Policy Oriented Secure Content Handling In Android
Machigar Ongtang, Kevin Butler, Patrick McDaniel, Pennsylvania State Univ.

Kells: A Protection Framework For Portable Data
Kevin Butler, Stephen McLaughlin, Patrick McDaniel, Pennsylvania State Univ.

Keeping Data Secret Under Full Compromise Using Porter Devices
Christina Ppper, David Basin, Srdjan Capkun, Cas Cremers, ETH Zurich

B. Papers San Jacinto West
Model Checking and Vulnerability Analysis
Chair: Sven Dietrich

Familiarity Breeds Contempt: The Honeymoon Effect And The Role Of Legacy Code In Zero-day Vulnerabilities
Sandy Clark, Univ. of Pennsylvania; Stefan Frei, Secunia; Matt Blaze, Jonathan Smith, Univ. of Pennsylvania

Quantifying Information Leaks In Software
Jonathan Heusser, Pasquale Malacaria, Queen Mary Univ. of London

Analyzing And Improving Linux Kernel Memory Protection: A Model Checking Approach
Siarhei Liakh, Michael Grace, Xuxian Jiang, North Carolina State Univ.

C. Panel San Jacinto East
The New Security Paradigms Experience
Richard Ford, Florida Institute of Technology (Moderator); Michael Locasto, Univ. of Calgary; Victor Raskin, Purdue; Julia M. Taylor, Purdue

D. Training Waterloo
TR3 Integrated Enterprise-Wide Risk Management Organization, Mission, and Information System View: NIST SP 800-39
Instructor: Dr. Marshall D. Abrams, The MITRE Corporation

17:00-17:45 **Classic Paper II** Ballroom AB

Back to Berferd
William Cheswick, AT&T LabsResearch, USA

It has been nearly twenty years since I published the Berferd paper. Much of it is quite outdated, reflecting the state of technology at the time. But it did touch a number of issues that have become quite important. I discuss some of the existing conditions around the time of the paper, and some of these issues.

About the Speaker: Ches is an early innovator in Internet security. He is known for his work in firewalls, proxies, and Internet mapping at Bell Labs and Lumeta Corp. He is best known for the book he co-authored with Steve Bellovin and now Avi Rubin, Firewalls and Internet Security; Repelling the Wily Hacker.

Ches is now a member of the technical staff at AT&T Labs - Research in Florham Park, NJ, where he is working on security, visualization, user interfaces, and a variety of other things.

18:00-21:00 **Posters/Works in Progress/Career Night/Reception** Ballroom AB

Works in Progress 18:00-19:30
Chair: Charles Payne

- *Ontologies for Modeling Enterprise Level Security Metrics*, Anoop Singhal, NIST
- *Hardware Hypervisor for a Secure Root of Trust*, Joseph Loomis, Southwest Research Institute
- *Federal Cloud Security Top 20*, Earl Crane, DHS
- *The Systems Security Engineering Process*, Toni Claud, NSA

Posters 18:00-19:30
Chair: Benjamin Kuperman, James P. Early

- *Graph-Based Tra.c Analysis for Network Intrusion Detection*, Gary Sandine, Los Alamos National Laboratory
- *Security through Usability: a user-centered approach for balanced security policy requirements*, Shamal Faily, Univ. of Oxford
- *Side Channel Finder (Version 1.0)*, Artem Starostin, TU Darmstadt
- *Service Automata for Secure Distributed Systems*, Richard Gay, TU Darmstadt
- *Accelerating Regular Expression Processing Using Hardware DFA Engines*, Jordi Ros-Giralt, Reservoir Labs
- *SIFEX: Tool for Static Analysis of Browser Extensions for Security Vulnerabilities*, Shikhar Agarwal, Indian Institute of Technology
- *RAVEN: Real-time Attack Visualization through Examining Network flows*, Ethan Singleton, Univ. of Tulsa
- *DDoS Attacks Avoidance by Securely Hiding Web Servers*, Mohamad Samir A. Eid, Univ. of Tokyo
- *Reliable Time Based Forensics in NTFS*, Xiaoqin Ding, Shanghai Jiao Tong Univ.
- *Inherent Problems in the Information Technology Supply Chain*, Courtney Cavness, Atsec Corporation

Career Fair 18:00-20:00
Chair: Ben Cook
New to 2010: ACSAC adds a career fair! Companies hiring in the area of information security and research will be on hand to discuss employment opportunities.

Friday, 10 December 2010

7:30-8:30 **Continental Breakfast** Ballroom Foyer

8:30-10:00 **Technical Tracks**

A. Papers Ballroom A
Intrusion Detection and Live Forensics
Chair: Kenneth F. Shotting

Comprehensive Shellcode Detection Using Runtime Heuristics
Michalis Polychronakis, Columbia Univ.; Kostas Anagnostakis, Niometrics R&D; Evangelos Markatos, FORTH-ICS

Cross-layer Comprehensive Intrusion Harm Analysis For Production Workload Server Systems
Shengzhi Zhang, Pennsylvania State Univ.; Xiaoqi Jia, Graduate Univ. of Chinese academy of sciences; Peng Liu, Pennsylvania State Univ.; Jiwu Jing, Graduate Univ. of Chinese academy of sciences

Forenscope: A Framework For Live Forensics
Ellick Chan, Shivaram Venkataraman, Univ. of Illinois; Francis David, Microsoft; Amey Chaugule, Univ. of Illinois

B. Papers San Jacinto West
Distributed Systems and Operating Systems
Chair: TBD

A Multi-user Steganographic File System On Untrusted Shared Storage
Jin Han, Meng Pan, Debin Gao, HweeHwa Pang, Singapore Management Univ.

