

Tuesday

ACSAC 2005 December 5-9 Quick Glance

December 6

8:30 Welcome and Distinguished Practitioner: Brian Snow, National Security Agency - "We Need Assurance!"

10:00 Break

<b>10:30 Software Security</b> <ul style="list-style-type: none"> <li>Model Checking An Entire Linux Distribution for Security Violations</li> <li>Strengthening Software Self-Checksumming via Self-Modifying Code</li> <li>Countering Trusting Trust through Diverse Double-Compiling</li> </ul>	<b>Network Intrusion Detection</b> <ul style="list-style-type: none"> <li>A Framework for Detecting Network-Based Code Injection Attacks Targeting Windows and UNIX</li> <li>Exploiting Independent State for Network Intrusion Detection</li> <li>A Host-Based Approach to Network Attack Chaining Analysis</li> </ul>	<b>Case Study: Security Management</b> <ul style="list-style-type: none"> <li>iTSafe</li> <li>Implementing Long-Term, Coarse Traffic Capture</li> <li>PATCHLINK UPDATE: Patch &amp; Vulnerability Management Remedy for MidMichigan Medical Center</li> </ul>
--	---	---

12:00 Lunch

<b>13:30 Security Designs</b> <ul style="list-style-type: none"> <li>A Nitpicker's Guide to a Minimal-Complexity Secure GUI</li> <li>A User-Level Framework for Auditing and Monitoring</li> <li>TARP: Ticket-based Address Resolution Protocol</li> </ul>	<b>Protocol Analysis</b> <ul style="list-style-type: none"> <li>Verify Results of Network Intrusion Alerts Using Lightweight Protocol Analysis</li> <li>Improving the Security of TCG Specification</li> <li>Code Security Analysis of a Biometric Authentication System Using Automated Theorem Provers - A Case Study</li> </ul>	<b>Case Study: Secure Access</b> <ul style="list-style-type: none"> <li>A Secure Public Sector Workflow Management System</li> <li>Representing Reality in a Research Environment</li> <li>Leveraging IPSec for Mandatory Access Control of Linux Network Communications</li> </ul>
--	--	---

15:00 Break

<b>15:30 Vulnerability Assessment</b> <ul style="list-style-type: none"> <li>Automated and Safe Vulnerability Assessment</li> <li>Understanding Complex Network Attack Graphs through Clustered Adjacency Matrices</li> <li>Intrusion Detection in RBAC-Administered Databases</li> </ul>	<b>Panel:</b> <b>How Does Information Assurance R&amp;D Impact Information Assurance in Practice?</b>  <b>Chair:</b> Dr. Doug Maughan DHS Dr. Steve King DoD/DDR&E Mr. Mark Powell FAA Mr. Michael Brown FAA	<b>Case Study: Managing the Enterprise</b> <ul style="list-style-type: none"> <li>Aligning Roles for a Managed Security Environment</li> <li>Security Methodology and Incident Response</li> <li>Designing for Insecurity</li> </ul>
---	--	--

17:00 Break

18:00 Exhibits, NISS Award, NIAP Ceremony and Reception

Wednesday

December 7

8:30 Invited Essayist: Mary Ellen Zurko, IBM Corporation - "User Centered Security: Social, Technical and Practical Challenges"

10:00 Break

<b>Automation</b> <ul style="list-style-type: none"> <li>ScriptGen: an Automated Script Generation Tool for Honeyd</li> <li>Automatic Generation of Buffer Overflow Attack Signatures: An Approach Based on Program Behavior Models</li> <li>Evolving Successful Stack Overflow Attacks for Vulnerability Testing</li> </ul>	<b>Security Analysis</b> <ul style="list-style-type: none"> <li>Java for Mobile Devices: A Security Study</li> <li>Lessons Learned: A Security Analysis of the Internet Chess Club</li> <li>Building Evidence Graphs for Network Forensics Analysis</li> </ul>	<b>Case Study: Internet Security Visualization</b> <ul style="list-style-type: none"> <li>Internet Security Visualization Case Study: Instrumenting a Network for NetFlow Security Visualization Tools</li> <li>Visualizing Connection Traffic</li> <li>Creating Dynamic Baselines Visually</li> </ul>
--	--	--

12:00 Lunch

13:30 Technology Blitz! Technology presentations from industry

15:00 Break

<b>OS Security Mechanisms</b> <ul style="list-style-type: none"> <li>Multi-level Security Requirements for Hypervisors</li> <li>Building a MAC-based Security Architecture for the Xen Opensource Hypervisor</li> <li>E-NeXSh: Achieving an Effectively Non-Executable Stack and Heap via System-Call Policing</li> </ul>	<b>Data Integrity</b> <ul style="list-style-type: none"> <li>Dynamic Taint Propagation for Java</li> <li>An Integrity Verification Scheme for DNS Zone File Based on Security Impact Analysis</li> <li>Paranoid: A Global Secure File Access Control System</li> </ul>	<b>Panel:</b> <b>Thinking of a Career in Information Assurance and How to Advance in the Field</b>  <b>Chair :</b> Marla Collier Internet Resources
---	--	---

