

# Table of Contents

<b>AsiaCCS 2019 Conference Organization .....</b>	<b>1</b>
---	----------

<b>AsiaCCS 2019 Sponsor &amp; Supporters .....</b>	<b>1</b>
--	----------

## Keynote 1

- **Establishing and Maintaining Root of Trust on Commodity Computer Systems .....** 1  
Virgil Gligor (*Carnegie Mellon University*)

## Session 1A: Binary Analysis and Hardening

- **Control-Flow Carrying Code .....** 3  
Yan Lin (*Singapore Management University*), Xiaoyang Cheng (*NanKai University*),  
Debin Gao (*Singapore Management University*)
- **SoK: Using Dynamic Binary Instrumentation for Security (And How You May Get Caught Red Handed) .....** 15  
Daniele Cono D'Elia, Emilio Coppa, Simone Nicchi (*Sapienza University of Rome*),  
Federico Palmaro (*Prisma*), Lorenzo Cavallaro (*King's College London*)
- **DeClassifier:Class-Inheritance Inference Engine for Optimized C++ Binaries .....** 28  
Rukayat Ayomide Erinfolami, Aravind Prakash (*Binghamton University*)

## Session 1B: Cloud Security

- **GraphSE2: An Encrypted Graph Database for Privacy-Preserving Social Search .....** 41  
Shangqi Lai (*Monash University/Data61, CSIRO*), Xingliang Yuan (*Monash University*),  
Shi-Feng Sun (*Monash University/Data61, CSIRO*), Joseph K. Liu (*Monash University*),  
Yuhong Liu (*Santa Clara University*), Dongxi Liu (*Data61, CSIRO*)
- **Identity-Based Broadcast Encryption with Outsourced Partial Decryption for Hybrid Security Models in Edge Computing .....** 55  
Jongkil Kim (*University of Wollongong*), Seyit Camtepe (*CSIRO*),  
Willy Susilo (*University of Wollongong*), Surya Nepal (*CSIRO*), Joonsang Baek (*University of Wollongong*)
- **Unveiling Systematic Biases in Decisional Processes: An Application to Discrimination Discovery .....** 67  
Laura Genga, Luca Allodi, Nicola Zannone (*Eindhoven University of Technology*)

## Session 2A: SGX-based Security

- **The SEVerESt Of Them All: Inference Attacks Against Secure Virtual Enclaves .....** 73  
Jan Werner (*University of North Carolina*), Joshua Mason (*University of Illinois*),  
Manos Antonakakis (*Georgia Institute of Technology*), Michalis Polychronakis (*Stony Brook University*),  
Fabian Monrose (*University of North Carolina*)
- **ObliDC: An SGX-based Oblivious Distributed Computing Framework with Formal Proof .....** 86  
Pengfei Wu, Qingni Shen (*Peking University*), Robert H. Deng (*Singapore Management University*),  
Ximeng Liu (*Fuzhou University*), Yinghui Zhang (*Xi'an University of Posts and Telecommunications*),  
Zhonghai Wu (*Peking University*)
- **A Hybrid Approach to Secure Function Evaluation using SGX .....** 100  
Joseph I. Choi, Dave (Jing) Tian, Grant Hernandez, Christopher Patton (*University of Florida*),  
Benjamin Mood (*Point Loma Nazarene University*),  
Thomas Shrimpton, Kevin R. B. Butler, Patrick Traynor (*University of Florida*)
- **Running Language Interpreters Inside SGX: A Lightweight, Legacy-Compatible Script Code Hardening Approach .....** 114  
Huibao Wang, Erick Bauman, Vishal Karande (*University of Texas at Dallas*),  
Zhiqiang Lin (*Ohio State University*), Yueqiang Cheng (*Baidu USA*), Yinqian Zhang (*Ohio State University*)

## Session 2B: Advanced Encryption Algorithms

- **Multi-Writer Searchable Encryption: An LWE-based Realization and Implementation** ..... 122  
Lei Xu (*Nanjing University of Science and Technology*), Xingliang Yuan, Ron Steinfeld (*Monash University*),  
Cong Wang (*City University of Hong Kong*), Chungxu Xu (*Nanjing University of Science and Technology*)
- **Delegatable Order-Revealing Encryption** ..... 134  
Yuan Li, Hongbing Wang, Yunlei Zhao (*Fudan University*)
- **MPC Joins The Dark Side** ..... 148  
John Cartledge (*University of Bristol*), Nigel P. Smart (*KU Leuven & University of Bristol*),  
Younes Talibi Alaoui (*KU Leuven*)
- **Flexibly and Securely Shape Your Data Disclosed to Others** ..... 160  
Qingqing Xie (*Jiangsu University*), Yantian Hou (*Boise State University*),  
Ke Cheng (*Xidian University*), Gaby G. Dagher (*Boise State University*),  
Liangmin Wang (*Jiangsu University*), Shucheng Yu (*Stevens Institute of Technology*)