Heap Taichi: Exploiting Memory Allocation Granularity In Heap-spraying Attacks
Yu Ding, Tao Wei, Tielei Wang, Peking Univ.; ZhenKai Liang, National Univ. of Singapore; Wei Zou, Peking Univ.

Scoba: Source Code Based Attestation On Custom Software
Liang Gu, Yao Guo, Anbang Ruan, Qingni Shen, Hong Mei, Peking Univ.

C. Case Studies San Jacinto East
Software Security Automation and Measurement
Joe Jarzombek, National Cyber Security Division, DHS (Moderator); Don Davidson, OASD-NII/DoD; Nadya Bartol, Booz Allen Hamilton; Robert Seacord, CERT Coordination Center, Carnegie Mellon Univ.; Carol Woody, SEI, Carnegie Mellon Univ.

D. Training Waterloo
TR4. Risk Assessments for Information Technology Systems: NIST SP 800-30
Instructor: Pete Gouldmann, U.S. Department of State

See details on page 27.

10:00-10:30 **Break** Ballroom Foyer

10:30-12:00 **Technical Tracks**

A. Papers Ballroom A

Mobile and Wireless
Chair: Christina Serban

Paranoid Android: Versatile Protection For Smartphones
Georgios Portokalidis, Columbia Univ.; Philip Homburg, Herbert Bos, Vrije Universiteit Amsterdam

Exploiting Smart-phone USB Connectivity For Fun And Profit
Zhaohui Wang, Angelos Stavrou, George Mason Univ.

Defending Dsss-based Broadcast Communication Against Insider Jammers Via Delayed Seed-disclosure
An Liu, Peng Ning, Huaiyu Dai, Yao Liu, North Carolina State Univ.; Cliff Wang, Army Research Office

B. Papers San Jacinto West

Security Engineering and Management
Chair: Edward A. Schneider

Always Up-to-date – Scalable Offline Patching Of Vm Images In A Compute Cloud
Wu Zhou, Peng Ning, North Carolina State Univ.; Xiaolan Zhang, Glenn Ammons, IBM; Ruowen Wang, North Carolina State Univ.; Vasanth Bala, IBM

A Framework For Testing Hardware-software Security Architectures
Jeffrey S. Dwoskin, Princeton Univ.; Mahadevan Gomathisankaran, Univ. of North Texas; Yu-Yuan Chen, Ruby B. Lee, Princeton Univ.

Two Methodologies For Physical Penetration Testing Using Social Engineering
Trajce Dimkov, Andre van Cleeff, Wolter Pieters, Pieter Hartel, Univ. of Twente

C. Training Waterloo

TR4. Risk Assessments for Information Technology Systems: NIST SP 800-30
Instructor: Pete Gouldmann, U.S. Department of State

See details on page 27.

12:00-12:30 **Closing Session/Best Paper Award** Ballroom A

13:00-15:00 **Optional Lunch at Stubb's BBQ**

Workshop Details

Layered Assurance Workshop (LAW)

Chair: Rance J. DeLong, Lynuxworks, Santa Clara Univ.

Monday December 6th and Tuesday December 7th, All Day. Separate registration and fee required.

LAW has provided a forum for vital exchange, as well as a maturing source of information, focused on key issues relating to the effective and efficient modular construction and certification of assured systems from assured components. It is widely recognized that such an approach is the most promising way to achieve diverse and flexible systems that can be certified quickly and cost effectively. LAW is concerned with the theoretical, engineering, and certification challenges to be met before this goal can be fully realized.

The Workshop concerns itself with the fundamental problems of "compositional assurance" and with a need for principles, methods, and techniques that can be applied to achieve the assurance necessary for security-critical, safety-critical, and mission-critical components and systems.

For the past three years, the Layered Assurance Workshop has grown and evolved. The first LAW in 2007 took an exploratory approach, relying heavily on the participants' input to establish the agenda. The second LAW in 2008 was attended by approximately 80 individuals representing more than 30 distinct organizations. In that Workshop more of the program was established in advance, with several keynote talks chosen from responses to an open invitation, followed by breakout sessions on diverse topics. The third LAW comprised two thematic days with a common structure: morning keynote talks, afternoon panels and breakout sessions. The theme of the first day was programmatic needs of government, while that of the second day was research and development on the problems of layered assurance.

This year, the fourth LAW will include talks by distinguished speakers, panels, discussions and technical training. Attendees are encouraged to participate in ACSAC in addition to LAW. The conjunction of LAW and ACSAC provides increased opportunities for academic and industry participants to contribute in the forum of their choice. Please pass along information about LAW to colleagues who may be interested.

The workshop is unclassified and will be open to all attendees. As a result of the transition to make LAW a permanent ACSAC workshop, there is now a LAW registration fee. This year, to ease the transition for attendees, the LAW sponsors have generously provided a sponsorship for early registrants.

For agenda and registration details, please visit `http://fm.csl.sri.com/LAW/2010/index.shtml`.

Workshop on Governance of Technology, Information, and Policies (GTIP): Addressing the Challenges of Worldwide Interconnectivity

Chair: Dr. Harvey H. Rubinovitz

Tuesday, 7 December 2008, 8:30 – 17:00. Separate registration and fee required.

The explosion in the use of the Internet over the last 10 years has connected institutions governments, researchers, and non-technical people throughout the world. The large number of devices connected to the networks has changed the Internet from a set of networks connecting computers to a set of networks connecting all types of objects. This trend, combined with the rise of collaborative technologies, virtual worlds, and cloud computing raises issues profoundly affecting how the management of systems, of computation, and of data is viewed.

