

# 2010 IEEE Symposium on Security and Privacy (IEEE S&P)

## Table of Contents

Message from the General Chair .....	viii
Message from the Program Chairs .....	x
Organizing Committee .....	xi
Program Committee Members .....	xii
Additional Reviewers .....	xiii

### Special 30th Anniversary Invited Papers

Reflections on the 30th Anniversary of the IEEE Symposium on Security and Privacy .....	3
<i>Peter G. Neumann, Matt Bishop, Sean Peisert, and Marv Schaefer</i>	
History of US Government Investments in Cybersecurity Research: A Personal Perspective .....	14
<i>Carl E. Landwehr</i>	
Crossing the “Valley of Death”: Transitioning Research into Commercial Products: A Personal Perspective .....	21
<i>W. Douglas Maughan</i>	

### Session 1: Malware Analysis

<i>Inspector Gadget: Automated Extraction of Proprietary Gadgets from Malware Binaries</i> .....	29
<i>Clemens Kolbitsch, Thorsten Holz, Christopher Kruegel, and Engin Kirda</i>	
Synthesizing Near-Optimal Malware Specifications from Suspicious Behaviors .....	45
<i>Matt Fredrikson, Somesh Jha, Mihai Christodorescu, Reiner Sailer, and Xifeng Yan</i>	
Identifying Dormant Functionality in Malware Programs .....	61
<i>Paolo Milani Comparetti, Guido Salvaneschi, Engin Kirda, Clemens Kolbitsch, Christopher Kruegel, and Stefano Zanero</i>	

### Session 2: Information Flow

Reconciling Belief and Vulnerability in Information Flow .....	79
<i>Sardaouna Hamadou, Vladimiro Sassone, and Catuscia Palamidessi</i>	
Towards Static Flow-Based Declassification for Legacy and Untrusted Programs .....	93
<i>Bruno P. S. Rocha, Sruthi Bandhakavi, Jerry den Hartog, William H. Winsborough, and Sandro Etalle</i>	
Noninterference through Secure Multi-execution .....	109
<i>Dominique Devriese and Frank Piessens</i>	
Object Capabilities and Isolation of Untrusted Web Applications .....	125
<i>Sergio Maffei, John C. Mitchell, and Ankur Taly</i>	

## Session 3: Root of Trust

TrustVisor: Efficient TCB Reduction and Attestation.....	143
<i>Jonathan M. McCune, Yanlin Li, Ning Qu, Zongwei Zhou, Anupam Datta, Virgil Gligor, and Adrian Perrig</i>	
Overcoming an Untrusted Computing Base: Detecting and Removing Malicious Hardware Automatically.....	159
<i>Matthew Hicks, Murph Finnicum, Samuel T. King, Milo M. K. Martin, and Jonathan M. Smith</i>	
Tamper Evident Microprocessors.....	173
<i>Adam Waksman and Simha Sethumadhavan</i>	

## Session 4: Information Abuse

Side-Channel Leaks in Web Applications: A Reality Today, a Challenge Tomorrow.....	191
<i>Shuo Chen, Rui Wang, XiaoFeng Wang, and Kehuan Zhang</i>	
Investigation of Triangular Spamming: A Stealthy and Efficient Spamming Technique.....	207
<i>Zhiyun Qian, Z. Morley Mao, Yinglian Xie, and Fang Yu</i>	
A Practical Attack to De-anonymize Social Network Users .....	223
<i>Gilbert Wondracek, Thorsten Holz, Engin Kirda, and Christopher Kruegel</i>	
SCiFI - A System for Secure Face Identification .....	239
<i>Margarita Osadchy, Benny Pinkas, Ayman Jarrous, and Boaz Moskovich</i>	

## Session 5: Network Security

Round-Efficient Broadcast Authentication Protocols for Fixed Topology Classes.....	257
<i>Haowen Chan and Adrian Perrig</i>	
Revocation Systems with Very Small Private Keys .....	273
<i>Allison Lewko, Amit Sahai, and Brent Waters</i>	
Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures .....	286
<i>Yao Liu, Peng Ning, and Huaiyu Dai</i>	

## Session 6: Systematization of Knowledge I

Outside the Closed World: On Using Machine Learning for Network Intrusion Detection.....	305
<i>Robin Sommer and Vern Paxson</i>	
All You Ever Wanted to Know about Dynamic Taint Analysis and Forward Symbolic Execution (but Might Have Been Afraid to Ask) .....	317
<i>Edward J. Schwartz, Thanassis Avgerinos, and David Brumley</i>	
State of the Art: Automated Black-Box Web Application Vulnerability Testing .....	332
<i>Jason Bau, Elie Bursztein, Divij Gupta, and John Mitchell</i>	

## Session 7: Secure Systems

A Proof-Carrying File System .....	349
<i>Deepak Garg and Frank Pfenning</i>	
Scalable Parametric Verification of Secure Systems: How to Verify Reference Monitors without Worrying about Data Structure Size.....	365
<i>Jason Franklin, Sagar Chaki, Anupam Datta, and Arvind Seshadri</i>	
HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity .....	380
<i>Zhi Wang and Xuxian Jiang</i>	

## Session 8: Systematization of Knowledge II

How Good Are Humans at Solving CAPTCHAs? A Large Scale Evaluation .....	399
<i>Elie Bursztein, Steven Bethard, Celine Fabry, John C. Mitchell, and Dan Jurafsky</i>	
Bootstrapping Trust in Commodity Computers.....	414
<i>Bryan Parno, Jonathan M. McCune, and Adrian Perrig</i>	

## Session 9: Analyzing Deployed Systems

Chip and PIN is Broken.....	433
<i>Steven J. Murdoch, Saar Drimer, Ross Anderson, and Mike Bond</i>	
Experimental Security Analysis of a Modern Automobile .....	447
<i>Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage</i>	
On the Incoherencies in Web Browser Access Control Policies .....	463
<i>Kapil Singh, Alexander Moshchuk, Helen J. Wang, and Wenke Lee</i>	

## Session 10: Language-Based Security

CONSCRIPT: Specifying and Enforcing Fine-Grained Security Policies for JavaScript in the Browser.....	481
<i>Leo A. Meyerovich and Benjamin Livshits</i>	
TaintScope: A Checksum-Aware Directed Fuzzing Tool for Automatic Software Vulnerability Detection .....	497
<i>Tielei Wang, Tao Wei, Guofei Gu, and Wei Zou</i>	
A Symbolic Execution Framework for JavaScript .....	513
<i>Prateek Saxena, Devdatta Akhawe, Steve Hanna, Feng Mao, Stephen McCamant, and Dawn Song</i>	

Author Index .....	529
--------------------	-----