## Session 3A: Web Attack Measurements

- **Waves of Malice: A Longitudinal Measurement of the Malicious File Delivery Ecosystem on the Web** ..... 168  
Colin C. Iff (*University College London*), Yun Shen (*Symantec Research Labs*),  
Steven J. Murdoch (*University College London*), Gianluca Stringhini (*Boston University*)
- **What Happens After You Leak Your Password: Understanding Credential Sharing on Phishing Sites** ..... 181  
Peng Peng, Chao Xu, Luke Quinn, Hang Hu, Bimal Viswanath, Gang Wang (*Virginia Tech*)
- **A Decade of Mal-Activity Reporting: A Retrospective Analysis of Internet Malicious Activity Blacklists**..... 193  
Benjamin Zi Hao Zhao (*University of New South Wales & Data61, CSIRO*),  
Muhammad Ikram (*Macquarie University & University of Michigan*),  
Hassan Jameel Asghar, Mohamed Ali Kaafar (*Macquarie University*), Abdelberi Chaabane (*No Affiliation*),  
Kanchana Thilakarathna (*The University of Sydney*)
- **Mobile Friendly or Attacker Friendly? A Large-scale Security Evaluation of Mobile-first Websites** ..... 206  
Tom Van Goethem, Victor Le Pochat, Wouter Joosen (*KU Leuven*)

## Session 3B: Learning and Authentication

- **Undermining User Privacy on Mobile Devices Using AI**..... 214  
Berk Gulmezoglu (*Worcester Polytechnic Institute*), Andreas Zankl (*Fraunhofer AISEC*),  
M. Caner Tol (*Middle East Technical University*), Saad Islam (*Worcester Polytechnic Institute*),  
Thomas Eisenbarth (*University of Lübeck*), Berk Sunar (*Worcester Polytechnic Institute*)
- **Robust Watermarking of Neural Network with Exponential Weighting** ..... 228  
Ryota Namba (*University of Tsukuba*), Jun Sakuma (*University of Tsukuba, RIKEN AIP*)
- **A Closer Look Tells More: A Facial Distortion Based Liveness Detection for Face Authentication** ..... 241  
Yan Li, Zilong Wang (*Xidian University*), Yingjiu Li, Robert Deng (*Singapore Management University*),  
Binbin Chen (*Advanced Digital Science Center*), Weizhi Meng (*Technical University of Denmark*),  
Hui Li (*Xidian University*)
- **R2Q: A Risk Quantification Framework to Authorize Requests in Web-based Collaborations**..... 247  
Nirnay Ghosh (*Indian Institute of Engineering Science and Technology*),  
Rishabh Singhal (*JP Morgan Chase & Co.*), Sajal K. Das (*Missouri University of Science and Technology*)

## Keynote 2

- **Security is the Weakest Link: Prevalent Culture of Victim Blaming in Cyberattacks**..... 255  
Surya Nepal (*CSIRO Data61*)

## Session 4A: Mobile Security

- **Exploiting Sound Masking for Audio Privacy in Smartphones** ..... 257  
Yu-Chih Tung, Kang G. Shin (*The University of Michigan*)
- **MoSSOT: An Automated Blackbox Tester for Single Sign-On Vulnerabilities in Mobile Applications** ..... 269  
Shangcheng Shi, Xianbo Wang, Wing Cheong Lau (*The Chinese University of Hong Kong*)
- **MagAttack: Guessing Application Launching and Operation via Smartphone** ..... 283  
Yushi Cheng, Xiaoyu Ji (*Zhejiang University & Alibaba-Zhejiang University Joint Institute of Frontier Technologies*),  
Wenyuan Xu (*Zhejiang University*), Hao Pan (*Shanghai Jiao Tong University*),  
Zhuangdi Zhu (*Michigan State University*), Chuang-Wen You (*National Taiwan University*),  
Yi-Chao Chen, Lili Qiu (*University of Texas at Austin*)
- **Towards Understanding Android System Vulnerabilities: Techniques and Insights** ..... 295  
Daoyuan Wu, Debin Gao (*Singapore Management University*),  
Eric K. T. Cheng (*The Hong Kong Polytechnic University*), Yichen Cao, Jintao Jiang (*SOBUG*),  
Robert H. Deng (*Singapore Management University*)
- **AndrEnsemble: Leveraging API Ensembles to Characterize Android Malware Families** ..... 307  
Omid Mirzaei (*Universidad Carlos III de Madrid*), Guillermo Suarez-Tangil (*King's College London*),  
Jose M. de Fuentes, Juan Tapiador (*Universidad Carlos III de Madrid*), Gianluca Stringhini (*Boston University*)

