ACM CCS 2015

22nd ACM Conference on Computer and Communications Security

The Denver Marriot City Center, Denver, Colorado, US

October 12-16, 2015

Home Announcements ▾ Organization ▾ Program/Reg. ▾ Workshops ▾ Information ▾

Accepted Papers

- **Automating Fast and Secure Translations from Type-I to Type-III Pairing Schemes**
  Joseph A. Akinyele (Johns Hopkins Univ.); Christina Garman (Johns Hopkins Univ.); Susan Hohenberger (Johns Hopkins Univ.)

- **Group Signatures with Probabilistic Revocation: A Computationally-Scalable Approach for Providing Privacy-Preserving Authentication**
  Vireshwar Kumar (Virginia Tech); He Li (Virginia Tech); Jung-Min (Jerry) Park (Virginia Tech); Kaigui Bian (Peking Univ.); Yaling Yang (Virginia Tech)

- **Face/Off: Preventing Privacy Leakage From Photos in Social Networks**
  Panagiotis Ilia (FORTH); Iasonas Polakis (Columbia Univ.); Elias Athanasopoulos (FORTH); Federico Maggi (Politecnico di Milano); Sotiris Ioannidis (FORTH)

- **VCCFinder: Finding Potential Vulnerabilities in Open-Source Projects to Assist Code Audits**
  Henning Perl (Fraunhofer FKIE); Daniel Arp (Universität Göttingen); Sergej Dechand (Universität Bonn); Fabian Yamaguchi (Universität Göttingen); Sascha Fahl (Fraunhofer FKIE); Yasemin Acar (Universität Hannover); Konrad Rieck (Universität Göttingen); Matthew Smith (Universität Bonn)

- **Where's Wally? Precise User Discovery Attacks in Location Proximity Services**
  Iasonas Polakis (Columbia Univ.); George Argyros (Columbia Univ.); Theofilos Petsios (Columbia Univ.); Suphannee Sivakorn (Columbia Univ.); Angelos D. Keromytis (Columbia Univ.)

- **From System Services Freezing to System Server Shutdown in Android: All You Need Is a Loop in an Application**
  Heqing Huang (The Pennsylvania State Univ.); Sencun Zhu (The Pennsylvania State Univ.); Kai Chen (Chinese Academy of Sciences); Peng Liu (The Pennsylvania State Univ.)

- **Security by Any Other Name: On the Effectiveness of Provider Based Email Security**
  Ian Foster (Univ. of California, San Diego); Jon Larson (Univ. of California, San Diego); Max Masich (Univ. of California, San Diego); Alex C. Snoeren (Univ. of California, San Diego); Stefan Savage (Univ. of California, San Diego); Kirill Levchenko (Univ. of California, San Diego)

- **Moat: Verifying Confidentiality of Enclave Programs**

Latest Updates

- **10-08-2015:** CCS 2015 Proceedings OpenTOC
- **10-07-2015:** Public Transportation in Denver (CCS 2015 Hotel is on Light Rail's D, F and H line, and served by RTD bus routes 38 and 44)
- **10-07-2015:** Denver International Airport (Shared-Ride Services)
- **10-07-2015:** Parking Information (On a map)
- **10-07-2015:** Weather Forecast
- **10-07-2015:** Restaurants
- **09-06-2015:**Keynote Speakers Updated
- **08-30-2015:** Agenda Updated
- **08-15-2015:**Accepted Papers Updated
- **08-03-2015:**Tutorials Updated
- **08-02-2015:**Now accepting applications for student travel award, deadline August 17, 2015
- **08-01-2015:**Registration is now open. Early bird registration ends September 20, 2015
- **07-30-2015:** Registration will be made available on August 1.
- **04-23-2015:** CCS paper submission site is up.
- **03-27-2015:** Accepted Workshops posted.
- **01-10-2015:** CCS 2015 web site is up.

Contact Information

Web Related Matters:

Rohit Sinha (Univ. of California, Berkeley); Sriram Rajamani (Microsoft Research); Sanjit Seshia (Univ. of California, Berkeley); Kapil Vaswani (Microsoft Research)

- **Cracking App Isolation on Apple: Unauthorized Cross-App Resource Access on MAC OS X and iOS**
  Luyi Xing (Indiana Univ. Bloomington); Xiaolong Bai (Indiana Univ. Bloomington & Tsinghua Univ.); Tongxin Li (Peking Univ.); XiaoFeng Wang (Indiana Univ. Bloomington); Kai Chen (Indiana Univ. Bloomington & Chinese Academy of Sciences); Xiaojing Liao (Georgia Institute of Technology); Shi-Min Hu (Tsinghua Univ.); Xinhui Han (Peking Univ.)

