# Table of Contents

Welcome from the Conference Chair ___________________________________________ ix  
Welcome from the Program Chairs ____________________________________________ x  
Conference Committee _______________________________________________________ xi  
Program Committee ________________________________________________________ xii  
Additional Reviewers and Tutorial Reviewers___________________________________ xiii  
ACSAC Steering Committee _________________________________________________ xiv  
Sponsor: Applied Computer Security Associates ________________________________ xv  

---

**Invited Talk**

Structuring for Strategic Cyber Defense: A Cyber Manhattan Project Blueprint ______________________________ 3  
*O. Sami Saydjari*

---

**Forensics and Security Management**

Practical Applications of Bloom Filters to the NIST RDS and Hard Drive Triage _____________________________ 13  
*Paul Farrell, Simson L. Garfinkel, and Douglas White*

Systematic Signature Engineering by Re-use of Snort Signatures _____________________________ 23  
*Sebastian Schmerl, Hartmut Koenig, Ulrich Flegel, Michael Meier, and René Rietz*

Analysing the Performance of Security Solutions to Reduce Vulnerability  
Exposure Window  
*Yolanta Beres, Jonathan Griffin, Simon Shiu, Max Heitman, David Markle, and Peter Ventura*
## Operating Systems and Memory Security

New Side Channels Targeted at Passwords

*Albert Tannous, Jonathan Trostle, Mohamed Hassan, Stephen E. McLaughlin, and Trent Jaeger*

PinUP: Pinning User Files to Known Applications

*William Enck, Patrick McDaniel, and Trent Jaeger*

Defending Against Attacks on Main Memory Persistence

*William Enck, Kevin Butler, Thomas Richardson, Patrick McDaniel, and Adam Smith*

## Kernel-Level Defensive Techniques

Automatic Inference and Enforcement of Kernel Data Structure Invariants

*Arati Baliga, Vinod Ganapathy, and Liviu Iftode*

VICI — Virtual Machine Introspection for Cognitive Immunity

*Timothy Fraser, Matthew R. Evenson, and William A. Arbaugh*

Soft-Timer Driven Transient Kernel Control Flow Attacks and Defense

*Jinpeng Wei, Bryan D. Payne, Jonathon Giffin, and Calton Pu*

## Graphical Passwords and Biometrics

On Purely Automated Attacks and Click-Based Graphical Passwords

*Amirali Salehi-Abari, Julie Thorpe, and P.C. van Oorschot*

YAGP: Yet Another Graphical Password Strategy

*Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, and Xiyang Liu*

Privacy-Aware Biometrics: Design and Implementation of a Multimodal Verification System

*Stelvio Cimato, Marco Gamassi, Vincenzo Piuri, Roberto Sassi, and Fabio Scotti*

Improving the Efficiency of Capture-Resistant Biometric Authentication Based on Set Intersection

*Xunhua Wang, Philip D. Huff, and Brett C. Tjaden*

## Access Control

ProActive Access Control for Business Process-Driven Environments

*Mathias Kohler and Andreas Schaad*

Assessing Quality of Policy Properties in Verification of Access Control Policies

*Evan Martin, JeeHyun Hwang, Tao Xie, and Vincent Hu*

Please Permit Me: Stateless Delegated Authorization in Mashups

*Ragib Hasan, Marianne Winslett, Richard Conlan, Brian Slesinsky, and Nandakumar Ramani*

Implementing ACL-Based Policies in XACML

*Günter Karjoth, Andreas Schade, and Els Van Herreweghen*
**Network Security**

- Execution Trace-Driven Automated Attack Signature Generation ........................................... 195  
  *Susanta Nanda and Tzi-cker Chiueh*

- Improving Security Visualization with Exposure Map Filtering .............................................. 205  
  *Mansour Alsaleh, David Barrera, and P.C. van Oorschot*

  *Yinqian Zhang, Xun Fan, Yijun Wang, and Zhi Xue*

- Host-Centric Model Checking for Network Vulnerability Analysis ............................................. 225  
  *Rattikorn Hewett and Phongphun Kijsanayothin*