A key issue that springs from the implications of managing the interconnection of people and devices throughout the world is how differing laws, customs, and world views have led to the application of technologies to meet goals that conflict, yet must interoperate. For example, the rules governing privacy vary throughout the world. However, with the advent of cloud computing it may no longer be possible to restrict data to jurisdictions with compatible rules because the cloud provider may migrate data or computation to leverage resources in other jurisdictions. How do we handle this situation technologically? How do we devise policies and processes to control the effects of this increasing interconnection, the technology, and the data? What implications does this have for laws, regulations, customs, and management?

The goal of this workshop is to explore these issues in a variety of contexts. We invited original position and research papers describing the challenges that must be resolved, policies, processes and technologies that may prove useful in dealing with these problems, security, technological, societal, and legal issues, as well as aspects of computing and managing data in a world of fragmented and incompatible rules.

For agenda and other details, please visit `http://www.acsac.org/2010/workshop/`.

Tutorial Details

Tutorial *M1. Educating Computer Security Professionals with the CyberCIEGE Video Game*

Instructor(s): Mr. Michael Thompson, Naval Postgraduate School

Monday, December 6th, Morning Only. Separate registration and fee required.

CyberCIEGE is a 3D video game that enhances computer network security education and training through constructive resource management techniques such as those employed in the Tycoon games. In the CyberCIEGE world, players spend virtual money to operate and defend networks, and can watch the consequences of their choices, while under attack. CyberCIEGE scenarios cover network management and defense including the use of network filters, VPNs, e-mail encryption, access control mechanisms, biometrics, and PKI. Players balance budget, productivity, and security by keeping the virtual world's personnel happy (e.g., by providing Internet access) while protecting assets from vandals and professional attacks. The tutorial will cover the use of the game for education and training, and will include hands on scenario play for the audience. In addition, the tutorial will cover use of the Scenario Development Kit for creating and customizing scenarios.

While CyberCIEGE includes a set of "training and awareness" scenarios for general audiences (such as those of other computer security games like "Anti-phishing Phil"), the primary purpose of the game is broader computer security education. CyberCIEGE is built around the fundamental concepts of information security policies. Attacks are fueled by attacker motives. And motives vary by asset and scenario. The fidelity of CyberCIEGE attacks is high enough to illustrate functions of technical protection mechanisms and configuration-related vulnerabilities. For example, an attack might occur because a particular firewall port is left open and a specific component lacks a suitable patch management policy. This attack engine is coupled with an economy engine that measures the virtual user's ability to achieve goals (i.e., read or write assets). This combination enables scenarios that illustrate real-world trade-offs such as the use of air-gaps vs. the risks of cross domain solutions when accessing assets on both sensitive and unclassified networks.

CyberCIEGE was created by the Naval Postgraduate School in partnership with Rivermind Inc., and it is deployed around the world in universities, community colleges and government organizations. The US Government has unlimited use of the game, and a no-cost license to use CyberCIEGE is available to educational institutions, and hundreds of such institutions have requested the game. The target audience of the tutorial is computer security instructors and those developing security training and education programs.

Outline

1. **Overview, purpose and intended audience of the game.** Introductory video. Training scenarios vs Educational scenarios. Online encyclopedia and tutorial movies. Example training scenario.

2. **Scenarios illustrating basic network security concepts.** Introductory tutorial scenario. Examples of game engine triggers, conditions and attacks. Basic game mechanics. Information security policy and physical security. Hands on play by attendees of introduction scenario.

3. **Intermediate computer security concepts.** Network filters and their limitations (Network filters Scenario). Access control policies and assurance (Genes R Us scenario). User identification. Encryption, VPNs, Email protection. Hands on play by attendees of filters scenario.

4. **Deploying the game for training and education.** Mechanics of distribution and deployment. Use of the game to augment case studies, directed group play. Student assessment tool.

5. **Creating and customizing scenarios.** Game engine: Attack models, Game economy, Triggers and conditions. Use of the Scenario Development Tool (SDT).

6. **Hands on supervised scenario play by the attendees.**

7. **Example of scenario construction.** SDT mechanics. Scenario testing.

Prerequisites. Attendees will each need access to a computer (e.g. laptop) having a Windows operating system. Those with Mac computers can run the game using VMWare Fusion and a Windows guest operating system. Most relatively modern laptops and notebooks will run the game. Test the game on your laptop using the free evaluation version available at `http://cisr.nps.edu/cyberciege/downloads/setup-demo.exe`.

About the Instructor. Mr. Michael Thompson is a Research Associate in the Center for Information Systems

Security Studies and Research at the Naval Postgraduate School in Monterey, California. He is the lead engineer for CyberCIEGE and is responsible for its ongoing development and maintenance. He holds a B.S. in Electrical Engineering from Marquette Univ.. His research interests include security engineering and high assurance computer security, and he has over twenty years experience in the field of computer security.

Tutorial *M2. State of the Practice: Intrusion Detection*

Instructor(s): Dr. Michael Collins and Dr. John McHugh, RedJack, LLC

Monday, December 6th, Afternoon Only. Separate registration and fee required.

This half day tutorial is intended to provide an overview of the state of practice in intrusion detection. It is intended to provide an understanding of the problems and potential pitfalls for researchers intending to undertake research efforts in the field, especially those who approach it from the viewpoint of other disciplines such as machine learning. The intended audience includes graduate students seeking PhD or MS topics, network security analysts who want deeper insights into the reasons why intrusion detection systems manifest relatively poor performance, and individuals desiring to evaluate intrusion detection products.