- **Differential Privacy with Bounded Priors: Reconciling Utility and Privacy in Genome-Wide Association Studies**
  Florian Tramèr (EPFL); Zhicong Huang (EPFL); Erman Ayday (Bilkent Univ.); Jean-Pierre Hubaux (EPFL)

- **Clean Application Compartmentalization with SOAAP**
  Khilan Gudka (Univ. of Cambridge); Robert N.M. Watson (Univ. of Cambridge); Jonathan Anderson (Memorial Univ.); David Chisnall (Univ. of Cambridge); Brooks Davis (SRI International); Ben Laurie (Google UK Ltd.); Ilias Marinos (Univ. of Cambridge); Peter G. Neumann (SRI International); Alex Richardson (Univ. of Cambridge)

- **Seeing Your Face Is Not Enough: An Inertial Sensor-Based Liveness Detection for Face Authentication**
  Yan LI (Singapore Management Univ.); Yingjiu LI (Singapore Management Univ.); Qiang YAN (Singapore Management Univ.); Hancong KONG (Singapore Management Univ.); Robert H. DENG (Singapore Management Univ.)

- **GCM-SIV: Full Nonce Misuse-Resistant Authenticated Encryption at Under One Cycle per Byte**
  Shay Gueron (Univ. of Haifa); Yehuda Lindell (Bar-Ilan Univ.)

- **Sunlight: Fine-grained Targeting Detection at Scale with Statistical Confidence**
  Mathias Lecuyer (Columbia Univ.); Riley Spahn (Columbia Univ.); Yannis Spiliopoulos (Columbia Univ.); Augustin Chaintreau (Columbia Univ.); Roxana Geambasu (Columbia Univ.); Daniel Hsu (Columbia Univ.)

- **Defeating IMSI Catchers**
  Fabian van den Broek (Radboud Univ. Nijmegen); Roel Verdult (Radboud Univ. Nijmegen); Joeri de Ruiter (Univ. of Birmingham)

- **Deniable Key Exchanges for Secure Messaging**
  Nik Unger (Univ. of Waterloo); Ian Goldberg (Univ. of Waterloo)

- **LOOP: Logic-Oriented Opaque Predicate Detection in Obfuscated Binary Code**
  Jiang Ming (The Pennsylvania State Univ.); Dongpeng Xu (The Pennsylvania State Univ.); Li Wang (The Pennsylvania State Univ.); Dinghao Wu (The Pennsylvania State Univ.)

- **Insecurity of Voice Solution VoLTE in LTE Mobile Networks**
  Chi-Yu Li (UCLA); Guan-Hua Tu (UCLA); Chunyi Peng (OSU); Zengwen Yuan (UCLA); Yuanjie Li (UCLA); Songwu Lu (UCLA); Xinbing Wang (Shanghai Jiao Tong Univ.)

- **Fast Garbling of Circuits Under Standard Assumptions**
  Shay Gueron (Univ. of Haifa and Intel); Yehuda Lindell (Bar Ilan Univ.); Ariel Nof (Bar Ilan Univ.); Benny Pinkas (Bar Ilan Univ.)

- **Drops for Stuff: An Analysis of Reshipping Mule Scams**
  Shuang Hao (UC Santa Barbara); Kevin Borgolte (UC Santa Barbara); Nick Nikiforakis (Stony Brook University); Gianluca Stringhini (University College London); Manuel Egele (Boston University); Michael Eubanks (Federal Bureau of Investigation); Brian Krebs (KrebsOnSecurity.com); Giovanni Vigna (UC Santa Barbara & Lastline Inc.)

- **Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions**
  Andrew Miller (Univ. of Maryland); Ahmed Kosba (Univ. of Maryland); Elaine Shi (Cornell Univ.);

Web Chairs Chuan Yue and Stacy Karas at: ccs2015web at gmail dot com

Visa Related:
Refer to the visa page

Other Matters:
Corresponding committees and members (Organization Tab)

Jonathan Katz (Univ. of Maryland)

- **Surpass: System-initiated user-replaceable passwords**
  Jun Ho Huh (Honeywell ACS Labs); Seongyeol Oh (Sungkyunkwan Univ.); Hyoungshick Kim (Sungkyunkwan Univ.); Konstantin Beznosov (Univ. of British Columbia); Apurva Mohan (Honeywell ACS Labs); Raj Rajagopalan (Honeywell ACS Labs)

- **Secure Deduplication of Encrypted Data without Additional Independent Servers**
  Jian Liu (Aalto Univ.); N. Asokan (Aalto Univ. and Univ. of Helsinki); Benny Pinkas (Bar Ilan Univ.);

- **Using Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data**
  Dario Catalano (Univ. of Catania); Dario Fiore (IMDEA Software Institute)

- **From Facepalm to Brain Bender: Exploring Client-Side Cross-Site Scripting**
  Ben Stock (FAU Erlangen-Nuremberg); Stephan Pfistner (SAP SE); Bernd Kaiser (FAU Erlangen-Nuremberg); Sebastian Lekies (Ruhr-Univ. Bochum); Martin Johns (SAP SE)

- **Leakage-Resilient Authentication and Encryption from Symmetric Cryptographic Primitives**
  Olivier Pereira (Universite catholique de Louvain); Francois-Xavier Standaert (Universite catholique de Louvain); Srinivas Vivek (Univ. of Luxembourg & Univ. of Bristol)

