24TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY

October 30-November 3, 2017 | Dallas, Texas

ACM CCS 2017

acm SIGSAC

UT DALLAS
The University of Texas at Dallas

2017 PROGRAM COMMITTEE

Program Chairs

David Evans, University of Virginia
Tal Malkin, Columbia University
Dongyan Xu, Purdue University

Program Committee

Sadia Afroz, UC Berkeley / ICSI
Gail-Joon Ahn, Arizona State University
Ehab Al-Shaer, University of North Carolina Charlotte
Elias Athanasopoulos, University of Cyprus
Foteini Baldimtsi, George Mason University
David Basin, ETH Zurich
Adam Bates, University of Illinois at Urbana Champaign
Lujo Bauer, Carnegie Mellon University
Konstantin Beznosov, University of British Columbia
Karthikeyan Bhargavan, INRIA
Alex Biryukov, University of Luxembourg
Jeremiah Blocki, Purdue University
Elette Boyle, IDC Herzliya
Levente Buttyán, CrySyS Lab, BME
Juan Caballero, IMDEA Software Institute
Joseph Calandrino, Federal Trade Commission
Aylin Caliskan, Princeton University
Yinzhi Cao, Lehigh University
Alvaro A. Cardenas, The University of Texas at Dallas
Lorenzo Cavallaro, Royal Holloway, University of London
Neha Chachra, Facebook
Melissa Chase, Microsoft Research
Haibo Chen, Shanghai Jiao Tong University
Hao Chen, University of California, Davis
Omar Chowdhury, University of Iowa
Nicolas Christin, Carnegie Mellon University
Véronique Cortier, Loria (CNRS, France)
Manuel Costa, Microsoft Research
Scott Coull, FireEye
Weidong Cui, Microsoft Research
Anupam Das, Carnegie Mellon University
Anupam Datta, Carnegie Mellon University
Lucas Davi, University of Duisburg-Essen
Emiliano De Cristofaro, University College London
Tamara Denning, University of Utah
Xuhua Ding, Singapore Management University
Brendan Dolan-Gavitt, New York University
Adam Doupé, Arizona State University
Tudor Dumitra, University of Maryland
Serge Egelman, UC Berkeley / ICSI
Ittay Eyal, Cornell University
Sascha Fahl, Saarland University
Christopher Fletcher, NVIDIA/UIUC
Aurélien Francillon, EURECOM
Matt Fredrikson, Carnegie Mellon University
Xinyang Ge, Microsoft Research
Daniel Genkin, University of Pennsylvania / University of Maryland
Rosario Gennaro, City College of New York
Phillipa Gill, University of Massachusetts Amherst
Dov Gordon, George Mason University
Andreas Haeberlen, University of Pennsylvania
J. Alex Halderman, University of Michigan
Shai Halevi, IBM Research
Matthew Hicks, MIT Lincoln Laboratory
Michael Hicks, University of Maryland
Thorsten Holz, Ruhr-Universität Bochum
Amir Houmansadr, University of Massachusetts Amherst
Yan Huang, Indiana University
Kyu Hyung Lee, University of Georgia
Trent Jaeger, Penn State University
Suman Jana, Columbia University
Limin Jia, Carnegie Mellon University
Yier Jin, University of Central Florida
Aaron Johnson, U.S. Naval Research Laboratory
Philipp Jovanovic, École Polytechnique Fédérale de Lausanne
Brent ByungHoon Kang, KAIST
Aniket Kate, Purdue University
Jonathan Katz, University of Maryland
Stefan Katzenbeisser, TU Darmstadt
Marcel Keller, University of Bristol
Aggelos Kiayias, University of Edinburgh