At the completion of the tutorial, the student should be conversant with the vocabulary of intrusion detection and have developed an appreciation for the difficulty of the problem area. The tutorial will cover the major classes of intrusion detection including host and network based classifications and signature and anomaly based classifications. Each of these approaches presents its own advantages and problems and each presents specific kinds of problems that need to be addressed by the research and operational communities. While there is a large body of published research in the area, relatively few of the academically developed approaches make any practical impact on the field and a unifying theme of the tutorial will be discussion of why this is the case. Specific topics of interest include the role of intrusion detection in system defense, sensing approaches, detection issues, and intrusion detection system evaluation.

Outline

1. **Introduction.** Intrusion detection systems history. Basic IDS technology: HIDS, NIDS, Signature-Based, Anomaly-Based. Major IDS families. Related technologies. Fallacies in IDS - false positives, false negatives, base-rate.
2. **General problems in IDS.** Data collection. Inferential fallacies - false positives, false negatives, base-rate, prosecutor's fallacy. IDS evasion. Problems with IDS on the floor: polymorphism, packers and signature evasion, zero-days, and chair-swiveling.
3. **Signature Based IDS: State of the practice.** Standard Signature Based IDS: Snort, Commercial systems. Signature management. Mechanisms for comparing and evaluating signatures. Current problems in signature based IDS: malware, signature management, deceptive signatures.
4. **Anomaly Based IDS: State of the Practice.** Historical anomaly detection timeshares. Modern anomaly detection systems. Successful anomaly detection. Current problems in anomaly based IDS: noise, training assumptions.
5. **IDS Evaluation.** Data available for evaluation. ROC curves and other evaluation mechanisms. Problems in 'normalcy'.
6. **Similar Systems.** IPS vs. IDS vs. Sensor. SIM/SEM. AV. DDoS Detection.

Prerequisites. None.

About the Instructors. Dr. Michael Collins is Chief Scientist for RedJack and a former scientist for the CERT / Network Situational Awareness Team at Carnegie Mellon Univ.. In this capacity, Dr. Collins was one of the lead designers of CENTAUR and the SiLK toolkit. Dr. Collins is an expert on traffic analysis, and has developed novel methods for tracking peer-to-peer applications and applying social network analysis to network traffic. His work is used by several federal agencies for traffic analysis and network defense. He is currently working on social network analysis of web usage.

Dr. John McHugh is the Senior Principal at RedJack LLC, a network data analysis and security consulting company and holds a visiting faculty position at UNC. Before joining RedJack, he was a Canada Research Chair in Privacy and Security at Dalhousie Univ. in Halifax, NS, and, earlier, 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 using visual analytic techniques and has developed tools for characterizing host and network behavior. Dr. McHugh received his PhD degree in computer science from the Univ. of Texas at Austin. He has a MS degree in computer science from the Univ. of Maryland, and a BS degree in physics from Duke Univ..

Tutorial *M3. Algorithms for Software Protection*

Instructor(s): Dr. Christian Collberg, Univ. of Arizona, and Dr. Jasvir Nagra, Google Inc.

Monday, December 6th, All Day. Separate registration and fee required.

Abstract. In this tutorial we will describe techniques for software protection. These are techniques for protecting secrets contained in computer programs from being discovered, modified, or redistributed. Important applications include protecting against software piracy, license check tampering, and cheating in on-line multiplayer games. With a series of interactive exercises and problems, you will get hands-on experience with methods you can use to protect your program as well as techniques that attackers use to analyze and crack applications. The attack model is very liberal: we assume that an adversary can study our program's code (maybe first disassembling or decompiling it), execute it to study its behavior (perhaps using a debugger), or alter it to make it do something different than what we intended (such as bypassing a license check). In a typical defense scenario we use code transformation techniques to add confusion to our code to make it more difficult to analyze (statically or dynamically), tamper-protection to prevent modification, and watermarking to assert our intellectual property rights (by embedding a hidden copyright notice or unique customer identifier).

Background. Software protection is a fairly new branch of computer security. It's a field that borrows techniques not only from computer security, but also from many other areas of Computer Science such as cryptography, steganography, media watermarking, software metrics, reverse engineering, and compiler optimization. The problems we work on are different from other branches of computer security: we are concerned with protecting the secrets contained within computer programs. We use the word secrets loosely, but the techniques we present in this tutorial (code obfuscation, software watermarking and fingerprinting, tamper-proofing, and birthmarking) are typically used to prevent others from exploiting the intellectual effort invested in producing a piece of software.

For example, software fingerprinting can be used to trace software pirates, code obfuscation can be used to make it more difficult to reverse engineer a program, and tamperproofing can make it harder for a hacker to remove a license check.

Outline

1. **Introduction.** What is software protection? What problems do we work on?
2. **Attack Models.** Who is our adversary? What techniques are at his disposal?
3. **Code Obfuscation.** Code transformation techniques for preventing malicious reverse engineering of programs. How do we defeat static analysis? How do we defeat dynamic analysis? How can adversaries use obfuscation to affect the results of electronic voting?
4. **Obfuscation Theory.** Theoretical background to obfuscation. What can we hide in a program? What can't we hide in a program?
5. **Tamperproofing.** Techniques for preventing modifications of programs. How can we stop the removal of licensing checks? How can we stop cheating in on-line games? How can we prevent attacks against the TCP stack that could potentially take down the Internet?
6. **Watermarking.** Techniques for embedding unique identifiers in programs to prevent software piracy.
7. **Conclusion.** Directions for future research.

Prerequisites. An understanding of basic compiler/program analyis techniques is helpful, but not necessary.