- **CoDisasm : Medium scale concatic disassembly of self-modifying binaries with overlapping instructions**
  Guillaume Bonfante (Universitè de Lorraine); Josè Fernandez (Ecole Politechnique, Canada); Jean-Yves Marion (Universitè de Lorraine); Rouxel (Universitè de Lorraine); Sabatier (INRIA); Thierry (Universitè de Lorraine)

- **HORNET: High-speed Onion Routing at the Network Layer**
  Chen Chen (ETH Zurich & Carnegie Mellon Univ.); Daniele E. Asoni (ETH Zurich); David Barrera (ETH Zurich); George Danezis (Univ. College London); Adrian Perrig (ETH Zurich);

- **Frequency-Hiding Order-Preserving Encryption**
  Florian Kerschbaum (SAP)

- **Transparent Data Deduplication in the Cloud**
  Frederik Armknecht (Univ. of Mannheim); Jens-Matthias Bohli (NEC Laboratories Europe); Ghassan O. Karame (NEC Laboratories Europe); Franck Youssef (NEC Laboratories Europe)

- **Monte Carlo Strength Evaluation: Fast and Reliable Password Checking**
  Matteo Dell'Amico (Symantec Research Labs); Maurizio Filippone (Univ. of Glasgow)

- **The Clock is Still Ticking: Timing Attacks in the Modern Web**
  Tom Van Goethem (KU Leuven); Wouter Joosen (KU Leuven); Nick Nikiforakis (Stony Brook Univ.)

- **Maneuvering Around Clouds: Bypassing Cloud-based Security Providers**
  Thomas Vissers (KU Leuven); Tom Van Goethem (KU Leuven); Wouter Joosen (KU Leuven); Nick Nikiforakis (Stony Brook Univ.)

- **Circuit ORAM: On Tightness of the Goldreich-Ostrovsky Lower Bound**
  Xiao Shaun Wang (Univ. of Maryland); T-H. Hubert Chan (HKU); Elaine Shi (Cornell Univ.)

- **Subversion-Resilient Signature Schemes**
  Giuseppe Ateniese (Sapienza Univ. of Rome); Bernardo Magri (Sapienza Univ. of Rome); Daniele Venturi (Sapienza Univ. of Rome)

- **Automated Analysis and Synthesis of Authenticated Encryption Schemes**
  Viet Tung Hoang (Univ. of Maryland, Georgetown Univ.); Jonathan Katz (Univ. of Maryland); Alex J. Malozemoff (Univ. of Maryland)

- **From Collision To Exploitation: Unleashing Use-After-Free Vulnerabilities in Linux Kernel**

Wen Xu (Shanghai Jiao Tong Univ.); Juanru Li (Shanghai Jiao Tong Univ.); Junliang Shu (Shanghai Jiao Tong Univ.); Wenbo Yang (Shanghai Jiao Tong Univ.); Tianyi Xie (Shanghai Jiao Tong Univ.); Yuanyuan Zhang (Shanghai Jiao Tong Univ.); Dawu Gu (Shanghai Jiao Tong Univ.)

- **Equivalence-based Security for Querying Encrypted Databases: Theory and Application to Privacy Policy Audits**
  Omar Chowdhury (Purdue Univ.); Deepak Garg (Max Planck Institute for Software Systems); Limin Jia (Carnegie Mellon Univ.); Anupam Datta (Carnegie Mellon Univ.)

- **FlowWatcher: Defending against Data Disclosure Vulnerabilities in Web Applications**
  Divya Muthukumaran (Imperial College London); Dan O'Keeffe (Imperial College London); Christian Priebe (Imperial College London); David Eyers (Univ. of Otago); Brian Shand (NCRS, Public Health England); Peter Pietzuch (Imperial College London)

- **Protecting Locations with Differential Privacy under Temporal Correlations**
  Yonghui Xiao (Emory Univ.); Li Xiong (Emory Univ.)

- **Ciphertext-only Cryptanalysis on Hardened Mifare Classic Cards**
  Carlo Meijer (Radboud University); Roel Verdult (Radboud University)

- **MalGene: Automatic Extraction of Malware Analysis Evasion Signature**
  Dhilung Kirat (UC Santa Barbara); Giovanni Vigna (UC Santa Barbara)

- **Static Detection of Packet Injection Vulnerabilities -- A Case for Identifying Attacker-controlled Implicit Information Leaks**
  Qi Alfred Chen (Univ. of Michigan); Zhiyun Qian (Univ. of California Riverside); Yunhan Jack Jia (Univ. of Michigan); Yuru Shao (Univ. of Michigan); Z. Morley Mao (Univ. of Michigan)

- **Per-Input Control-Flow Integrity**
  Ben Niu (Lehigh Univ.); Gang Tan (Lehigh Univ.)

- **Mitigating Storage Side Channels Using Statistical Privacy Mechanisms**
  Qiuyu Xiao (Univ. of North Carolina at Chapel Hill); Michael K. Reiter (Univ. of North Carolina at Chapel Hill); Yinqian Zhang (The Ohio State Univ.)