2017 PROGRAM COMMITTEE

Taesoo Kim, Georgia Tech
Yongdae Kim, KAIST
Engin Kirda, Northeastern University
David Kotz, Dartmouth
Farinaz Koushanfar, UC San Diego
Ralf Küsters, University of Stuttgart
Andrea Lanzi, University of Milan
Byoungyoung Lee, Purdue University
Wenke Lee, Georgia Tech
Brian N. Levine, University of Massachusetts Amherst
Zhichun Li, NEC Labs
Zhou Li, RSA
David Lie, University of Toronto
Yao Liu, University of South Florida
Matteo Maffei, TU Vienna
Mohammad Mahmody, University of Virginia
Z. Morley Mao, University of Michigan
Ivan Martinovic, University of Oxford
Michelle L. Mazurek, University of Maryland
Jonathan McCune, Google
Andrew Miller, University of Illinois at Urbana Champaign
Tal Moran, IDC Herzliya
Muhammad Naveed, University of Southern California
Nick Nikiforakis, Stony Brook University
Hamed Okhravi, MIT Lincoln Laboratory
Alina Oprea, Northeastern University
Mathias Payer, Purdue University
Adrian Perrig, ETH Zurich
Michalis Polychronakis, Stony Brook University
Georgios Portokalidis, Stevens Institute of Technology
Bart Preneel, KU Leuven
Zhiyun Qian, University of California, Riverside
Kasper Rasmussen, University of Oxford
Aseem Rastogi, Microsoft Research India
Mariana Raykova, Yale University
Kaveh Razavi, Vrije Universiteit
William Robertson, Northeastern University
Christian Rossow, Saarland University
Mike Rosulek, Oregon State University
Patrick Schaumont, Virginia Tech
Abhi Shelat, Northeastern University
Micah Sherr, Georgetown University
Timothy Sherwood, UC Santa Barbara
Reza Shokri, Cornell Tech
Stelios Sidiroglou-Douskos, MIT
Chengyu Song, UC Riverside
Douglas Stebila, McMaster University
Deian Stefan, UC San Diego
Gianluca Stringhini, University College London
Kun Sun, George Mason University
Ewa Syta, Trinity College
Mohit Tiwari, UT Austin
Patrick Traynor, University of Florida
Carmela Troncoso, IMDEA Software Institute
Blase Ur, University of Chicago
Marten van Dijk, University of Connecticut
Haining Wang, University of Delaware
XiaoFeng Wang, Indiana University
Zhi Wang, Florida State University
Matthew Wright, Rochester Institute of Technology
Dinghao Wu, Pennsylvania State University
Zhenyu Wu, NEC Laboratories America
Luyi Xing, Indiana University
Xinyu Xing, Pennsylvania State University
Guanhua Yan, Binghamton University
Lok Yan, Air Force Research Laboratory
Heng Yin, University of California, Riverside
Samee Zahur, Google
Fengwei Zhang, Wayne State University
Kehuan Zhang, Chinese University of Hong Kong
Yanchao Zhang, Arizona State University
Yinqian Zhang, The Ohio State University
Sencun Zhu, Pennsylvania State University
Saman Zonouz, Rutgers University

ORGANIZING COMMITTEE

General Chair

Bhavani Thuraisingham, The University of Texas at Dallas

Program Chairs

David Evans, University of Virginia
Tal Malkin, Columbia University
Dongyan Xu, Purdue University

Workshop Chairs

Taesoo Kim, Georgia Tech
Cliff Wang, Army Research Office

Tutorial Chairs

Guofei Gu, Texas A&M University
Maribel Fernandez, Kings College, University of London

Poster/Demo Chairs

Kevin Hamlen, The University of Texas at Dallas
Heng Yin, University of California, Riverside

Treasurer

Alvaro Cardenas, The University of Texas at Dallas

Web Chair

JV Rajendran, Texas A&M University

Panel Chairs

Ahmad-Reza Sadeghi, TU Darmstadt, CYSEC
Yiorgos Makris, The University of Texas at Dallas

Registration Chair

Murat Kantarcioglu, The University of Texas at Dallas

Student Travel Grant Chairs

Hassan Takabi, University of North Texas
Brent Kang, KAIST
Zhi Wang, Florida State University