## Session 4B: Privacy

- **EPISODE: Efficient Privacy-Preserving Similar Sequence Queries on Outsourced Genomic Databases** ..... 315  
Thomas Schneider, Oleksandr Tkachenko (*TU Darmstadt*)
- **Revisiting Assumptions for Website Fingerprinting Attacks** ..... 328  
Weiqi Cui, Tao Chen, Christian Fields, Julianna Chen, Anthony Sierra (*Oklahoma State University*),  
Eric Chan-Tin (*Loyola University Chicago*)
- **Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control** ..... 340  
Iskander Sanchez-Rola (*University of Deusto & Symantec Research Labs*),  
Matteo Dell'Amico (*Symantec Research Labs*),  
Platon Kotzias (*IMDEA Software Institute & University Politécnica de Madrid*),  
Davide Balzarotti (*EURECOM*), Leyla Bilge, Pierre-Antoine Vervier (*Symantec Research Labs*),  
Igor Santos (*University of Deusto*)
- **Understanding Users' Risk Perceptions about Personal Health Records Shared on Social Networking Services** ..... 352  
Yuri Son (*Sungkyunkwan University & Samsung Electronics*),  
Geumhwan Cho, Hyounghick Kim, Simon Woo (*Sungkyunkwan University*)

## Session 5A: Web Security

- **Purchased Fame: Exploring the Ecosystem of Private Blog Networks** ..... 366  
Tom Van Goethem (*KU Leuven*), Najmeh Miramirkhani (*Stony Brook University*),  
Wouter Joosen (*KU Leuven*), Nick Nikiforakis (*Stony Brook University*)
- **TweetScore: Scoring Tweets via Social Attribute Relationships for Twitter Spammer Detection** ..... 379  
Yihe Zhang (*University of Louisiana at Lafayette*), Hao Zhang (*ACM Member*),  
Xu Yuan, Nian-Feng Tzeng (*University of Louisiana at Lafayette*)
- **ScriptProtect: Mitigating Unsafe Third-Party JavaScript Practices** ..... 391  
Marius Musch (*TU Braunschweig*),  
Marius Steffens, Sebastian Roth, Ben Stock (*CISPA Helmholtz Center for Information Security*),  
Martin Johns (*TU Braunschweig*)

## Session 5B: Fault Attacks and Side Channel Analysis

- **SoK: On DFA Vulnerabilities of Substitution-Permutation Networks**..... 403  
Mustafa Khairallah (NTU), Xiaolu Hou (Acronis), Zakaria Najm (NTU and TU Delft),  
Jakub Breier, Shivam Bhasin, Thomas Peyrin (NTU)
- **Practical Side-Channel Attacks against WPA-TKIP** ..... 415  
Domien Schepers, Aanjan Ranganathan (Northeastern University),  
Mathy Vanhoef (New York University Abu Dhabi)
- **Exploiting Determinism in Lattice-based Signatures: Practical Fault Attacks on pqm4  
Implementations of NIST Candidates**..... 427  
Prasanna Ravi (Nanyang Technological University), Mahabir Prasad Jhanwar (Ashoka University),  
James Howe (PQShield, Ltd.), Anupam Chattopadhyay, Shivam Bhasin (Nanyang Technological University)