- **Control Jujutsu: On the Weaknesses of Fine-Grained Control Flow Integrity**
  Isaac Evans (MIT Lincoln Laboratory); Fan Long (MIT CSAIL); Ulziibayar Otgonbaatar (MIT CSAIL); Howard Shrobe (MIT CSAIL); Martin Rinard (MIT CSAIL); Hamed Okhravi (MIT Lincoln Laboratory); Stelios Sidiroglou-Douskos (MIT CSAIL)

- **Authenticating Privately over Public Hotspots**
  Aldo Cassola (Northeastern Univ. & Univ. San Francisco de Quito); Erik-Oliver Blass (Airbus Group Innovations & Northeastern Univ.); Guevara Noubir (Northeastern Univ.)

- **Hare Hunting in the Wild Android: A Study on the Threat of Hanging Attribute References**
  Yousra Aafer (Syracuse Univ.); Nan Zhang (Indiana Univ. Bloomington); Zhongwen Zhang (Institute of Information Engineering, Chinese Academic of Sciences); Xiao Zhang (Syracuse Univ.); Kai Chen (Indiana Univ. Bloomington, Chinese Academy of Sciences); XiaoFeng Wang (Indiana Univ. Bloomington); Xiaoyong Zhou (Samsung Research America); Wenliang Du (Syracuse Univ.); Michael Grace (Samsung Research America)

- **Practicing Oblivious Access on Cloud Storage: the Gap, the Fallacy and the New Way Forward**
  Vincent Bindschaedler (Univ. of Illinois at Urbana-Champaign); Muhammad Naveed (Univ. of Illinois at Urbana-Champaign); Xiaorui Pan (Indiana Univ. Bloomington); XiaoFeng Wang (Indiana Univ. Bloomington); Yan Huang (Indiana Univ. Bloomington)

- **GUITAR: Piecing Together Android App GUIs from Memory Images**
  Brendan Saltaformaggio (Purdue Univ.); Rohit Bhatia (Purdue Univ.); Zhongshu Gu (Purdue Univ.); Xiangyu Zhang (Purdue Univ.); Dongyan Xu (Purdue Univ.)

- **Inference Attacks on Property-Preserving Encrypted Databases**

Muhammad Naveed (Univ. of Illinois at Urbana-Champaign); Seny Kamara (Microsoft Research); Charles V Wright (Portland State Univ.)

- **Perplexed Messengers from the Cloud: Automated Security Analysis of Push-Messaging Integrations**
  Yangyi Chen (Indiana Univ. Bloomington); Tongxin Li (Peking Univ.); XiaoFeng Wang (Indiana Univ. Bloomington); Kai Chen (Indiana Univ. Bloomington and Institute of Information Engineering, CAS); Xinhui Han (Peking Univ.)

- **A Cryptographic Analysis of the TLS 1.3 Handshake Protocol Candidates**
  Benjamin Dowling (Queensland Univ. of Technology); Marc Fischlin (Technische Universität Darmstadt); Felix Günther (Technische Universität Darmstadt); Douglas Stebila (Queensland Univ. of Technology)

- **Unearthing Stealthy Program Attacks Buried in Extremely Long Execution Paths**
  Xiaokui Shu (Virginia Tech); Danfeng (Daphne) Yao (Virginia Tech); Naren Ramakrishnan (Virginia Tech)

- **Tampering with the Delivery of Blocks and Transactions in Bitcoin**
  Arthur Gervais (ETH Zurich); Hubert Ritzdorf (ETH Zurich); Ghassan O. Karame (NEC Laboratories Europe); Srdjan Capkun (ETH Zurich)

- **WebCapsule: Towards a Lightweight Forensic Engine for Web Browsers**
  Christopher Neasbitt (Univ. of Georgia); Bo Li (Univ. of Georgia); Roberto Perdisci (Univ. of Georgia); Long Lu (Stony Brook Univ.); Kapil Singh (IBM Research); Kang Li (Univ. of Georgia)

- **On the Security of TLS 1.3 and QUIC Against Weaknesses in PKCS#1 v1.5 Encryption**
  Tibor Jager (Ruhr Univ. Bochum); Jörg Schwenk (Ruhr Univ. Bochum); Juraj Somorovsky (Ruhr Univ. Bochum)

- **(Un)linkable Pseudonyms for Governmental Databases**
  Jan Camenisch (IBM Research Zurich); Anja Lehmann (IBM Research Zurich)

- **Demystifying Incentives In The Consensus Computer**
  Loi Luu (National Univ. of Singapore); Jason Teutsch (National Univ. of Singapore); Raghav Kulkarni (National Univ. of Singapore); Prateek Saxena (National Univ. of Singapore)

- **A Multi-Modal Neuro-Physiological Study of Phishing Detection and Malware Warnings**
  Ajaya Neupane (Univ. of Alabama at Birmingham); Md. Lutfor Rahman (Marvin Technologies); Nitesh Saxena (Univ. of Alabama at Birmingham); Leanne Hirshfield (Syracuse Univ.)

