

# **2014 IEEE Symposium on Security and Privacy**

**(SP 2014)**

**San Jose, California, USA  
18-21 May 2014**



**IEEE Catalog Number: CFP14020-POD  
ISBN: 978-1-4799-4685-3**

# 2014 IEEE Symposium on Security and Privacy

## SP 2014

### Table of Contents

Message from the General Chair.....	x
Message from the Program Chairs.....	xiã
Program Committee.....	xiiã

---

#### Session 1: Attacks 1

Hunting the Red Fox Online: Understanding and Detection of Mass Redirect-Script Injections .....	3
<i>Zhou Li, Sumayah Alrwais, XiaoFeng Wang, and Eihal Alowaisheq</i>	
Stealing Webpages Rendered on Your Browser by Exploiting GPU Vulnerabilities .....	19
<i>Sangho Lee, Youngsok Kim, Jangwoo Kim, and Jong Kim</i>	
All Your Screens Are Belong to Us: Attacks Exploiting the HTML5 Screen Sharing API .....	34
<i>Yuan Tian, Ying-Chuan Liu, Amar Bhosale, Lin-Shung Huang, Patrick Tague, and Collin Jackson</i>	
Chip and Skim: Cloning EMV Cards with the Pre-play Attack .....	49
<i>Mike Bond, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov, and Ross Anderson</i>	

#### Session 2: SSL/TLS

When HTTPS Meets CDN: A Case of Authentication in Delegated Service .....	67
<i>Jinjin Liang, Jian Jiang, Haixin Duan, Kang Li, Tao Wan, and Jianping Wu</i>	
Analyzing Forged SSL Certificates in the Wild .....	83
<i>Lin-Shung Huang, Alex Rice, Erling Ellingsen, and Collin Jackson</i>	
Triple Handshakes and Cookie Cutters: Breaking and Fixing Authentication over TLS .....	98
<i>Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Alfredo Pironti, and Pierre-Yves Strub</i>	

Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations .....	114
<i>Chad Brubaker, Suman Jana, Baishakhi Ray, Sarfraz Khurshid, and Vitaly Shmatikov</i>	

### **Session 3: Automation**

Automating Isolation and Least Privilege in Web Services .....	133
<i>Aaron Blankstein and Michael J. Freedman</i>	
Hidden GEMs: Automated Discovery of Access Control Vulnerabilities in Graphical User Interfaces .....	149
<i>Collin Mulliner, William Robertson, and Engin Kirda</i>	
Automated Analysis of Security Protocols with Global State .....	163
<i>Steve Kremer and Robert Künnemann</i>	
Automated Verification of Group Key Agreement Protocols .....	179
<i>Benedikt Schmidt, Ralf Sasse, Cas Cremers, and David Basin</i>	

### **Session 4: Attacks 2**

Practical Evasion of a Learning-Based Classifier: A Case Study .....	197
<i>Nedim Šrndić and Pavel Laskov</i>	
Doppelgänger Finder: Taking Stylometry to the Underground .....	212
<i>Sadia Afroz, Aylin Caliskan-Islam, Ariel Stolerman, Rachel Greenstadt, and Damon McCoy</i>	
Hacking Blind .....	227
<i>Andrea Bittau, Adam Belay, Ali Mashtizadeh, David Mazières, and Dan Boneh</i>	
Framing Signals - A Return to Portable Shellcode .....	243
<i>Erik Bosman and Herbert Bos</i>	

### **Session 5: Systems Security**

Pivot: Fast, Synchronous Mashup Isolation Using Generator Chains .....	261
<i>James Mickens</i>	
SoK: Automated Software Diversity .....	276
<i>Per Larsen, Andrei Homescu, Stefan Brunthaler, and Michael Franz</i>	
KCoFI: Complete Control-Flow Integrity for Commodity Operating System Kernels .....	292
<i>John Criswell, Nathan Dautenhahn, and Vikram Adve</i>	
Dancing with Giants: Wimpy Kernels for On-Demand Isolated I/O .....	308
<i>Zongwei Zhou, Miao Yu, and Virgil D. Gligor</i>	