Publicity Chairs

Yvo Desmedt, The University of Texas at Dallas
Giancarlo Pellegrino, Saarland University
Daniel Xiapu Luo, The Hong Kong Polytechnic University
Barbara Carminati, University of Insubria

Social Media Chairs

Siddharth Garg, New York University

Proceedings Chairs

Matthew Wright, Rochester Institute of Technology
Apu Kapadia, Indiana University Bloomington

Sponsor/Industry Outreach Chairs

Janell Straach, The University of Texas at Dallas
Peng Liu, Penn State University
Gail-Joon Ahn, Arizona State University

Local Arrangement Chairs

Zhiqiang Lin, The University of Texas at Dallas
Rhonda Walls, The University of Texas at Dallas

Volunteer Coordinator/Chair

Latifur Khan, The University of Texas at Dallas
Meera Sridhar, University of North Carolina at Charlotte

General Chair's Welcome

It is our great pleasure to welcome you to the 2017 ACM Conference on Computer and Communications Security (CCS) in Dallas, Texas. We are honored to organize ACM CCS 2017 in Dallas this year and extend our welcome to attendees from around the globe to this exciting city. We hope that you enjoy what the conference has to offer this year, both for the scientific discussions, and for the social events.

Dallas is one of the fastest growing urban areas in America, with one million residents coming to the region every seven years. It is also one of the most demographically diverse and young cities in the country, which imbues the city with a friendly, outgoing sense of hospitality and genuine civic pride. Here you will find a large collection of international corporations, nationally recognized sports teams, and world class shopping. The Dallas Arts District and the many parks and gardens throughout Dallas will provide you with opportunities to enjoy the local culture while you are here.

ACM CCS is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery. CCS brings together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results. It provides an environment to conduct intellectual discussions. From its inception, CCS has established itself as a high standard research conference in its area. Its reputation continues to grow and is reflected in the prestigious technical program of high quality papers, workshops, tutorials, panel discussion and prestigious keynote addresses.

CCS 2017 would not have been possible without the help of numerous volunteers. We first want to thank all the authors who have submitted their work to CCS – without their commitment CCS 2017 would never have been possible. We also thank the program chairs, the program committee and the entire ACM organization and SIGSAC steering committee for their dedication and commitment. Special thanks go to Ms. Rhonda Walls and her team for the wonderful handling of the organization. Last but not least, we would like to express our gratitude to our generous sponsors of the conference, listed in the program, for their valuable support.

We hope that you will find this program interesting and thought-provoking and that the conference will provide you with a valuable opportunity to share ideas with other researchers and practitioners from institutions around the world. We wish you a pleasant and enjoyable stay in Dallas, Texas.

Dr. Bhavani Thuraisingham
ACM CCS 2017 General Chair
The University of Texas at Dallas

Program Chairs' Welcome

Welcome to the 24th ACM Conference on Computer and Communications Security!

Since 1993, CCS has been the ACM's flagship conference for research in all aspects of computing and communications security and privacy. This year's conference attracted a record number of 836 reviewed research paper submissions, of which a record number of 151 papers were selected for presentation at the conference and inclusion in the proceedings.

The papers were reviewed by a Program Committee of 146 leading researchers from academia, government, and industry from around the world. Reviewing was done in three rounds, with every paper being reviewed by two PC members in the first round, and additional reviews being assigned in later rounds depending on the initial reviews. Authors had an opportunity to respond to reviews received in the first two rounds. We used a subset of PC members, designated as the Discussion Committee, to help ensure that reviewers reconsidered their reviews in light of the author responses and to facilitate substantive discussions among the reviewers. Papers were discussed extensively online in the final weeks of the review process, and late reviews were requested from both PC members and external reviewers when additional expertise or perspective was needed to reach a decision. We are extremely grateful to the PC members for all their hard work in the review process, and to the external reviewers that contributed to selecting the papers for CCS.

