

*Proceedings*

---

# 24th Annual Computer Security Applications Conference

Anaheim, California  
December 8-12, 2008

**Sponsored by**  
Applied Computer Security Associates



Los Alamitos, California  
Washington • Tokyo



# TABLE OF CONTENTS

<b>Structuring for Strategic Cyber Defense: A Cyber Manhattan Project Blueprint</b> .....	1
<i>O. Sami Saydjari</i>	
<b>Practical Applications of Bloom Filters to the NIST RDS and Hard Drive Triage</b> .....	9
<i>Paul Farrell, Simson L. Garfinkel, Douglas White</i>	
<b>Systematic Signature Engineering by Re-use of Snort Signatures</b> .....	19
<i>Sebastian Schmerl, Hartmut Koenig, Ulrich Flegel, Michael Meier, René Rietz</i>	
<b>Analysing the Performance of Security Solutions to Reduce Vulnerability Exposure Window</b> .....	29
<i>Yolanta Beres, Jonathan Griffin, Simon Shiu, Max Heitman, David Markle, Peter Ventura</i>	
<b>New Side Channels Targeted at Passwords</b> .....	39
<i>Albert Tannous, Jonathan Trostle, Mohamed Hassan, Stephen E. McLaughlin, Trent Jaeger</i>	
<b>PinUP: Pinning User Files to Known Applications</b> .....	49
<i>William Enck, Patrick McDaniel, Trent Jaeger</i>	
<b>Defending Against Attacks on Main Memory Persistence</b> .....	59
<i>William Enck, Kevin Butler, Thomas Richardson, Patrick McDaniel, Adam Smith</i>	
<b>Automatic Inference and Enforcement of Kernel Data Structure Invariants</b> .....	69
<i>Arati Baliga, Vinod Ganapathy, Liviu Iftode</i>	
<b>VICI — Virtual Machine Introspection for Cognitive Immunity</b> .....	79
<i>Timothy Fraser, Matthew R. Evenson, William A. Arbaugh</i>	
<b>Soft-Timer Driven Transient Kernel Control Flow Attacks and Defense</b> .....	89
<i>Jinpeng Wei, Bryan D. Payne, Jonathon Giffin, Calton Pu</i>	
<b>On Purely Automated Attacks and Click-Based Graphical Passwords</b> .....	100
<i>Amirali Salehi-Abari, Julie Thorpe, P.C. van Oorschot</i>	
<b>YAGP: Yet Another Graphical Password Strategy</b> .....	110
<i>Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, Xiyang Liu</i>	
<b>Privacy-Aware Biometrics: Design and Implementation of a Multimodal Verification System</b> .....	119
<i>Stelvio Cimato, Marco Gamassi, Vincenzo Piuri, Roberto Sassi, Fabio Scotti</i>	
<b>Improving the Efficiency of Capture-Resistant Biometric Authentication Based on Set Intersection</b> .....	129
<i>Xunhua Wang, Philip D. Huff, Brett C. Tjaden</i>	
<b>ProActive Access Control for Business Process-Driven Environments</b> .....	139
<i>Mathias Kohler and Andreas Schaad</i>	
<b>Assessing Quality of Policy Properties in Verification of Access Control Policies</b> .....	149
<i>Evan Martin, JeeHyun Hwang, Tao Xie, Vincent Hu</i>	
<b>Please Permit Me: Stateless Delegated Authorization in Mashups</b> .....	159
<i>Ragib Hasan, Marianne Winslett, Richard Conlan, Brian Slesinsky, Nandakumar Ramani</i>	
<b>Implementing ACL-Based Policies in XACML</b> .....	169
<i>Günter Karjoth, Andreas Schade, Els Van Herreweghen</i>	
<b>Execution Trace-Driven Automated Attack Signature Generation</b> .....	179
<i>Susanta Nanda Tzi-cker Chiueh</i>	