## Session 6: Privacy and Anonymity

Bootstrapping Privacy Compliance in Big Data Systems .....	327
<i>Shayak Sen, Saikat Guha, Anupam Datta, Sriram K. Rajamani, Janice Tsai, and Jeannette M. Wing</i>	
Formal Analysis of Chaumian Mix Nets with Randomized Partial Checking .....	343
<i>Ralf Küsters, Tomasz Truderung, and Andreas Vogt</i>	
Blind Seer: A Scalable Private DBMS .....	359
<i>Vasilis Pappas, Fernando Krell, Binh Vo, Vladimir Kolesnikov, Tal Malkin, Seung Geol Choi, Wesley George, Angelos Keromytis, and Steve Bellovin</i>	
ANONIZE: A Large-Scale Anonymous Survey System .....	375
<i>Susan Hohenberger, Steven Myers, Rafael Pass, and abhi shelat</i>	

## Session 7: Android

Upgrading Your Android, Elevating My Malware: Privilege Escalation through Mobile OS Updating .....	393
<i>Luyi Xing, Xiaorui Pan, Rui Wang, Kan Yuan, and XiaoFeng Wang</i>	
The Peril of Fragmentation: Security Hazards in Android Device Driver Customizations .....	409
<i>Xiaoyong Zhou, Yeonjoon Lee, Nan Zhang, Muhammad Naveed, and XiaoFeng Wang</i>	
From Zygote to Morula: Fortifying Weakened ASLR on Android .....	424
<i>Byoungyoung Lee, Long Lu, Tielei Wang, Taesoo Kim, and Wenke Lee</i>	

## Session 8: E-Cash

Secure Multiparty Computations on Bitcoin .....	443
<i>Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek</i>	
Zerocash: Decentralized Anonymous Payments from Bitcoin .....	459
<i>Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza</i>	
Permacoin: Repurposing Bitcoin Work for Data Preservation .....	475
<i>Andrew Miller, Ari Juels, Elaine Shi, Bryan Parno, and Jonathan Katz</i>	

## Session 8: Miscellaneous

Cloak and Swagger: Understanding Data Sensitivity through the Lens of User Anonymity .....	493
<i>Sai Teja Peddinti, Aleksandra Korolova, Elie Bursztein, and Geetanjali Sampemane</i>	
Stopping a Rapid Tornado with a Puff .....	509
<i>José Lopes and Nuno Neves</i>	
SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks .....	524
<i>Michael Rushanan, Aviel D. Rubin, Denis Foo Kune, and Colleen M. Swanson</i>	
Quantifying Information Flow for Dynamic Secrets .....	540
<i>Piotr Mardziel, Mario S. Alvim, Michael Hicks, and Michael R. Clarkson</i>	

## Session 9: Attacks 3

Not-So-Random Numbers in Virtualized Linux and the Whirlwind RNG .....	559
<i>Adam Everspaugh, Yan Zhai, Robert Jellinek, Thomas Ristenpart, and Michael Swift</i>	
Out of Control: Overcoming Control-Flow Integrity .....	575
<i>Enes Göktaş, Elias Athanasopoulos, Herbert Bos, and Georgios Portokalidis</i>	
Modeling and Discovering Vulnerabilities with Code Property Graphs .....	590
<i>Fabian Yamaguchi, Nico Golde, Daniel Arp, and Konrad Rieck</i>	
SoK: Introspections on Trust and the Semantic Gap .....	605
<i>Bhushan Jain, Mirza Basim Baig, Dongli Zhang, Donald E. Porter, and Radu Sion</i>	

## Session 10: Secure Computation and Storage

Automating Efficient RAM-Model Secure Computation .....	623
<i>Chang Liu, Yan Huang, Elaine Shi, Jonathan Katz, and Michael Hicks</i>	
Dynamic Searchable Encryption via Blind Storage .....	639
<i>Muhammad Naveed, Manoj Prabhakaran, and Carl A. Gunter</i>	
Wysteria: A Programming Language for Generic, Mixed-Mode Multiparty Computations .....	655
<i>Aseem Rastogi, Matthew A. Hammer, and Michael Hicks</i>	

## Session 11: Authentication

An Expressive Model for the Web Infrastructure: Definition and Application to the Browser ID SSO System .....	673
<i>Daniel Fett, Ralf Küsters, and Guido Schmitz</i>	
A Study of Probabilistic Password Models .....	689
<i>Jerry Ma, Weining Yang, Min Luo, and Ninghui Li</i>	

ZEBRA: Zero-Effort Bilateral Recurring Authentication .....705  
*Shrirang Mare, Andrés Molina-Markham, Cory Cornelius, Ronald Peterson,  
and David Kotz*

**Author Index** .....721