- **CrowdTarget: Target-based Detection of Crowdturfing in Online Social Networks**
  Jonghyuk Song (Pohang Univ. of Science and Technology); Sangho Lee (Pohang Univ. of Science and Technology); Jong Kim (Pohang Univ. of Science and Technology)

- **Automated Symbolic Proofs of Observational Equivalence**
  David Basin (ETH Zurich); Jannik Dreier (ETH Zurich); Ralf Sasse (ETH Zurich)

- **Symbolic Execution of Obfuscated Code**
  Babak Yadegari (Univ. of Arizona); Saumya Debray (Univ. of Arizona)

- **A Domain-Specific Language for Low-Level Secure Multiparty Computation Protocols**
  Peeter Laud (Cybernetica AS); Jaak Randmets (Cybernetica AS & Univ. of Tartu)

- **Certified PUP: Abuse in Authenticode Code Signing**
  Platon Kotzias (IMDEA Software Institute); Srdjan Matic (Universita degli Studi di Milano); Richard Rivera (IMDEA Software Institute); Juan Caballero (IMDEA Software Institute)

- **Blazing Fast 2PC in the Offline/Online Setting with Security for Malicious Adversaries**
  Yehuda Lindell (Bar-Ilan Univ.); Ben Riva (Bar-Ilan Univ.)

- **Caronte: Detecting Location Leaks for Deanonymizing Tor Hidden Services**
  Srdjan Matic (Universita degli Studi di Milano); Platon Kotzias (IMDEA Software Institute); Juan

Caballero (IMDEA Software Institute)

- **When Good Becomes Evil: Keystroke Inference with Smartwatch**
  Xiangyu Liu (The Chinese Univ. of Hong Kong); Zhe Zhou (The Chinese Univ. of Hong Kong); Wenrui Diao (The Chinese Univ. of Hong Kong); Zhou Li (ACM Member); Kehuan Zhang (The Chinese Univ. of Hong Kong)

- **Towards Automatic Generation of Security-Centric Descriptions for Android Apps**
  Mu Zhang (NEC Laboratories America); Yue Duan (Syracuse Univ.); Qian Feng (Syracuse Univ.); Heng Yin (Syracuse Univ.)

- **SEDA: Scalable Embedded Device Attestation**
  N. Asokan (Aalto Univ. and Univ. of Helsinki); Ferdinand Brasser (Technische Universität Darmstadt); Ahmad Ibrahim (Technische Universität Darmstadt); Ahmad-Reza Sadeghi (Technische Universität Darmstadt); Matthias Schunter (Intel Collaborative Research Institute for Secure Computing (ICRI-SC), Darmstadt); Gene Tsudik (Univ. of California, Irvine); Christian Wachsmann (Technische Universität Darmstadt)

- **Losing Control: On the Effectiveness of Control-Flow Integrity under Stack Attacks**
  Christopher Liebchen (Technische Universität Darmstadt); Marco Negro (Technische Universität Darmstadt); Per Larsen (Univ. of California, Irvine); Lucas Davi (Technische Universität Darmstadt); Ahmad-Reza Sadeghi (Technische Universität Darmstadt); Stephen Crane (Univ. of California, Irvine); Mohaned Qunaibit (Univ. of California, Irvine); Michael Franz (Univ. of California, Irvine); Mauro Conti (Univ. of Padua)

- **GRECS: Graph Encryption for Approximate Shortest Distance Queries**
  Xianrui Meng (Boston Univ.); Seny Kamara (Microsoft Research); Kobbi Nissim (Ben-Gurion Univ.); George Kollios (Boston Univ.)

- **Practical Context-Sensitive CFI**
  Victor van der Veen (VU University Amsterdam); Dennis Andriesse (VU University Amsterdam); Enes Göktas (VU University Amsterdam); Ben Gras (VU University Amsterdam); Lionel Sambuc (VU University Amsterdam); Asia Slowinska (VU University Amsterdam, Lastline, Inc.); Herbert Bos (VU University Amsterdam); Cristiano Giuffrida (VU University Amsterdam);

- **Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges**
  Jeremy Clark (Concordia Univ.); Gaby Dagher (Concordia Univ.); Benedikt Bünz (Stanford Univ.); Joseph Bonneau (Stanford Univ. & EFF); Dan Boneh (Stanford Univ.)

- **iRiS: Vetting Private API Abuse in iOS Applications**
  Zhui Deng (Purdue Univ.); Brendan Saltaformaggio (Purdue Univ.); Xiangyu Zhang (Purdue Univ.); Dongyan Xu (Purdue Univ.)

- **CCFI: Cryptographically Enforced Control Flow Integrity**
  Ali Jose Mashtizadeh (Stanford Univ.); Andrea Bittau (Stanford Univ.); Dan Boneh (Stanford Univ.); David Mazieres (Stanford Univ.)