Before starting the review process of the 842 submissions, the PC chairs removed six papers that clearly violated submission requirements or were duplicates, leaving 836 papers to review. In general, we were lenient on the requirements, only excluding papers that appeared to deliberately disregard the submission requirements. Instead of excluding papers which carelessly deanonymized the authors, or which abused appendices in the opinion of the chairs, we redacted (by modifying the submitted PDF) the offending content and allowed the papers to be reviewed, and offered to make redacted content in appendices available to reviewers upon request.

Our review process involved three phases. In the first phase, each paper was assigned two reviewers. Following last year's practice, we adopted the Toronto Paper Matching System (TPMS) for making most of the review assignments, which were then adjusted based on technical preferences declared by reviewers. Each reviewer had about three weeks to complete reviews for around 12 papers. Based on the results of these reviews, an additional reviewer was assigned to every paper that had at least one positive-leaning review. Papers where both initial reviews were negative, but with low confidence or significant positive aspects, were also assigned additional reviews. At the conclusion of the second reviewing round, authors had an opportunity to see the initial reviews and to submit a short rebuttal. To ensure that all the authors' responses were considered seriously by the reviewers, the Discussion Committee members worked closely with the reviewers to make sure that they considered and responded to the authors' rebuttals. When reviewers could not reach an agreement, or additional expertise was needed, we solicited additional reviews. The online discussion period was vibrant and substantive, and at the end of this process, the 151 papers you find here were selected for CCS 2017.

We are grateful to all the PC members and external reviewers for their hard work and thoughtful discussions; to the General Chair, Bhavani Thuraisingham, for saving us from having to deal with anything other than the program and answering all our questions promptly and helpfully; to the Proceedings Chairs, Matthew Wright and Apu Kapadia, for all their efforts working with the publisher to produce the proceedings; to Hui Lu for managing the submission server and its interface with TPMS; and to all the authors who submitted papers to CCS.

We hope everyone finds the conference engaging, enlightening, and inspiring!

David Evans
University of Virginia

Tal Malkin
Columbia University

Dongyan Xu
Purdue University

ACM CCS 2017 Program Committee Co-Chairs

Tuesday, October 31st, 2017, 9:00 a.m., Keynote, Dallas Ballroom BC

David Wagner
Professor, Computer Science Division
University of California, Berkeley

Security and Machine Learning

Machine learning has seen increasing use for a wide range of practical applications. What are the security implications of relying upon machine learning in these settings? Recent research suggests that modern machine learning methods are fragile and easily attacked, which raises concerns about their use in security-critical settings. This talk will explore several attacks on machine learning and survey directions for making machine learning more robust against attack.

David Wagner is Professor of Computer Science at the University of California at Berkeley. He has published over 100 peer-reviewed papers in the scientific literature and has co-authored two books on encryption and computer security. His research has analyzed and contributed to the security of cellular networks, 802.11 wireless networks, electronic voting systems, and other widely deployed systems.

Overview

Cache Side Channels: State-of-the-Art and Research Opportunities

Tuesday, October 31st, 10:45am – 12:15pm, Dallas Ballroom D3
Yinqian Zhang (Ohio State University)

Cliptography: Post-Snowden Cryptography

Tuesday, October 31st, 1:45pm – 5:00pm, Dallas Ballroom D3
Qiang Tang (New Jersey Institute of Technology), Moti Yung (Snap, Inc. & Columbia University)

Identity-related Threats, Vulnerabilities, and Risks Mitigation in Online Social Networks

Wednesday, November 1st, 11:00am – 12:30pm, Dallas Ballroom D3
Leila Bahri (Royal Institute of Technology, Sweden)

Web Tracking Technologies and Protection Mechanisms

Wednesday, November 1st, 1:45pm – 5:00pm, Dallas Ballroom D3
Nataliia Bielova (Inria, France)