About the Instructors. Dr. Christian Collberg received a BSc in Computer Science and Numerical Analysis and a Ph.D. in Computer Science from Lund Univ., Sweden. He is currently an Associate Professor in the Department of Computer Science at the Univ. of Arizona and has also worked at the Univ. of Auckland, New Zealand, and the Chinese Academy of Sciences in Beijing. Prof. Collberg is a leading researcher in the intellectual property protection of software, and also maintains an interest in compiler and programming language research. In his spare time he writes songs, sings, and plays guitar for The Zax and hopes one day to finish up his Great Swedish Novel.

Dr. Jasvir Nagra received his B.Sc. in Mathematics and Computer Science and a Ph.D. in Computer Science from the Univ. of Auckland, New Zealand. He's been a Post Doctoral scholar on the RE-TRUST project at the Univ. of Trento where his focus was on applying obfuscation, tamperproofing and watermarking techniques to protect the integrity of software executing on a remote untrusted platform. His research interests also include the design of programming languages and its impact on the security of applications. He's currently with Google,

Inc where he is building Caja, a open-sourced, secure-subset of javascript. In his spare time Jasvir dabbles with Lego and one day hopes to finish building his Turing machine made entirely out of Lego blocks.

Tutorial *T4. System Life Cycle Security Engineering*

Instructor(s): Ms. Thuy D. Nguyen and Dr. Cynthia E. Irvine, Naval Postgraduate School

Monday, December 6th, All Day. Separate registration and fee required.

Within the discipline of systems engineering, information systems security engineering (ISSE) applies information assurance principles across a system's life cycle. Grounded by underlying security principles and a rigorous methodology, ISSE follows the "system thinking" approach for assessing system security behaviors based on dependencies, interactions and emergent properties of its components in the context of a larger system.

This tutorial aims to provide attendees with an overview of the ISSE methodologies and processes for the design, implementation and assessment of risk-based security solutions. Concepts and practices of information systems security engineering are presented from a system life cycle perspective. Core topics include security requirement engineering, architecture and design analysis, system implementation assessment, requirements/ implementation traceability correspondence, security test and evaluation strategy, and risk management. These topics are structured to follow the NIST risk management framework. In each stage of the system development life cycle, the roles and responsibilities of the ISSE team are explained.

Through the tutorial, attendees will understand the importance of capturing user's needs in a tractable form to guide development and risk analysis activities. They will be familiar with the properties used to evaluate different security architectures, the inherent trust problems relating to the composition of systems and components, and security issues associated with the adaptation of existing systems to meet the need for technological and environmental evolution.

Outline

1. **Introduction to Information Systems Security Engineering.** This module presents an overview of the following ISSE activities in a system development life cycle: (1) Discover Information Protection Needs; (2) Define System Security Requirements; (3) Design System Security Architecture; (4) Develop Detailed Security Design; (5) Implement System Security. This module also explores the Risk Management Framework defined by NIST and reviews ISSE responsibilities in the risk management cycle of a system to assess the effectiveness and residual risk of the system's protection mechanisms.

2. **Life Cycle Assurance Practices.** This module emphasizes the "baked in" security strategy and the notions of defense in breadth and defense in depth. Topics to be covered include: (1) Defense in breadth: evaluating risk throughout a system's life cycle; (2) Defense in depth: protecting against attacks by employing appropriate protection mechanisms in keys areas; (3) Trust relationships among components in large/complex systems: composition, balanced assurance, interconnection.

3. **Security Requirement Engineering.** This module presents a general security requirements engineering framework that includes the following activities: (1) Security requirements elicitation; (2) Threat/risk analysis; (3) Security requirements derivation; (4) Security requirements validation.

4. **Security Architecture and Design.** This module focuses on the following: (1) Architectural properties and strategies for reasoning about the security architecture of a system; (2) Security design requirements and engineering activities for developing and analyzing the security design for a secure system.

Prerequisites. It is assumed that participants have knowledge of basic security concepts and principles, and an understanding of computer, software and network security fundamentals. In addition, familiarity with system life cycle assurance (including threat characterization and risk analysis) and general systems engineering processes would be useful.

About the Instructor. Ms. Thuy D. Nguyen is a Senior Research Associate of Computer Science at the Naval Postgraduate School in Monterey, California. She has 25 years of experience and specializes in high assurance software and systems development, security evaluation and information systems security engineering. Ms. Nguyen performs research on high assurance platforms, trusted operating systems and separation kernels, secure collaborative applications, MLS federated architectures and dynamic security services. She is the lead architect/engineer of the MYSEA multilevel secure (MLS) project and oversees the construction of a MLS testbed. She co-authored a Common Criteria Protection Profile for highly robust separation kernels and

a draft Computing Platform Architecture and Security Criteria for the High Assurance Platform Program. She has developed and taught courses on security requirements engineering and applied information systems security engineering. Prior to NPS, she developed commercial security products, including a TCSEC Class A1 security kernel.

Dr. Cynthia E. Irvine is a Professor in the Department of Computer Science and Director of the Center for Information Systems Security Studies and Research (CISR) at the Naval Postgraduate School, where she has worked since 1994. She was the founding director of the Cebrowski Institute at NPS from 2001 to 2003. A graduate of Rice and Case Western Reserve Universities, her research centers on the design and construction of high assurance systems and multilevel security. The author on over 150 papers and reports on cyber security, she has supervised over 120 Masters and PhD students. Dr. Irvine has served on numerous government computer and network security committees and review boards. Her memberships include: the ACM, ASP (life), IEEE (Senior) and the IEEE Computer Society Golden Core. A recipient of the Navy Information Assurance Award as well as numerous research and service awards, she served as Chair of the IEEE Technical Committee on Security and Privacy from 2007 to 2009.

