February 26 – March 1, 2017

24th Annual Network and Distributed System Security Symposium

Catamaran Resort Hotel and Spa

San Diego, California

PROGRAM

Sunday, February 26

8:30 AM – 6:00 PM	**Useable Security Workshop**	Macaw
9:00 AM – 5:30 PM	**DNS Privacy Workshop**	Toucan
6:00 PM – 7:00 PM	**Welcome Reception**	The Boardroom & Foyer

Monday, February 27

7:30 AM – 9:00 AM	**Continental Breakfast**	Kon Tiki Ballroom Foyer
9:00 AM – 9:20 AM	**Welcome and Opening Remarks**	Kon Tiki Ballroom
9:20 AM – 10:20 AM	**Keynote: Recount 2016: A Security Audit of the Presidential Election** J. Alex Halderman, Professor of Computer Science and Engineering, University of Michigan and Director of Michigan's Center for Computer Security and Society	
10:20 AM – 10:45 AM	**Break**	Kon Tiki Ballroom Foyer

Special thanks to our sponsors

Baidu 百度 · Cisco · Afilias · Check Point Software Technologies Ltd. · Qualcomm · salesforce · NSF · Internet Society

10:45 AM – 12:25 PM **Session 1: Applied Crypto and Cryptocurrencies** Kon Tiki Ballroom

Session Chair: Nadia Heninger

IO-DSSE: Scaling Dynamic Searchable Encryption to Millions of Indexes By Improving Locality

Ian Miers, Payman Mohassel

ObliviSync: Practical Oblivious File Backup and Synchronization

Adam J. Aviv, Seung Geol Choi, Travis Mayberry, Daniel S. Roche

TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub

Ethan Heilman, Leen Alshenibr, Foteini Baldimtsi, Alessandra Scafuro, Sharon Goldberg

P2P Mixing and Unlinkable Bitcoin Transactions

Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate

SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks

Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei

12:25 PM – 2:00 PM **Lunch** North Beach

2:00 PM – 3:20 PM **Session 2A: Virtualization and SDN** Kon Tiki Ballroom

Session Chair: Juan Caballero

DELTA: A Security Assessment Framework for Software-Defined Networks

Seungsoo Lee, Changhoon Yoon, Chanhee Lee, Seungwon Shin, Vinod Yegneswaran, Phillip Porras

PSI: Precise Security Instrumentation for Enterprise Networks

Tianlong Yu, Seyed K. Fayaz, Michael Collins, Vyas Sekar, Srinivasan Seshan

On the Safety and Efficiency of Virtual Firewall Elasticity Control

Juan Deng, Hongda Li, Hongxin Hu, Kuang-Ching Wang, Gail-Joon Ahn, Ziming Zhao, Wonkyu Han

Special thanks to our sponsors

Deconstructing Xen

Lei Shi, Yuming Wu, Yubin Xia, Nathan Dautenhahn, Haibo Chen, Binyu Zang, Haibing Guan, Jinming Li

Session 2B: Web Security Aviary Ballroom

Session Chair: David Choffnes

Though Shalt Not Depend on Me: Analysing the Use of Outdated JavaScript Libraries on the Web

Tobias Lauinger, Abdelberi Chaabane, Sajjad Arshad, William Robertson, Christo Wilson, Engin Kirda

Enabling Reconstruction of Attacks on Users via Efficient Browsing Snapshots

Jienan Liu, Bo Li, Babak Rahbarinia, Kyu Hyung Lee, Roberto Perdisci

(Cross-)Browser Fingerprinting via OS and Hardware Level Features

Yinzhi Cao, Song Li, Erik Wijmans

Fake Co-visitation Injection Attacks to Recommender Systems

Guolei Yang, Neil Zhenqiang Gong, Ying Cai

3:20 PM – 3:50 PM **Break** Kon Tiki Ballroom Foyer

3:50 PM – 5:30 PM **Session 3A: User Authentication** Kon Tiki Ballroom

Session Chair: Srdjan Capkun

Broken Hearted: How to Attack ECG Biometrics

Simon Eberz, Nicola Paoletti, Marc Roeschlin, Andrea Patané, Marta Kwiatkowska, Ivan Martinovic

Towards Implicit Visual Memory-Based Authentication

Claude Castelluccia, Markus Dürmuth, Maximilian Golla, Fatma Imamoglu

KEH-Gait: Towards a Mobile Healthcare User Authentication System by Kinetic Energy Harvesting