SGX Security and Privacy

Thursday, November 2nd, 9:00am – 12:30pm, Dallas Ballroom D3
Taesoo Kim (Georgia Tech), Zhiqiang Lin (UT Dallas), Chia-Che Tsai (UC Berkeley/Texas A&M University)

Private Information Retrieval

Thursday, November 2nd, 2:00pm – 5:00pm, Dallas Ballroom D3
Ryan Henry (Indiana University)

Tuesday, October 31, 10:45 a.m. – 12:15 p.m., Dallas Ballroom D3

Yinqian Zhang *(Ohio State University)*

Cache Side-Channels: State-of-the-Art and Research Opportunities

Abstract: Cache side-channels are a type of attack vectors through which an adversary infers secret information of a running program by observing its use of CPU caches or other caching hardware. The study of cache side channels, particularly access-driven cache side channels, is gaining traction among security researchers in recent years. A large volume of papers on cache side-channel attacks or defenses is being published in both security and computer architecture conferences each year. However, due to the diversity of the research goals, methods, and perspectives, it becomes much harder for researchers new to this field to keep track of the frontiers of this research topic. As such, in this tutorial, we will provide a high-level overview of the studies of cache side-channels to help other security researchers to comprehend the state-of-the-art of this research area, and to identify research problems that have not been addressed by the community. We also hope to bridge the gap between the security community and the computer architecture community on this specific research topic by summarizing research papers from both sides.

Biography: **Dr. Yinqian Zhang** is an assistant professor of the Department of Computer Science and Engineering at The Ohio State University. He received his Ph.D. from University of North Carolina at Chapel Hill. His research interest lies in system security in general. His current research focus is side-channel attacks and defenses. In the past years, he has investigated several topics under this research theme, and published multiple research papers in top security conferences such as IEEE S&P, ACM CCS, and Usenix Security. His research has been supported by NSF. He held three U.S. patents that were derived from his previous research. In the recent years, he has served on the technical program committees of multiple security conferences, including IEEE S&P, ACM CCS, Usenix Security, and NDSS.

Tuesday, October 31, 1:45 p.m. – 5:00 p.m., Dallas Ballroom D3

Qiang Tang *(New Jersey Institute of Technology)*
Moti Yung *(Snap, Inc. & Columbia University)*

Cliptography: Post-Snowden Cryptography

Abstract: This tutorial covers a systematic overview of kleptography: stealing information subliminally from black-box cryptographic implementations; and cliptography: defending mechanisms that clip the power of kleptographic attacks via specification re-designs (without altering the underlying algorithms).

Despite the laudatory history of development of modern cryptography, applying cryptographic tools to reliably provide security and privacy in practice is notoriously difficult. One fundamental practical challenge, guaranteeing security and privacy without explicit trust in the algorithms and implementations that underlie basic security infrastructure, remains. While the dangers of entertaining adversarial implementation of cryptographic primitives seem obvious, the ramifications of such attacks are surprisingly dire: it turns out that, in wide generality, adversarial implementations of cryptographic (both deterministic and randomized) algorithms may leak private information while producing output that is statistically indistinguishable from that of a faithful implementation. Such attacks were formally studied in Kleptography.

Snowden revelations have shown us how security and privacy can be lost at a very large scale even when traditional cryptography seems to be used to protect Internet communication, when Kleptography was not taken into consideration.

We first explain how the above-mentioned Kleptographic attacks can be carried out in various settings. We then introduce several simple but rigorous immunizing strategies that were inspired by folklore practical wisdoms to protect different algorithms from implementation subversion. Those strategies can be applied to ensure security of most of the fundamental cryptographic primitives such as PRG, digital signatures, public key encryptions against kleptographic attacks when they are implemented accordingly. Our new design principles may suggest new standardization methods that help reduce the threats of subverted implementation. We also hope our tutorial stimulates community-wide efforts to further tackle this fundamental challenge.