**Role-Based Access Control**

- The Role Hierarchy Mining Problem: Discovery of Optimal Role Hierarchies ................................ 237  
  *Qi Guo, Jaideep Vaidya, and Vijayalakshmi Atluri*

- Permission Set Mining: Discovering Practical and Useful Roles .............................................. 247  
  *Dana Zhang, Kotagiri Ramamohanarao, Tim Ebringer, and Trevor Yann*

- Enforcing Role-Based Access Control Policies in Web Services with UML and OCL .................. 257  
  *Karsten Sohr, Tanveer Mustafa, Xinyu Bao, and Gail-Joon Ahn*

**Intrusion Detection**

- Addressing Low Base Rates in Intrusion Detection via Uncertainty-Bounding Multi-Step Analysis .......... 269  
  *Robert J. Cole and Peng Liu*

- Toward Automatic Generation of Intrusion Detection Verification Rules .................................. 279  
  *Frederic Massicotte, Yvan Labiche, and Lionel C. Briand*

- STILL: Exploit Code Detection via Static Taint and Initialization Analyses ............................... 289  
  *Xinran Wang, Yoon-Chan Jhi, Sencun Zhu, and Peng Liu*

**Malware and Data Protection**

- McBoost: Boosting Scalability in Malware Collection and Analysis ................................. 301  
  *Roberto Perdisci, Andrea Lanzi, and Wenke Lee*

- MalTRAK: Tracking and Eliminating Unknown Malware .................................................. 311  
  *Amit Vasudevan*

- Preventing Information Leaks through Shadow Executions .................................................. 322  
  *Roberto Capizzi, Antonio Longo, V.N. Venkatakrishnan, and A. Prasad Sistla*

**Web-Based Applications Security**

- XSSDS: Server-Side Detection of Cross-Site Scripting Attacks ............................................ 335  
  *Martin Johns, Björn Engelmann, and Joachim Posegga*

- Anti-Phishing in Offense and Defense ................................................................................ 345  
  *Chuan Yue and Haining Wang*

- OMOS: A Framework for Secure Communication in Mashup Applications .................................. 355  
  *Saman Zarandioon, Danfeng (Daphne) Yao, and Vinod Ganapathy*
Anomaly and Misuse Detection

Behavior-Profile Clustering for False Alert Reduction in Anomaly Detection Sensors

Vanessa Frias-Martinez, Salvatore J. Stolfo, and Angelos D. Keromytis

Bluetooth Network-Based Misuse Detection

Terrence OConnor and Douglas Reeves

Bridging the Gap between Data-Flow and Control-Flow Analysis for Anomaly Detection

Peng Li, Hyundo Park, Debin Gao, and Jianming Fu

Classic Papers

Epilogue for RFC 1281, Guidelines for the Secure Operation of the Internet

Barbara Fraser and Steve Crocker

The Evolution of System-Call Monitoring

Stephanie Forrest, Steven Hofmeyr, and Anil Somayaji

Authentication

PAS: Predicate-Based Authentication Services Against Powerful Passive Adversaries

Xiaole Bai, Wenjun Gu, Sriram Chellappan, Xun Wang, Dong Xuan, and Bin Ma

pwdArmor: Protecting Conventional Password-Based Authentications

Timothy W. van der Horst and Kent E. Seamons

DARE: A Framework for Dynamic Authentication of Remote Executions

Erdem Aktas and Kanad Ghose

Applied Cryptography

Instruction Set Extensions for Enhancing the Performance of Symmetric-Key Cryptography

Sean O’Melia and Adam J. Elbirt

A Survey to Guide Group Key Protocol Development

Ahren Studer, Christina Johns, Jaanus Kase, Kyle O’Meara, and Lorrie Cranor

Transaction Oriented Text Messaging with Trusted-SMS

Antonio Grillo, Alessandro Lentini, Gianluigi Me, and Giuseppe F. Italiano

Author Index

viii