Weita Xu, Guohao Lan, Qi Lin, Sara Khalifa, Neil Bergmann, Mahbub Hassan, Wen Hu

A Large-scale Analysis of the Mnemonic Password Advice

Johannes Kiesel, Benno Stein, Stefan Lucks

Cracking Android Pattern Lock in Five Attempts

Guixin Ye, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Kwang In Kim, Ben Taylor, Zheng Wang

Session 3B: Malware Aviary Ballroom

Session Chair: Marcus Peinado

Dial One for Scam: A Large-Scale Analysis of Technical Support Scams

Najmeh Miramirkhani, Oleksii Starov, Nick Nikiforakis

Automated Synthesis of Semantic Malware Signatures using Maximum Satisfiability

Yu Feng, Osbert Bastani, Ruben Martins, Isil Dillig, Saswat Anand

MaMaDroid: Detecting Android Malware by Building Markov Chains of Behavioral Models

Enrico Mariconti, Lucky Onwuzurike, Panagiotis Andriotis, Emiliano De Cristofaro, Gordon Ross, Gianluca Stringhini

A Broad View of the Ecosystem of Socially Engineered Exploit Documents

Stevens Le Blond, Cedric Gilbert, Utkarsh Upadhyay, Manuel Gomez Rodriguez, David Choffnes

Catching Worms, Trojan Horses and PUPs: Unsupervised Detection of Silent Delivery Campaigns

Bum Jun Kwon, Virinchi Srinivas, Amol Deshpande, Tudor Dumitras

7:00 PM – 9:00 PM **Poster Reception** The Boardroom & Foyer

Tuesday, February 28

7:30 AM – 9:00 AM **Continental Breakfast** Kon Tiki Ballroom Foyer

9:00 AM – 10:20 AM **Session 4A: TLS et al.** Kon Tiki Ballroom

Session Chair: Johanna Amann

Measuring Small Subgroup Attacks Against Diffie-Hellman

Luke Valenta, David Adrian, Antonio Sanso, Shaanan Cohney, Joshua Fried, Marcella Hastings, J. Alex Halderman, Nadia Heninger

Indiscreet Logs: Persistent Diffie-Hellman Backdoors in TLS

Kristen Dorey, Nicholas Chang-Fong, Aleksander Essex

WireGuard: Next Generation Kernel Network Tunnel

Jason A. Donenfeld

The Security Impact of HTTPS Interception

Zakir Durumeric, Zane Ma, Drew Springall, Richard Barnes, Nick Sullivan, Elie Bursztein, Michael Bailey, J. Alex Halderman, Vern Paxson

Session 4B: Secure Computation Aviary Ballroom

Session Chair: Patrick Traynor

Fast Actively Secure OT Extension for Short Secrets

Arpita Patra, Pratik Sarkar, Ajith Suresh

Constant Round Maliciously Secure 2PC with Function-Independent Preprocessing Using LEGO

Jesper Buus Nielsen, Thomas Schneider, Roberto Trifiletti

Pushing the Communication Barrier in Secure Computation Using Lookup Tables

Ghada Dessouky, Farinaz Koushanfar, Ahmad-Reza Sadeghi, Thomas Schneider, Shaza Zeitouni, Michael Zohner

Using Fully Homomorphic Encryption for Statistical Analysis of Categorical, Ordinal and Numerical Data

Wen-jie Lu, Shohei Kawasaki, Jun Sakuma

10:20 AM – 10:45 AM **Break** Kon Tiki Ballroom Foyer

10:45 AM – 12:25 PM **Session 5A: Mobile Privacy and Security** Kon Tiki Ballroom

Session Chair: Manuel Egele

Dark Hazard: Learning-based, Large-Scale Discovery of Hidden Sensitive Operations in Android Apps

Xiaorui Pan, Xueqiang Wang, Yue Duan, XiaoFeng Wang, Heng Yi

Show Me the Money! Finding Flawed Implementations of Third-party In-app Payment in Android Apps

Wenbo Yang, Yuanyuan Zhang, Juanru Li, Hui Liu, Qing Wang, Yueheng Zhange, Dawu Gu

WindowGuard: Systematic Protection of GUI Security in Android

Chuangang Ren, Peng Liu, Sencun Zhu

Obfuscation-Resilient Privacy Leak Detection for Mobile Apps Through Differential Analysis