- **Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures**
  Matt Fredrikson (Carnegie Mellon Univ.); Somesh Jha (Univ. of Wisconsin); Thomas Ristenpart (Cornell Tech)

- **Automated Synthesis of Optimized Circuits for Secure Computation**
  Daniel Demmler (TU Darmstadt); Ghada Dessouky (TU Darmstadt); Farinaz Koushanfar (Rice Univ.); Ahmad-Reza Sadeghi (TU Darmstadt); Thomas Schneider (TU Darmstadt); Shaza Zeitouni (TU Darmstadt)

- **PyCRA: Physical Challenge-Response Authentication for Active Sensors Under Spoofing Attacks**
  Yasser Shoukry (UCLA); Paul Martin (UCLA); Yair Yona (UCLA); Suhas Diggavi (UCLA); Mani Srivastava (UCLA)

- **Detecting and Exploiting Second Order Denial-of-Service Vulnerabilities in Web**

Applications
Oswaldo Olivo (The Univ. of Texas at Austin); Isil Dillig (The Univ. of Texas at Austin); Calvin Lin (The Univ. of Texas at Austin)

- **Mass-surveillance without the State: Strongly Undetectable Algorithm-Substitution Attacks**
  Mihir Bellare (UCSD); Joseph Jaeger (UCSD); Daniel Kane (UCSD)

- **It's a TRAP: Table Randomization and Protection against Function Reuse Attacks**
  Stephen Crane (Univ. of California, Irvine); Stijn Volckaert (Universiteit Gent); Felix Schuster (Ruhr-Universität Bochum); Christopher Liebchen (Technische Universität Darmstadt); Per Larsen (Univ. of California, Irvine); Lucas Davi (Technische Universität Darmstadt); Ahmad-Reza Sadeghi (Technische Universität Darmstadt); Thorsten Holz (Ruhr-Universität Bochum); Bjorn De Sutter (Universiteit Gent); Michael Franz (Univ. of California, Irvine)

- **TOPAS --- 2-Pass Key Exchange with Full Perfect Forward Secrecy and Optimal Communication Complexity**
  Sven Schäge (Ruhr-Universität Bochum)

- **Inlined Information Flow Monitoring for JavaScript**
  Andrey Chudnov (Stevens Institute of Technology); David A. Naumann (Stevens Institute of Technology)

- **Heisenbyte: Thwarting Memory Disclosure Attacks using Destructive Code Reads**
  Adrian Tang (Columbia Univ.); Simha Sethumadhavan (Columbia Univ.); Salvatore Stolfo (Columbia Univ.)

- **Liar, Liar, Coins on Fire! --- Penalizing Equivocation By Loss of Bitcoins**
  Tim Ruffing (CISPA, Saarland Univ.); Aniket Kate (CISPA, Saarland Univ.); Dominique Schröder (CISPA, Saarland Univ.)

- **Privacy-Preserving Deep Learning**
  Reza Shokri (Univ. of Texas at Austin); Vitaly Shmatikov (Cornell Tech)

- **Cross-Site Search Attacks**
  Nethanel Gelernter (Bar-Ilan Univ.); Amir Herzberg (Bar-Ilan Univ.)

- **AUTOREB: Automatically Understanding the Review-to-Behavior Fidelity in Android Applications**
  Deguang Kong (Samsung Research America); Lei Cen (Purdue Univ.); Hongxia Jin (Samsung Research America)

- **Thwarting Memory Disclosure with Efficient Hypervisor-enforced Intra-domain Isolation**
  Yutao Liu (Shanghai Jiao Tong Univ.); Tianyu Zhou (Shanghai Jiao Tong Univ.); Kexin Chen (Shanghai Jiao Tong Univ.); Haibo Chen (Shanghai Jiao Tong Univ.); Yubin Xia (Shanghai Jiao Tong Univ.)

- **Timely Rerandomization for Mitigating Memory Disclosures**
  David Bigelow (MIT Lincoln Laboratory); Thomas Hobson (MIT Lincoln Laboratory); Robert Rudd (MIT Lincoln Laboratory); William Streilein (MIT Lincoln Laboratory); Hamed Okhravi (MIT Lincoln Laboratory)

- **TrustOTP: Transforming Smartphones into Secure One-Time Password Tokens**
  He Sun (College of William and Mary & Chinese Academy of Sciences); Kun Sun (College of William and Mary); Yuewu Wang (Chinese Academy of Sciences); Jiwu Jing (Chinese Academy of Sciences)

- **Exploiting Temporal Dynamics in Sybil Defenses**
  Peng Gao (Princeton Univ.); Changchang Liu (Princeton Univ.); Matthew Wright (Univ. of Texas at Arlington); Prateek Mittal (Princeton Univ.)