17:00 Break

17:30 Works in Progress - 19 presentations in 90 minutes

<b>8:30</b>	<b>Classic Papers</b> <ul style="list-style-type: none"> <li>• <i>Looking Back on the Bell-LaPadula Model</i>, David Elliott Bell</li> <li>• <i>The Pump: A Decade of Covert Fun</i>, Myong H. Kang, Naval Research Laboratory</li> </ul>
-------------	---

**10:00 Break**

<b>10:30 Malware</b> <ul style="list-style-type: none"> <li>• <i>Design and Implementation of an Extrusion-Based Break-In Detector for Personal Computers</i></li> <li>• <i>Detecting Intra-Enterprise Scanning Worms based on Address Resolution</i></li> <li>• <i>Stealth Breakpoints</i></li> </ul>	<b>Panel:</b> <b>Highlights from the 2005 New Security Paradigms Workshop</b> <b>Chair: Abe Singer</b> <i>San Diego Supercomputer Center</i>	<b>Case Study: Security in Health Care</b> <ul style="list-style-type: none"> <li>• <i>The OneHealthPort Trusted Community: Simplifying Access to Information for Healthcare</i></li> <li>• <i>Curing Secure Remote Access Pains</i></li> <li>• <i>Enterprise Single Sign-On: How City Hospital Cured Its Password Pain</i></li> </ul>
--	---	--

**12:00 Lunch**

<b>13:30 Distributed System Security</b> <ul style="list-style-type: none"> <li>• <i>mSSL: Extending SSL to Support Data Sharing Among Collaborative Clients</i></li> <li>• <i>Layering a Public-Key Distribution Service over Secure DNS</i></li> <li>• <i>PorKI: Making User PKI Safe on Machines of Heterogeneous Trustworthiness</i></li> </ul>	<b>Access Control</b> <ul style="list-style-type: none"> <li>• <i>Uniform Application-Level Access Control Enforcement of Organizationwide Policies</i></li> <li>• <i>Using Continuous Biometric Verification to Protect Interactive Login Sessions</i></li> <li>• <i>Improved Port Knocking with Strong Authentication</i></li> </ul>	<b>Case Study: Common Criteria</b> <ul style="list-style-type: none"> <li>• <i>Writing a Protection Profile for a Security Service Package</i></li> <li>• <i>MILS, Multiple Independent Levels of Security</i></li> <li>• <i>A Comprehensive Review of the National Information Assurance Partnership</i></li> </ul>
---	--	--

**15:00 Break**

<b>15:30 Passwords and Applied Crypto</b> <ul style="list-style-type: none"> <li>• <i>Graphical Passwords: A Survey</i></li> <li>• <i>Have the Cake and Eat It Too – Infusing Usability into Text- Password Based Authentication Systems</i></li> <li>• <i>Fault Attacks on Dual-Rail Encoded Systems</i></li> </ul>	<b>Defense in Depth / Database Security</b> <ul style="list-style-type: none"> <li>• <i>Survivability Architecture of a Mission-Critical System: the DPASA Example</i></li> <li>• <i>Generating Policies for Defense in Depth</i></li> <li>• <i>Defensive Execution of Transactional Processes Against Attacks</i></li> </ul>	<b>Case Study: Privacy</b> <ul style="list-style-type: none"> <li>• <i>Privacy Requirements Implemented with a JavaCard</i></li> <li>• <i>Privacy-Preserving Alert Correlation: A Concept Hierarchy Based Approach</i></li> <li>• <i>Securing Email Archives through User Modeling</i></li> </ul>
--	---	---

**17:00**

**Monday Tutorials and Issues Workshop December 5**

<b>8:30</b>	M1 <b>Web Application Security</b>	M2 <b>Common Criteria Version 3</b>	M3 <b>Trust Management</b>	Issues Workshop <b>Malicious Software (Prevention and Defense) Special Workshop</b>
<b>12:00</b>	<b>Lunch</b>			
<b>13:30</b>			M4 <b>Defenses Against Viruses, Worms, and Malicious Software</b>	

**17:00**

**Friday Tutorials December 9**

<b>8:30</b>	F5 <b>Acquisition and Analysis of Large Scale Network Data V.2.</b>	F6 <b>Practical Security Policy Modeling</b>	F7 <b>Securing Enterprise &amp; Government Web Service Applications: A Lifecycle Perspective</b>
<b>12:00</b>	<b>Lunch</b>		
<b>13:30</b>			F8 <b>Identifying and Addressing Mobile Security Issues</b>

**17:00**