Tutorial *T5. Virtualization and Security*

Instructor(s): Mr. Zed Abbadi, Public Company Accounting Oversight Board (PCAOB)

Tuesday, December 7th, Morning Only. Separate registration and fee required.

In recent years, virtualization has become one of the most deployed technologies in the IT field. It provides clear benefits when it comes to utilization, maintenance, redundancy and lower power consumption. However, just like every new technology, virtualization is still evolving and there are still unanswered security questions. Virtualization is a concept that encompasses many types of technologies used in different configurations and for a variety of reasons. Each one of these technologies presents its own unique sets of security challenges and benefits.

This tutorial will provide a basic understanding of the various virtualization technologies and discuss the security aspects and characteristics of each one. It will provide the audience with valuable material on how to utilize virtualization to decrease risks from security attacks and how to avoid vulnerabilities that may accompany virtualization technologies.

Outline

1. **Virtualization Basics:** An introduction to the various types of virtualization technologies and their typical usage. This includes server and client virtualization, and the different software/hardware solutions that exit in the market today.
2. **Server Virtualization Security:** A detailed discussion focused on server virtualization and the underlying security benefits and challenges. The discussion will cover bare-metal (monolithic vs. microkernel) and hosted technologies.
3. **Client Virtualization Security:** A detailed discussion focused on client virtualization and the underlying security benefits and challenges. The discussion will cover desktop (local and hosted) and application (local and hosted) virtualization technologies.
4. **Other Virtualization Technologies:** Other evolving virtualization technologies including OS Steaming and Workspace Virtualization and the security implications that accompany them.

Prerequisites. General understanding of computer architecture and basic security concepts.

About the Instructor. Mr. Zed Abbadi is an Application Security Manager with the Public Company Accounting Oversight Board (PCAOB). He has over 18 years of experience in software and security engineering. His experience ranges from providing security consulting services to building large-scale software systems. In his current role he is responsible for the security of all software applications that run on PCAOB's infrastructure.

Zed holds a Bachelor of Science in Computer Science and a Masters degree in Systems Engineering from George Mason Univ.. He is a published author and has presented at various security conferences.

Tutorial *T6. Keeping Your Web Apps Secure: The OWASP Top 10 & Beyond*

Instructor(s): Mr. Robert H'obbes' Zakon, Zakon Group LLC

Tuesday, December 7th, Afternoon Only. Separate registration and fee required.

The Open Web Application Security Project (OWASP) Top 10 provides an overview of the most critical web application security risks. This tutorial introduces the OWASP Top 10 (2010 edition) along with other risks,

and discusses the techniques and practices to protect against them. References to software tools and other secure coding resources will also be provided. This tutorial is a must if you are developing web applications, managing developers, researching web security, or simply are a security enthusiast.

Outline

1. **Introduction.** Overview of the need for secure coding practices in web application development.
2. **The OWASP Top 10.** From Injection and Cross-Site Scripting (XSS) to Insecure Cryptographic Storage and Cross-Site Request Forgery (CSRF) we will cover OWASP's Top 10 Risks in detail how these risks lead to vulnerabilities, and how to mitigate them.
3. **Beyond the Top 10.** The Top 10 are not meant to be comprehensive, but to make developers aware of the most commonly encountered risks. Here we will cover additional risks and vulnerabilities that every web developer needs to be aware of, along with how to mitigate them.
4. **Gotchas, Pitfalls & Prevention.** In addition to secure coding practices addressing potential vulnerabilities, there are still some underlying technologies that could result in unintended consequences. Learn about what these are and how to prevent them from being exploited.
5. **Security Tools & Resources.** It's a half-day course, so you get lots of references to additional resources and tools.

Prerequisites. Some understanding of web application development may be helpful when discussing risk mitigation techniques.

About the Instructor. Mr. Robert Zakon is a technology consultant and developer who has been programming web applications since the Web's infancy, over 15 years ago. In addition to developing web applications for web sites receiving millions of daily hits, he works with organizations in an interim CTO capacity, and advises corporations, non-profits and government agencies on technology, information, and security architecture and infrastructure. Robert is a former Principal Engineer with MITRE's infosec group, CTO of an Internet consumer portal and application service provider, and Director of a university research lab. He is a Senior Member of the IEEE, and holds BS & MS degrees from Case Western Reserve Univ. in Computer Engineering & Science with concentrations in Philosophy & Psychology. His interests are diverse and can be explored at `www.Zakon.org`.

Tutorial *T7. State of the Practice: Secure Coding*

Instructor(s): Mr. Robert C. Seacord, CERT Software Engineering Institute

Tuesday, December 7th, All Day. Separate registration and fee required.

State of the practice courses provide an introduction and overview of the current state of research in a particular discipline with the intent of informing beginning doctoral students an overview of research, technology and outstanding problems in a particular discipline. This state of the practice tutorial describes the state of the practice in secure C language programming as defined by the C99 standard and the emerging C1X standard. The tutorial also identifies outstanding problems in these standards, and identifies where further research is necessary. The tutorial also describes The CERT C Secure Coding Standard as well as the work and progress of the WG14 C Secure Coding Guidelines study group.

Outline

1. **History of C language programming.** Origins. The C90, C99, and C1X standards. Common vulnerabilities. The role of secure coding standards.
2. **C programming language and library research.** Implementation-defined, unspecified, and undefined behaviors. Poorly designed library functions. Poorly understood behaviors. Dangerous optimizations. Unmanaged environments. Encoding and decoding pointers. Security attributes. Concurrency.
3. **C1X improvements.** Annex K Bounds-checking interfaces. Annex L Analyzability. Static Assertions. File I/O.
4. **Analysis Research.** Static analysis. Dynamic analysis. Safe secure C/C++ methods. Model checking. Contributing analysis tools: case studies.
5. **Runtime protection schemes research.** Randomization. W^X. Pointer encoding/decoding. Secure heap. Capability-based systems.
6. **Additional Research Areas.** Underlying causes of vulnerabilities, effective and enforceable secure coding guidelines, and effectiveness of static analysis in analyzing open source software.