Andrea Continella, Yanick Fratantonio, Martina Lindorfer, Alessandro Puccetti, Ali Zand, Christopher Kruegel, Giovanni Vigna

Automated Analysis of Privacy Requirements for Mobile Apps

Sebastian Zimmeck, Ziqi Wang, Lieyong Zou, Roger Iyengar, Bin Liu, Florian Schaub, Shomir Wilson, Norman Sadeh, Steven M. Bellowin, Joel Reidenberg

Session 5B: Software and System Security (Part I) Aviary Ballroom

Session Chair: Ethan Heilman

Dachshund: Digging for and Securing (Non-)Blinded Constants in JIT Code

Giorgi Maisuradze, Michael Backes, Christian Rossow

SafeInit: Comprehensive and Practical Mitigation of Uninitialized Read Vulnerabilities

Alyssa Milburn, Herber Bos, Cristiano Giuffrida

MARX: Uncovering Class Hierarchies in C++ Programs

Andrew Pawlowski, Moritz Contag, Victor van der Veen, Chris Ouwehand, Thorsten Holz, Herbert Bos, Elias Athanasopoulos, Cristiano Giuffrida

PT-Rand: Practical Mitigation of Data-only Attacks Against Page Tables

Lucas Davi, David Gens, Christopher Liebchen, Ahmad-Reza Sadeghi

Dynamic Virtual Address Range Adjustment for Intra-Level Privilege Separation on ARM

Yeongpil Cho, Donghyun Kwon, Hayoon Yi, Yunheung Paek

12:25 PM – 2:00 PM **Lunch** North Beach

2:00 PM – 3:20 PM **Session 6A: Cloud and Potpourri** Kon Tiki Ballroom

Session Chair: Adam Bates

Hello From the Other Side: SSH over Robust Cache Covert Channels in the Cloud

Clémentine Maurice, Manuel Weber, Michael Schwarz, Lukas Giner, Daniel Gruss, Carlo Alberto Boano, Stefan Mangard, Kay Römer

Dynamic Differential Location Privacy with Personalized Error Bounds

Lei Yu, Ling Liu, Calton Pu

Are We There Yet? On RPKI's Deployment and Security

Yossi Gilad, Avichai Cohen, Amir Herzberg, Michael Schapira, Haya Shulman

TenantGuard: Scalable Runtime Verification of Cloud-Wide VM-Level Network Isolation

Yushun Wang, Taous Madi, Suryadipta Majumdar, Yosr Jarray, Amir Alimohammadifar, Makan Pourzandi, Lingyu Wang, Mourad Debbabi

Session 6B: Tor Aviary Ballroom

Session Chair: Prateek Mittal

Dissecting Tor Bridges: A Security Evaluation of their Private and Public Infrastructures

Srdjan Matic, Carmela Troncoso, Juan Caballero

The Effect of DNS on Tor's Anonymity

Benjamin Greschbach, Tobias Pulls, Laura M. Roberts, Philipp Winter, Nick Feamster

Avoiding The Man on the Wire: Improving Tor's Security with Trust-Aware Path Selection

Aaron Johnson, Rob Jansen, Aaron D. Jaggard, Joan Feigenbaum, Paul Syverson

HisTorε: Differentially Private and Robust Statistics Collection for Tor

Akshaya Mani, Micah Sherr

3:20 PM – 3:50 PM **Break** Kon Tiki Ballroom Foyer

3:50 PM – 5:30 PM **Session 7: Trusted Execution Environments** Kon Tiki Ballroom

Session Chair: Amir Herzberg

SGX-Shield: Enabling Address Space Layout Randomization for SGX Programs

Jaebaek Seo, Byoungyoung Lee, Seongmin Kim, Ming-Wei Shih, Insik Shin, Dongsu Han, Taesoo Kim

T-SGX: Eradicating Controlled-Channel Attacks Against Enclave Programs

Ming-Wei Shih, Sangho Lee, Taesoo Kim, Marcus Peinado

BOOMERANG: Exploiting the Semantic Gap in Trusted Execution Environments

Aravind Machiry, Eric Gustafson, Chad Spensky, Christopher Salls, Nick Stephens, Ruoyu Wang, Antonio Bianchi, Yung Ryn Choe, Christopher Kruegel, Giovanni Vigna