<b>Improving Security Visualization with Exposure Map Filtering</b> .....	189
<i>Mansour Alsaleh, David Barrera, P.C. van Oorschot</i>	
<b>Attack Grammar: A New Approach to Modeling and Analyzing Network Attack Sequences</b> .....	199
<i>Yinqian Zhang, Xun Fan, Yijun Wang, Zhi Xue</i>	
<b>Host-Centric Model Checking for Network Vulnerability Analysis</b> .....	209
<i>Rattikorn Hewett, Phongphun Kijsanayothin</i>	
<b>The Role Hierarchy Mining Problem: Discovery of Optimal Role Hierarchies</b> .....	219
<i>Qi Guo, Jaideep Vaidya, Vijayalakshmi Atluri</i>	
<b>Permission Set Mining: Discovering Practical and Useful Roles</b> .....	229
<i>Dana Zhang, Kotagiri Ramamohanarao, Tim Ebringer Trevor Yann</i>	
<b>Enforcing Role-Based Access Control Policies in Web Services with UML and OCL</b> .....	239
<i>Karsten Sohr, Tanveer Mustafa, Xinyu Bao, Gail-Joon Ahn</i>	
<b>Addressing Low Base Rates in Intrusion Detection via Uncertainty-Bounding Multi-Step Analysis</b> .....	249
<i>Robert J. Cole, Peng Liu</i>	
<b>Toward Automatic Generation of Intrusion Detection Verification Rules</b> .....	259
<i>Frederic Massicotte, Yvan Labiche, Lionel C. Briand</i>	
<b>STILL: Exploit Code Detection via Static Taint and Initialization Analyses</b> .....	269
<i>Xinran Wang, Yoon-Chan Jhi, Sencun Zhu, Peng Liu</i>	
<b>McBoost: Boosting Scalability in Malware Collection and Analysis Using Statistical Classification of Executables</b> .....	279
<i>Roberto Perdisci, Andrea Lanzì, Wenke Lee</i>	
<b>MalTRAK: Tracking and Eliminating Unknown Malware</b> .....	289
<i>Amit Vasudevan</i>	
<b>Preventing Information Leaks through Shadow Executions</b> .....	300
<i>Roberto Capizzi, Antonio Longo, V.N. Venkatakrishnan, A. Prasad Sistla</i>	
<b>XSSDS: Server-Side Detection of Cross-Site Scripting Attacks</b> .....	310
<i>Martin Johns, Björn Engelmann, Joachim Posegga</i>	
<b>Anti-Phishing in Offense and Defense</b> .....	320
<i>Chuan Yue and Haining Wang</i>	
<b>OMOS: A Framework for Secure Communication in Mashup Applications</b> .....	330
<i>Saman Zarandioon, Danfeng (Daphne) Yao, Vinod Ganapathy</i>	
<b>Behavior-Profile Clustering for False Alert Reduction in Anomaly Detection Sensors</b> .....	340
<i>Vanessa Frias-Martinez, Salvatore J. Stolfo, Angelos D. Keromytis</i>	
<b>Bluetooth Network-Based Misuse Detection</b> .....	350
<i>Terrence OConnor Douglas Reeves</i>	
<b>Bridging the Gap between Data-Flow and Control-Flow Analysis for Anomaly Detection</b> .....	365
<i>Peng Li, Hyundo Park, Debin Gao, Jianming Fu</i>	
<b>Epilogue for RFC 1281, Guidelines for the Secure Operation of the Internet</b> .....	375
<i>Barbara Fraser, Steve Crocker</i>	
<b>The Evolution of System-Call Monitoring</b> .....	388
<i>Stephanie Forrest, Steven Hofmeyr, Anil Somayaji</i>	
<b>PAS: Predicate-Based Authentication Services Against Powerful Passive Adversaries</b> .....	401
<i>Xiaole Bai, Wenjun Gu, Sriram Chellappan, Xun Wang, Dong Xuan, Bin Ma</i>	

<b>pwdArmor: Protecting Conventional Password-Based Authentications</b> .....	411
<i>Timothy W. van der Horst, Kent E. Seamons</i>	
<b>DARE: A Framework for Dynamic Authentication of Remote Executions</b> .....	421
<i>Erdem Aktas and Kanad Ghose</i>	
<b>Instruction Set Extensions for Enhancing the Performance of Symmetric-Key Cryptography</b> .....	431
<i>Sean O'Melia, Adam J. Elbirt</i>	
<b>A Survey to Guide Group Key Protocol Development</b> .....	441
<i>Ahren Studer, Christina Johns, Jaanus Kase, Kyle O'Meara, Lorrie Cranor</i>	
<b>Transaction Oriented Text Messaging with Trusted-SMS</b> .....	451
<i>Antonio Grillo, Alessandro Lentini, Gianluigi Me, Giuseppe F. Italiano</i>	
<b>Author Index</b>	