Prerequisites. Tutorial participants should be familiar with C language programming. Practicing C and C++ programmers will derive the greatest benefit but programmers who use other languages such as Java will also find the tutorial useful.

About the Instructor. Mr. Robert C. Seacord is the author of The CERT C Secure Coding Standard (Addison-Wesley, 2008) and Secure Coding in C and C++ (Addison-Wesley, 2005), providing guidance on secure practices in C and C++ programming. Seacord leads the Secure Coding Initiative at CERT, located in Carnegie Mellon's Software Engineering Institute (SEI) in Pittsburgh, PA. CERT's Secure Coding Initiative develops and promulgates secure coding practices and techniques, such as CERT's Secure Code Analysis Laboratory (SCALe), the first to certify software for conformance with secure coding standards. His research group develops publicly available tools for the analysis and development of secure software. Seacord is an adjunct professor in the Carnegie Mellon Univ. School of Computer Science and in the Information Networking Institute and frequent speaker throughout the world. Seacord is also a technical expert for the ISO/IEC JTC1/SC22/WG14 international standardization working group for the C programming language.

Tutorial *T8. An Introduction to Usable Security*

Instructor(s): Dr. Jeff Yan, Newcastle Univ., UK, and Mary Ellen Zurko, IBM, USA

Tuesday, December 7th, All Day. Separate registration and fee required.

For a long time, computer security was mainly concerned with the design of various technical mechanisms for defending against adversaries, as well as with the underlying mathematical foundations such as cryptography primitives. However, the usability of such technical mechanisms was largely ignored, which unfortunately has proved a major cause of many computer security failures. In particular, many technical solutions though theoretically sound were practically insecure because of their poor usability.

In recent years, "usable security" (or "security usability") has attracted fast growing attention in both academia and industry. More and more people agree that we need usable security systems - unusable secure systems are not used properly or at all, and thus only usable systems can provide effective security. However, there is less agreement about how to design systems that are both usable and secure.

Outline This full-day tutorial will give an overview of the field of usable security with the focus on principles, approaches and research methods of usable security. A large number of real-life examples will be used to illustrate that it is feasible to develop security solutions that are simultaneously secure and usable. With the aim to enable participants to both evaluate and produce high-quality work in usable security, the tutorial is tentatively structured as follows:

1. **Part 1: Fundamentals.** How security has failed due to the failure of usability of security technologies. Psychological aspect of computer security, highlighting that what security engineers expect to work and what the user makes to work, can differ greatly. The contrast between theoretical and effective practical security will be highlighted. Examples of how security has failed due to usability will enable the attendee to recognize common mistakes. Early research in the field will be touched on, providing a background on motivations and an historical context for the field.

2. **Part 2: Approaches and methods.** Common approaches to usable security and relevant design principles for security usability will be discussed. Methods for improving security usability and methods for empirically establishing such improvement will be discussed in detail. Usability techniques successfully applied to security, including usable design (with an emphasis on error handling and task flow), lab user studies (a field advanced enough that simple and useful guidance is available in book form), field user studies, and techniques for evaluating organizational cultures. The difficulties peculiar to the usability of security will also be discussed.

3. **Part 3: Case studies.** Real-life examples illustrating how security and usability can be simultaneously improved, and how the principles and methods introduced in the previous part were applied. Reflections and critiques on the application of the methods. Topics that have received much attention will be highlighted, including authentication (particularly password use and graphical authentication), access control and authorization, phishing defenses, the utility of education of the user, and CAPTCHAs. The impact of organizational culture will receive particular attention, as we expect compliance, education, and organizational rules and guidelines to be of particular interest to ACSAC attendees. Recent usable security and privacy research in social networks will also be included.

4. **Conclusions.**

Prerequisites. Basic understanding of computer security. The intended audience are security researchers who want to step into the field of usable security, and security practitioners who wish to understand the impact of usable security on their work and integrate some of its lessons, techniques, and developments. PhD students and new researchers in usable security who want to have a quick start in this field will also benefit. Those who want to teach this topic can also find the tutorial relevant - a set of summary notes and a large number of pointers to further readings will be provided, so that it should be easy for them to extend the tutorial into a full course.

About the Instructor. Dr. Jeff Yan is on the faculty of computer science at Newcastle Univ., England. He has a PhD in computer security from Cambridge Univ.. The password security and memorability study he carried out with colleagues in 1999 - 2000 was an early influential work in the field of usable security. He is a contributor to the O'Reilly book "Security and Usability: Designing Secure Systems that People Can Use" (2005), the first book on usable security, and was on the program committee for the first Symposium on Usable Privacy and Security (SOUPS) held at Carnegie Mellon in 2005. Recent work on usable security in his team includes 1) a novel graphical password scheme (CCS'07), which was selected by the Royal Society - the UK's national academy - for their 2008 Summer Science Exhibition, and 2) the robustness and usability of CAPTCHAs (CCS'08, SOUPS'08), which has influenced the design of a number of CAPTCHAs including those that have been deployed by Microsoft and Yahoo!

Mary Ellen Zurko is security architect of the collaboration cloud offerings at IBM. She has over two decades of work in user-centered security, in product development, early product prototyping, and research. Her experience spans across the entire lifecycle of software products, from initial product definition and delivery, to mature product maintenance, with an emphasis on distributed middleware and collaboration. She is chair of the steering committee of the International WWW Conference series, on the steering committee of New Security Paradigms Workshop and a senior fellow on ACSA.