Biography: **Qiang Tang** is an Assistant Professor at the Department of Computer Science at New Jersey Institute of Technology (NJIT). Before joining NJIT, he was a postdoctoral associate at Cornell University and was also affiliated with the Initiative of CryptoCurrency and Contracts (IC3). He obtained his PhD from the University of Connecticut with a Taylor Booth Scholarship. He also held visiting researcher positions at various institutes including the University of Wisconsin, Madison, NTT Research, Tokyo and the University of Athens, Greece. His research interests are applied and theoretical cryptography, privacy and computer security, and, in particular, post-Snowden cryptography, and blockchain technology. He has made contributions on using cryptocurrency to deter copyright infringement and to enforce key management policy, re-designing cryptographic specifications to defend against implementation subversion, as well as information theoretical security.

Moti Yung is a computer scientist whose main interests are in cryptography, security, and privacy. He is currently with Snap, Inc., and has been holding adjunct professor appointments at Columbia University where he has co-advised several Ph.D. students. He was with IBM, CertCo, RSA Lab, and Google. Dr. Yung made extensive contributions on the foundation of modern cryptography as well as innovative secure industrial technology within actual large scale systems, including the Greek National Lottery system, the security and privacy aspects of Google's global systems such as the Ad Exchange (ADX) and the ephemeral ID efforts for Google's BLE beacons, and Snap's "my eyes only memories' cloud security. Also, his invention of Cryptovirology (including Kleptography) envisioned the explosion of ransomware, and algorithm subversion on crypto systems and standards such as the Dual_EC DRNG subversion. Dr. Yung has been giving distinguished and keynote speeches at numerous top-tier crypto/security/distributed computing conferences. He is a Fellow of ACM, IEEE, IACR, and EATCS.

Wednesday, November 1, 11:00 a.m. - 12:30 p.m., Dallas Ballroom D3
Leila Bahri *(Royal Institute of Technology, Sweden)*

Identity-related Threats, Vulnerabilities, and Risks Mitigation in Online Social Networks

Abstract: The continuous increase in the numbers and sophistication levels of fake accounts in Online Social Networks (OSNs) constitutes a big threat to the privacy and to the security of honest OSN users. Uninformed OSN users could be easily fooled into accepting friendship links with fake accounts, giving them by that access to personal information they intend to exclusively share with their real friends. Moreover, these fake accounts subvert the security of the system by spreading malware, connecting with honest users for nefarious goals such as sexual harassment or child abuse, and make the social computing environment mostly untrustworthy.

There is a considerable body of work in the area of detecting fake accounts in OSNs, mostly under the research topic known as Sybil detection. One of the objectives of this tutorial is to provide a summarized but comprehensive review of the main techniques suggested for Sybil detection. The tutorial will also shed the light on the shortcomings of these methods, especially in front of more sophisticated Sybil accounts that learn general social behaviour patterns and try to imitate them. Therefore, we will also talk about the need for identity validation techniques, and present some of the available works in this direction. Overall, the tutorial's goal is to initiate the audience to the topic of Sybil detection and identity validation, to increase awareness on the privacy and security threats related to fake accounts, and on our role, both as informed OSN users and as researchers, in taking informed actions towards minimizing the effects of fake accounts.

Biography: **Leila Bahri** has a PhD in computer science from the University of Insubria in Italy. She has been a Marie-Curie research fellow under the European Commission funded project iSocial, where she has worked on designing privacy-preserving services and access control models for decentralized online social networks. Her main research work during her PhD was on decentralized privacy-preserving services for online social networks, mostly as related to identity management and validation in a user-centric and community-sourced fashions.

She is currently a postdoc researcher at the Royal Institute of Technology in Stockholm, Sweden, where she works on designing accountable data governance and privacy models that are aligned with the European GDPR. She is currently investigating topics related to the Blockchain technology and its potential in the field of privacy and trust in the social web.