- **ASLR-Guard: Stopping Address Space Leakage for Code Reuse Attacks**
  Kangjie Lu (Georgia Institute of Technology); Chengyu Song (Georgia Institute of Technology);

Byoungyoung Lee (Georgia Institute of Technology); Simon P. Chung (Georgia Institute of Technology); Taesoo Kim (Georgia Institute of Technology); Wenke Lee (Georgia Institute of Technology)

- **Observing and Preventing Leakage in MapReduce**
  Olga Ohrimenko (Microsoft Research); Manuel Costa (Microsoft Research); Cédric Fournet (Microsoft Research); Christos Gkantsidis (Microsoft Research); Markulf Kohlweiss (Microsoft Research); Divya Sharma (Carnegie Mellon University)

- **CacheBrowser: Bypassing Chinese Censorship without Proxies Using Cached Content**
  John A. Holowczak (Univ. of Massachusetts Amherst); Amir Houmansadr (Univ. of Massachusetts Amherst)

- **Automated Proofs of Pairing-Based Cryptography**
  Gilles Barthe (IMDEA Software Institute); Benjamin Grègoire (INRIA); Benedikt Schmidt (IMDEA Software Institute)

- **Traitor Deterring Schemes: Using Bitcoin as Collateral for Digital Content**
  Aggelos Kiayias (National and Kapodistrian Univ. of Athens); Qiang Tang (Univ. of Connecticut);

- **White-Box Cryptography Revisited: Space-Hard Ciphers**
  Andrey Bogdanov (Technical Univ. of Denmark); Takanori Isobe (Sony Corporation)

- **Leakage-Abuse Attacks Against Searchable Encryption**
  David Cash (Rutgers Univ.); Paul Grubbs (Cornell Univ., SkyHigh Networks); Jason Perry (Rutgers Univ.); Thomas Ristenpart (Cornell Tech)

- **Constant Communication ORAM with Small Blocksize**
  Tarik Moataz (Colorado State Univ. & Telecom Bretagne); Travis Mayberry (United States Naval Academy); Erik-Oliver Blass (Airbus Group Innovations)

- **Walls Have Ears! Opportunistically Communicating Secret Messages Over the Wiretap Channel: from Theory to Practice**
  Qian Wang (Wuhan Univ.); Kui Ren (The State Univ. of New York at Buffalo); Guancheng Li (Wuhan Univ.); Chenbo Xia (Wuhan Univ.); Xiaobing Chen (Wuhan Univ.); Zhibo Wang (Wuhan Univ.); Qin Zou (Wuhan Univ.)

- **A Search Engine Backed by Internet-Wide Scanning**
  Zakir Durumeric (Univ. of Michigan); David Adrian (Univ. of Michigan); Ariana Mirian (Univ. of Michigan); Michael Bailey (Univ. of Illinois at Urbana-Champaign); J. Alex Halderman (Univ. of Michigan)

- **An Empirical Study of Web Vulnerability Discovery Ecosystems**
  Mingyi Zhao (Pennsylvania State Univ.); Jens Grossklags (Pennsylvania State Univ.); Peng Liu (Pennsylvania State Univ.)

- **Fast and Secure Three-party Computation: The Garbled Circuit Approach**
  Payman Mohassel (Yahoo Labs); Mike Rosulek (Oregon State Univ.); Ye Zhang (Penn State Univ.)

- **Nomad: Mitigating Arbitrary Cloud Side Channels via Provider-Assisted Migration**
  Soo-Jin Moon (Carnegie Mellon Univ.); Vyas Sekar (Carnegie Mellon Univ.); Michael K. Reiter (Univ. of North Carolina at Chapel Hill)

- **Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice**
  David Adrian (Univ. of Michigan); Karthikeyan Bhargavan (INRIA Paris-Rocquencourt); Zakir Durumeric (Univ. of Michigan); Pierrick Gaudry (INRIA Nancy-Grand Est, CNRS and Université de Lorraine); Matthew Green (Johns Hopkins Univ.); J. Alex Halderman (Univ. of Michigan); Nadia Heninger (Univ. of Pennsylvania); Drew Springall (Univ. of Michigan); Emmanuel Thomé (INRIA Nancy-Grand Est, CNRS and Université de Lorraine); Luke Valenta (Univ. of Pennsylvania); Benjamin VanderSloot (Univ. of Michigan); Eric Wustrow (Univ. of Michigan); Santiago Zanella-Béguelin (Microsoft Research); Paul Zimmermann (INRIA Nancy-Grand Est, CNRS and Université de Lorraine)

- **The Spy in the Sandbox: Practical Cache Attacks in Javascript and their Implications**
  Yossef Oren (Columbia Univ.); Vasileios P. Kemerlis (Columbia Univ.); Simha Sethumadhavan (Columbia Univ.); Angelos D. Keromytis (Columbia Univ.)