HOP: Hardware Makes Obfuscation Practical

Kartik Nayak, Christopher W. Fletcher, Ling Ren, Nishanth Chandran, Satya Lokam, Elaine Shi, Vipul Goyal

Panoply: Low-TCB Linux Applications With SGX Enclaves

Shweta Shinde, Dat Le Tien, Shruti Tople, Prateek Saxena

7:00 PM – 9:00 PM **Symposium Dinner** Aviary Ballroom

Wednesday, March 1

7:30 AM – 9:00 AM **Continental Breakfast** Kon Tiki Ballroom Foyer

9:00 AM – 9:20 AM **Awards and Acknowledgements** Kon Tiki Ballroom

9:20 AM – 10:20 AM **Keynote: Securing the Ecosystem - Collaborating Inside and Out**
Trent Adams, Information Security Director, PayPal

10:20 AM – 10:45 AM **Break** Kon Tiki Ballroom Foyer

10:45 AM – 12:25 PM **Session 8: Cyberphysical Security** Kon Tiki Ballroom

Session Chair: Dongyan Xu

Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit

Luis Garcia, Ferdinand Brasser, Mehmet H. Cintuglu, Ahmad-Reza Sadeghi, Osama Mohammed, Saman A. Zonouz

ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms

Yunhan Jack Jia, Qi Alfred Chen, Shiqi Wang, Amir Rahmati, Earlence Fernandes, Z. Morley Mao, Atul Prakash

FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild

Zhenhua Li, Weiwei Wang, Christo Wilson, Jian Chen, Chen Qian, Taeho Jung, Lan Zhang, Kebin Liu, Xiangyang Li, Yunhao Liu

Internet-scale Probing of CPS: Inference, Characterization and Orchestration Analysis

Claude Fachkha, Elias Bou-Harb, Anastasis Keliris, Nasir Memon, Mustaque Ahamad

Wi-Fly?: Detecting Privacy Invasion Attacks by Consumer Drones

Simon Birnbach, Richard Baker, Ivan Martinovic

12:25 PM – 2:00 PM **Lunch** North Beach

2:00 PM – 3:20 PM **Session 9: Attacks** Kon Tiki Ballroom

Session Chair: Will Robertson

ASLR^Cache: Practical Cache Attacks on the MMU

Ben Gras, Kaveh Razavi, Erik Bosman, Herbert Box, Cristiano Giuffrida

Unleashing Use-Before-Initialization Vulnerabilities in the Linux Kernel Using Targeted Stack Spraying

Kangjie Lu, Marie-Therese Walter, David Pfaff, Stefan Nürnberger, Wenke Lee, Michael Backes

Address Oblivious Code Reuse: On the Effectiveness of Leakage Resilient Diversity

Robert Rudd, Richard Skowyra, David Bigelow, Veer Dedhia, Thomas Hobson, Stephen Crane, Christopher Liebchen, Per Larsen, Lucas Davi, Michael Franz, Ahmad-Reza Sadeghi, Hamed Okhravi

An Evil Copy: How the Loader Betrays You

Xinyang Ge, Mathias Payer, Trent Jaeger

3:20 PM – 3:50 PM **Break** Kon Tiki Ballroom Foyer

3:50 PM – 5:30 PM **Session 10: Software and System Security (Part II)** Kon Tiki Ballroom

Session Chair: Trent Jaeger

Stack Object Protection with Low Fat Pointers

Gregory J. Duck, Roland H. C. Yap, Lorenzo Cavallaro

VUzzer: Application-aware Evolutionary Fuzzing

Sanjay Rawat, Vivek Jain, Ashish Kumar, Lucian Cojocar, Cristiano Giuffrida, Herbert Bos

Self Destructing Exploit Executions via Input Perturbation

Yonghwi Kwon, Brendan Saltaformaggio, I Luk Kim, Kyu Hyung Lee, Xiangyu Zhang, Dongyan Xu

A Call to ARMs: Understanding the Costs and Benefits of JIT Spraying Mitigations

Wilson Lian, Hovav Shacham, Stefan Savage

Ramblr: Making Reassembly Great Again

Ruoyu Wang, Yan Shoshitaishvili, Antonio Bianchi, Aravind Machiry, John Grosen, Paul Grosen, Christopher Kruegel, Giovanni Vigna

5:30 PM – 5:40 PM **Closing Remarks** Kon Tiki Ballroom