Wednesday, November 1, 1:45 p.m. - 5:00 p.m., Dallas Ballroom D3
Nataliia Bielova *(Inria, France)*

Web Tracking Technologies and Protection Mechanisms

Abstract: Billions of users browse the Web on a daily basis, leaving their digital traces on millions of websites. Every such visit, every mouse move or button click may trigger a wide variety of hidden data exchanges across multiple tracking companies. As a result, these companies collect a vast amount of user's data, preferences and habits, that are extremely useful for online advertisers and profitable for data brokers, however very worrisome for the privacy of the users. In this tutorial we will cover the wide variety of Web tracking technologies, ranging from simple cookies to advanced cross-device fingerprinting. We will describe the main mechanisms behind web tracking and what users can do to protect themselves. Moreover, we will discuss solutions Web developers can use to automatically eliminate tracking from the third-party content they include in their applications. This tutorial will be of interest to a general audience of computer scientists, and we do not require any specific prerequisite knowledge for attendees.

Biography: **Nataliia Bielova** is a Research Scientist at Inria, French National Institute for Research in Computer Science and Automation. Nataliia is internationally known for her work on applying formal methods to security and privacy of web browsers. Her main interest is privacy- and transparency-enhancing technologies for Web applications. She works on measurement, detection and prevention of web tracking, including advanced behaviour-based fingerprinting. Nataliia received the French Doctoral Supervision and Research Award (PEDR) in 2017. Before obtaining her permanent position in 2013, Nataliia was a postdoctoral researcher at Inria Rennes from 2012 to 2013, where she worked on automatic detection of web tracking scripts using program analysis. She received her PhD in Computer Science from the University of Trento, Italy in 2011.

Thursday, November 2, 9:00 a.m. – 12:30 p.m., Dallas Ballroom D3

Taesoo Kim *(Georgia Tech),*
Zhiqiang Lin *(UT Dallas),*
Chia-Che Tsai *(UC Berkeley/Texas A&M University)*

SGX Security and Privacy

Abstract: In this tutorial, we will first introduce the basic concepts of Intel SGX, its development workflows, potential applications and performance characteristics. Then, we will explain known security concerns, including cache/branch side-channel attacks and memory safety issues, and corresponding defenses with various working demos. Last but not least, we will introduce various ways to quickly start writing SGX applications, specifically by utilizing library OSes or thin shielding layers; we will explain the pros and cons of each approach in terms of security and usability.

Biography: **Taesoo Kim** is an Assistant Professor in the School of Computer Science at Georgia Tech. He also serves as the director of the Georgia Tech Systems Software and Security Center (GTS3). He is interested in building a system that has underlying principles for why it should be secure. Those principles include the design of a system, analysis of its implementation, and clear separation of trusted components. His thesis work, in particular, focused on detecting and recovering from attacks on computer systems. He holds a BS from KAIST (2009), a SM (2011) and a PhD (2014) from MIT in CS.

Zhiqiang Lin is an Associate Professor of Computer Science at The University of Texas at Dallas. He earned his PhD from Computer Science Department at Purdue University in 2011. His primary research interests are systems and software security, with an emphasis on developing program analysis techniques and applying them to secure both application programs including mobile apps and the underlying system software such as Operating Systems and hypervisors. Dr. Lin is a recipient of the NSF CAREER Award and the AFOSR Young Investigator Award.

Chia-Che Tsai is a PhD candidate at Stony Brook University, and will soon join the RISE Lab at UC Berkeley as a postdoc researcher. He is also joining the Computer Science and Engineering department of Texas A&M University in Fall 2018 as a faculty. He is interested in building OSes and runtimes with a balance between usability, security, and performance. He is the main contributor to the Graphene library OS, an open-source framework for reusing unmodified Linux applications on Intel SGX and other various host options.