- **Location-restricted Service Access Control Leveraging Pinpoint Waveforming**
  Tao Wang (Univ. of South Florida); Yao Liu (Univ. of South Florida); Qingqi Pei (Xidian Univ.); Tao Hou (Univ. of South Florida)

- **The SICILIAN Defense: Signature-based Whitelisting of Web JavaScript**
  Pratik Soni (National Univ. of Singapore); Enrico Budianto (National Univ. of Singapore); Prateek Saxena (National Univ. of Singapore)

- **IntegriDB: Verifiable SQL for Outsourced Databases**
  Yupeng Zhang (Univ. of Maryland); Jonathan Katz (Univ. of Maryland); Charalampos Papamanthou (Univ. of Maryland)

- **How to Use Bitcoin to Play Decentralized Poker**
  Ranjit Kumaresan (MIT); Tal Moran (IDC Herzliya); Iddo Bentov (Technion)

- **Micropayments for Decentralized Currencies**
  Rafael Pass (Cornell Tech); abhi shelat (U Virginia)

- **Android Root and its Providers: A Double-Edged Sword**
  Hang Zhang (Univ. of California, Riverside); Dongdong She (Univ. of California, Riverside); Zhiyun Qian (Univ. of California, Riverside)

- **Seeing through Network Protocol Obfuscation**
  Liang Wang (Univ. of Wisconsin); Kevin P. Dyer (Portland State Univ.); Aditya Akella (Univ. of Wisconsin); Thomas Ristenpart (Cornell Tech); Thomas Shrimpton (Portland State Univ.)

- **UCognito: Private Browsing without Tears**
  Meng Xu (Georgia Institute of Technology); Yeongjin Jang (Georgia Institute of Technology); Xinyu Xing (Georgia Institute of Technology); Taesoo Kim (Georgia Institute of Technology); Wenke Lee (Georgia Institute of Technology)

- **SafeDSA: Safeguard Dynamic Spectrum Access against Fake Secondary Users**
  Xiaocong Jin (Arizona State Univ.); Jingchao Sun (Arizona State Univ.); Rui Zhang (Univ. of Hawaii); Yanchao Zhang (Arizona State Univ.)

- **Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations**
  Hongil Kim (KAIST); Dongkwan Kim (KAIST); Minhee Kwon (KAIST); HyungSeok Han (KAIST); Yeongjin Jang (Georgia Institute of Technology); Dongsu Han (KAIST); Taesoo Kim (Georgia Institute of Technology); Yongdae Kim (KAIST)

- **Trusted Display on Untrusted Commodity Platforms**
  Miao Yu (Carnegie Mellon Univ.); Virgil D. Gligor (Carnegie Mellon Univ.); Zongwei Zhou (Carnegie Mellon Univ.)

- **VCR: App-Agnostic Recovery of Photographic Evidence from Android Device Memory Images**
  Brendan Saltaformaggio (Purdue Univ.); Rohit Bhatia (Purdue Univ.); Zhongshu Gu (Purdue Univ.); Xiangyu Zhang (Purdue Univ.); Dongyan Xu (Purdue Univ.)

- **Fast Non-Malleable Commitments**
  Hai Brenner (IDC Herzliya); Vipul Goyal (Microsoft Research, Bangalore); Silas Richelson (UCLA); Alon Rosen (IDC Herzliya); Margarita Vald (Tel Aviv Univ.)

- **Optimal Distributed Password Verification**
  Jan Camenisch (IBM Research - Zurich); Anja Lehmann (IBM Research - Zurich); Gregory Neven (IBM Research - Zurich)

- **Lattice Basis Reduction Attack against Physically Unclonable Functions**
  Fatemeh Ganji (Technische Universität Berlin); Juliane Krämer (Technische Universität

Darmstadt); Jean-Pierre Seifert (Technische Universität Berlin); Shahin Tajik (Technische Universität Berlin)

- **The Dropper Effect: Insights into Malware Distribution with Downloader Graph Analytics**
  Bum Jun Kwon (Univ. of Maryland); Jayanta Mondal (Univ. of Maryland); Jiyong Jang (IBM Research, Yorktown Heights); Leyla Bilge (Symantec Research Labs, France); Tudor Dumitraș (Univ. of Maryland)

- **Efficient Genome-Wide, Privacy-Preserving Similar Patient Query based on Private Edit Distance**
  Xiao Shaun Wang (Univ. of Maryland); Yan Huang (Indiana Univ. Bloomington); Yongan Zhao (Indiana Univ. Bloomington); Haixu Tang (Indiana Univ. Bloomington); Xiaofeng Wang (Indiana Univ. Bloomington); Diyue Bu (Indiana Univ. Bloomington)

- **SPRESSO: A Secure, Privacy-Respecting Single Sign-On System for the Web**
  Daniel Fett (Univ. of Trier); Ralf Kuesters (Univ. of Trier); Guido Schmitz (Univ. of Trier)

- **DEMOS-2: Scalable E2E Verifiable Elections without Random Oracles**
  Aggelos Kiayias (National and Kapodistrian Univ. of Athens); Thomas Zacharias (National and Kapodistrian Univ. of Athens); Bingsheng Zhang (Lancaster Univ.)

- **Falcon Codes: Fast, Authenticated LT Codes (Or: Making Rapid Tornadoes Unstoppable)**
  Ari Juels (Cornell Tech); James Kelley (NetApp); Roberto Tamassia (Brown Univ.); Nikos Triandopoulos (RSA Laboratories & Boston Univ.)