## Session 6A: IoT Security

- **Process-Aware Cyberattacks for Thermal Desalination Plants** ..... 441  
Prashant Hari Narayan Rajput, Pankaj Rajput (New York University),  
Marios Sazos, Michail Maniatakos (New York University Abu Dhabi)
- **Misbinding Attacks on Secure Device Pairing and Bootstrapping** ..... 453  
Mohit Sethi (Ericsson Research & Aalto University),  
Aleksi Peltonen, Tuomas Aura (Aalto University)
- **Alexa Lied to Me: Skill-based Man-in-the-Middle Attacks on Virtual Assistants** ..... 465  
Richard Mitev, Markus Miettinen, Ahmad-Reza Sadeghi (Technische Universität Darmstadt)
- **HADES-IoT: A Practical Host-Based Anomaly Detection System for IoT Devices** ..... 479  
Dominik Breitenbacher, Ivan Homoliak, Yan Lin Aung (Singapore University of Technology and Design),  
Nils Ole Tippenhauer (CISPA Helmholtz Center for Information Security),  
Yuval Elovici (Singapore University of Technology and Design)
- **A Pilot Study on Consumer IoT Device Vulnerability Disclosure and Patch  
Release in Japan and the United States** ..... 485  
Asuka Nakajima, Takuya Watanabe, Eitaro Shioji, Mitsuki Akiyama (NTT Secure Platform Laboratories),  
Maverick Woo (Carnegie Mellon University)
- **E-Spion: A System-Level Intrusion Detection System for IoT Devices** ..... 493  
Anand Mudgerikar (Purdue University), Puneet Sharma (HPE), Elisa Bertino (Purdue University)

## Session 6B: Applied Cryptography

- **K2SN-MSS: An Efficient Post-Quantum Signature**..... 501  
Sabyasachi Karati (National Institute of Science Education and Research),  
Reihaneh Safavi-Naini (University of Calgary)
- **Proper Usage of the Group Signature Scheme in ISO/IEC 20008-2**..... 515  
Ai Ishida, Yusuke Sakai, Keita Emura, Goichiro Hanaoka  
(National Institute of Advanced Industrial Science and Technology),  
Keisuke Tanaka (Tokyo Institute of Technology)
- **Practical Aggregate Signature from General Elliptic Curves,  
and Applications to Blockchain** ..... 529  
Yunlei Zhao (Fudan University)
- **Examining DES-based Cipher Suite Support within the TLS Ecosystem**..... 539  
Vanessa Frost, Dave (Jing) Tian, Christie Ruales, Vijay Prakash, Patrick Traynor,  
Kevin R. B. Butler (University of Florida)

## Keynote 3

- **From Attacker Models to Reliable Security**..... 547  
Heiko Mantel (TU Darmstadt)

## Session 7: Hardware and Systems

- **Pinpoint Rowhammer: Suppressing Unwanted Bit Flips on Rowhammer Attacks** ..... 549  
Sangwoo Ji , Youngjoo Ko, Saeyoung Oh, Jong Kim (*Pohang University of Science and Technology*)
- **RIP-RH: Preventing Rowhammer-based Inter-Process Attacks** ..... 561  
Carsten Bock, Ferdinand Brasser, David Gens, Christopher Liebchen,  
Ahamd-Reza Sadeghi (*Technische Universität Darmstadt*)
- **eHIFS: An Efficient History Independent File System** ..... 573  
Biao Gao (*University of Chinese Academy of Sciences*), Bo Chen (*Michigan Technological University*),  
Shijie Jia (*Institute of Information Engineering, Chinese Academy of Sciences*),  
Luning Xia (*University of Chinese Academy of Sciences*)
- **Thermanator: Thermal Residue-Based Post Factum Attacks on Keyboard Data Entry** ..... 586  
Tyler Kaczmarek, Ercan Ozturk, Gene Tsudik (*University of California, Irvine*)
- **Design Procedure of Knowledge Base for Practical Attack Graph Generation** ..... 594  
Masaki Inokuchi, Yoshinobu Ohta, Shunichi Kinoshita, Tomohiko Yagyu (*NEC Corporation*),  
Orly Stan, Ron Bitton, Yuval Elovici, Asaf Shabtai (*Ben-Gurion University of the Negev*)