Training Details

Training TR1 *Cyber Security Controls: NIST SP 800-53 Rev3 & CNSSI 1253*

Instructor: Dr. Marshall D. Abrams, The MITRE Corporation

Wednesday, December 8th, 10:30-12:00 & 13:30-15:00

The National Institute of Standards and Technology (NIST), in collaboration with the Office of the Director of National Intelligence, the Department of Defense, and the Committee on National Security Systems (CNSS), recently updated Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations. This historic publication, for the first time, contains a unified set of security controls for both non national security and national security systems. This session provides an overview of the unified security control catalog and the security control selection process described in NIST SP 800-53, Revision 3, as well as an introduction to CNSS Instruction 1253, the publication that provides implementation guidance for the national security community using SP 800-53.

Prerequisites. None.

About the Instructor. Dr. Marshall D. Abrams is a Principal Scientist at the MITRE Corporation in McLean, Virginia. He holds two patents and has authored many documents addressing cyber security. He has taught cyber security courses on six continents. He received the BSEE from Carnegie Institute of Technology and the MSEE and Ph.D. from the Univ. of Pittsburgh. While at the National Bureau of Standards he received the Department of Commerce Silver Metal Award. Two awards were received from the Federal Aviation Administration for contributions to the Information Systems Security Program. He is a Senior Life Member of the IEEE and has been honored with the IEEE Computer Society Golden Core award. He is also a Senior Fellow of the Applied Computer Security Associates. Marshall has been involved with the NIST FISMA Implementation Project since its inception.

Training TR2 *Near Real-Time Risk Management Process: NIST SP 800-37*

Instructor: Dr. Marshall D. Abrams, The MITRE Corporation

Wednesday, December 8th, 15:30-17:00 & Thursday, December 9th, 10:30-12:00

The National Institute of Standards and Technology (NIST), in collaboration with the Office of the Director of National Intelligence, the Department of Defense, and the Committee on National Security Systems (CNSS), recently updated Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, (formerly the security certification and accreditation guideline). The revised publication transforms the traditional static, stovepiped certification and accreditation process into a process that supports near real-time risk management. This session describes how the process of certification and accreditation is integrated into the Risk Management Framework, and focuses on the continuous monitoring of security controls to determine the security state of organizational information systems and environments of operation.

Prerequisites. None.

Training TR3 *Integrated Enterprise-Wide Risk Management Organization, Mission, and Information System View: NIST SP 800-39*

Instructor: Dr. Marshall D. Abrams, The MITRE Corporation

Thursday, December 9th, 13:30-15:00 & 15:30-17:00

Information technology is widely recognized as the engine that drives the U.S. economy, giving industry a competitive advantage in global markets, enabling the federal government to provide better services to its citizens, and facilitating greater productivity as a nation. Risk related to the operation and use of information systems is one of many components of organizational risk that senior leaders address as a routine part of their ongoing risk management responsibilities. Effective risk management requires that organizations operate in a highly complex and interconnected world using state-of-the-art and legacy information systems systems that organizations depend upon to accomplish critical missions and to conduct important business-related functions. Special Publication 800-39 is the flagship document in the series of FISMA publications and provides a structured, yet flexible approach for managing that portion of risk resulting from the operation and use of information systems to support the missions and mission/business processes of organizations. This session will examine Special Publication 800-39 guidelines for an integrated, enterprise wide approach to managing risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of information systems.

Prerequisites. None - Open to anyone interested in increasing their understanding of Risk Management.

Training TR4 *Risk Assessments for Information Technology Systems: NIST SP 800-30*

Instructor: Pete Gouldmann, U.S. Department of State

Friday, December 10th, 8:30-10:00 & 10:30-12:00

Prerequisites. None - Open to anyone interested in increasing their understanding of Risk Assessment.

About the Instructor. Mr. Peter Gouldmann is the Department of State Liaison to the National Institute of Standards and Technology (NIST) and Co-Chair of the Permanent Subcommittee to the Committee for National Security Systems (CNSS). As a Supervisory Information Technology Specialist in the Office of Information Assurance, Mr. Gouldmann has served as Risk Officer, Chief of Systems Authorization, and Security Architect. Over the past 32 years, Mr. Gouldmann has held IT and IT security-leadership positions within the Department of State, the private sector and the United States Air Force. He holds a Masters Degree in Information Management from Syracuse Univ., and is a distinguished graduate of the National Defense Univ.'s Advanced Management Program. Mr. Gouldmann has been awarded the CIO certificate in Federal Executive Competencies from the CIO Univ., and holds the Certified Information Systems Security Professional (CISSP) credential.

Sponsors

ACSAC Steering Committee

Marshall Abrams, The MITRE Corporation
Jeremy Epstein, SRI International
Daniel Faigin, The Aerospace Corporation
Ann Marmor-Squires, The Sq Group
Steve Rome, Booz Allen Hamilton
Ron Ross, National Institute of Standards and Technology
Christoph Schuba, Oracle Corporation
Cristina Serban, AT&T
Dan Thomsen, SIFT

ACSA

Marshall Abrams, The MITRE Corporation (Founder and Asst Treasurer)
Jeremy Epstein, SRI International (Vice President)
Daniel Faigin, The Aerospace Corporation (Secretary)
Ann Marmor-Squires, The Sq Group
Steve Rome, Booz Allen Hamilton (President)
Harvey Rubinovitz, The MITRE Corporation (Treasurer)
Cristina Serban, AT&T
Mary Ellen Zurko, IBM Corporation

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