## Session 8: Blockchain Security

- **On the Difficulty of Hiding the Balance of Lightning Network Channels** ..... 602  
Jordi Herrera-Joancomartí, Guillermo Navarro-Arribas (*Universitat Autònoma de Barcelona, Cybercat*),  
Alejandro Ranchal-Pedrosa (*Institut Polytechnique de Paris, CNRS SAMOVAR, Telecom SudParis*),  
Cristina Pérez-Solà (*Universitat Oberta de Catalunya, Cybercat*),  
Joaquin Garcia-Alfaro (*Institut Polytechnique de Paris, CNRS SAMOVAR, Telecom SudParis*)
- **A New Blind ECDSA Scheme for Bitcoin Transaction Anonymity** ..... 613  
Xun Yi (*MIT University*), Kwok-Yan Lam (*Nanyang Technological University*)
- **On The Unforkability of Monero** ..... 621  
Dimaz Ankaa Wijaya, Joseph K. Liu, Ron Steinfeld (*Monash University*),  
Dongxi Liu (*Data61, CSIRO*), Jiangshan Yu (*Monash University*)

## Session 9: Fuzzing

- **PTrix: Efficient Hardware-Assisted Fuzzing for COTS Binary** ..... 633  
Yaohui Chen (*Northeastern University*), Dongliang Mu (*Penn State University*),  
Jun Xu (*Stevens Institute of Technology*), Zhichuang Sun (*Northeastern University*),  
Wenbo Shen (*Zhejiang University*), Xinyu Xing (*Penn State University*),  
Long Lu (*Northeastern University*), Bing Mao (*Nanjing University*)
- **An Empirical Study of Prioritizing JavaScript Engine Crashes via Machine Learning** ..... 646  
Sunnyeo Park, Dohyeok Kim, Soeul Son (*Korea Advanced Institute of Science & Technology*)
- **A Feature-Oriented Corpus for Understanding, Evaluating and Improving Fuzz Testing** ..... 658  
Xiaogang Zhu, Xiaotao Feng, Tengyun Jiao, Sheng Wen, Yang Xiang (*Swinburne University of Technology*),  
Seyit Camtepe (*DATA61 CSIRO*), Jingling Xue (*The University of New South Wales*)

## Poster Presentations

- **POSTER: How to Securely Record Logs based on ARM TrustZone** ..... 664  
Seungho Lee, Wonsuk Choi (*Korea University*), Hyo Jin Jo (*Hallym University*),  
Dong Hoon Lee (*Korea University*)
- **POSTER: Characterizing Adversarial Subspaces by Mutual Information** ..... 667  
Chia-Yi Hsu (*National Chung Hsing University*), Pin-Yu Chen (*IBM Research*),  
Chia-Mu Yu (*National Chung Hsing University*)
- **POSTER: A Data Life Cycle Modeling Proposal by Means of Formal Methods** ..... 670  
Madalina G. Ciobanu, Fausto Fasano (*University of Molise*), Fabio Martinelli (*IIT-CNR*),  
Francesco Mercaldo (*IIT-CNR & University of Molise*), Antonella Santone (*University of Molise*)
- **POSTER: Cracking the Graph Routes in WirelessHART Networks** ..... 673  
Xia Cheng, Junyang Shi, Mo Sha (*State University of New York at Binghamton*)

• <b>POSTER: Fidelity: A Property of Deep Neural Networks to Measure the Trustworthiness of Prediction Results</b> .....	676
Ziqi Yang ( <i>National University of Singapore</i> )	
• <b>POSTER: Towards Identifying Early Indicators of a Malware Infection</b> .....	679
Sareena Karapoola, Chester Rebeiro ( <i>Indian Institute of Technology Madras</i> ), Unnati Parekh ( <i>IIT Madras</i> ), Kamakoti Veezhinathan ( <i>Indian Institute of Technology Madras</i> )	
• <b>POSTER: Vendor-Independent Monitoring on Programmable Logic Controller Status for ICS Security Log Management</b> .....	682
Jongwon Choi, HyungKwan Kim, Seungoh Choi, Jeong-Han Yun, Byung-Gil Min, HyoungChun Kim ( <i>The affiliated institute of ETRI</i> )	
• <b>POSTER: IoT Application-Centric Access Control (ACAC)</b> .....	685
Mohammed Al-Shaboti, Ian Welch, Aaron Chen ( <i>Victoria University of Wellington</i> )	
• <b>POSTER: High Efficiency, Low-noise Meltdown Attack by using a Return Stack Buffer</b> .....	688
TaeHyun Kim, Youngjoo Shin ( <i>Kwangwoon University</i> )	
• <b>POSTER: Smart Contract-based Miner Registration and Block Validation</b> .....	691
Shijie Zhang, Jong-Hyoun Lee ( <i>Sangmyung University</i> )	
<b>Author Index</b> .....	694