Thursday, November 2, 2:00 p.m. – 5:00 p.m., Dallas Ballroom D3

Ryan Henry *(Indiana University)*

Private Information Retrieval

Abstract: Private information retrieval (PIR) is a cryptographic primitive that facilitates the seemingly impossible task of letting users fetch records from untrusted and remote database servers without revealing to those servers which records are being fetched. The vast research literature on PIR spans over two decades since its 1995 introduction by Chor, Goldreich, Kushilevitz, and Sudan. The cryptography, privacy, and theoretical computer science research communities have studied PIR intensively and from a variety of perspectives. Despite a series of significant advances, most privacy practitioners and theoreticians alike fall into one of two camps: (i) those who believe that PIR is so inefficient and abstruse as to make it all-but-useless in practice, or (ii) those who remain blissfully unaware that PIR even exists.

This tutorial presents a bird's-eye overview of the current state of PIR research. Topics covered will span from purely theoretical through imminently applicable and all points in between, thereby providing participants with an awareness of what modern PIR techniques have (and do not have) to offer. This introductory tutorial will be accessible to anyone comfortable with college-level mathematics (basic linear algebra and some elementary probability and number theory).

Biography: **Ryan Henry** is an Assistant Professor in the Computer Science department at Indiana University in Bloomington, Indiana. His research explores the systems challenges of applied cryptography, with an emphasis on using cryptography to build secure systems that preserve the privacy of their users. In addition to designing and analyzing privacy-enhancing systems, Professor Henry is interested in practical matters like implementing and working toward the deployment of such systems, as well as more theoretical matters like devising number-theoretic attacks against non-standard cryptographic assumptions and developing new models and theories to understand just how efficient "heavy-weight" cryptographic primitives can be. He received his MMath (2010) and PhD (2014) from the University of Waterloo, where he held a Vanier Canada Graduate Scholarship (Vanier CGS), the most prestigious graduate scholarship in Canada. He has published several papers on PIR at top research venues (e.g., CCS, NDSS, and PETS), is a contributor to Percy++ (an open-source implementation of PIR protocols in C++), and two of his three active NSF grants heavily involve PIR research.

Wednesday, November 1, 5:15 p.m. - 6:45 p.m., Dallas Ballroom BC

The AI-Industrial Complex: The Challenge of AI Ethics

It took almost 20 years for Artificial Intelligent (AI) hype to strike back. AI systems are becoming reality and deployed in various application domains, ranging from social networks and ad targeting to autonomous vehicles and precision medicine. AI promises many benefits by improving accuracy, efficiency and safety of systems. Consulting companies make up new AI growth prognoses and statistics (as they do for every other hype). As the public and industrial funding in this field is increasing more and more, researchers and enterprises, particularly startup companies, are jumping on the AI train. AI will have a significant societal impact for which service providers with their huge user and data base will play a key and even more dominant role.

Much has been said and written in the recent past about benefits and hazards of AI. On one hand, AI presents a variety of security, privacy and safety challenges, such as opaque and biased decision-making, vulnerability to (input-oriented) attacks, violating privacy, sophisticated surveillance, trapping users into echo chambers in social networks, cyber deception, or malicious/faulty autonomous vehicle and weapon systems, to name a few. Indeed these issues and concerns have re-initiated the public debate as well as a number of initiatives on "AI Ethics" which has already become an active research field with rapid growth in research funding worldwide.

On the other hand, AI advocates point to many benefits of AI and in particular to its usefulness for enhancing cybersecurity, privacy as well as cyber safety of individuals, such as identifying attack patterns, improving the accuracy and false reject rates of automated approvals in payment systems, identifying hate speech and cyberbullying in online social networks, or highlighting fake news, etc.

This expert panel aims to discuss promises, pitfalls and ethics of AI, as well as future research directions in this fascinating area. Specifically, the panel will briefly discuss AI's compliance with possible regulations (e.g., Data Protection Regulation (GDPR) that is on the verge of being implemented).

PANEL CHAIR

Ahmad-Reza Sadeghi is a Professor of Computer Science at the Technische Universität Darmstadt, in Germany, where he heads the Scientific Excellence Team of the Cybersecurity center TU Darmstadt (CYSEC). Since January 2012 he is also the Director of Intel Collaborative Research Institute for Secure Computing (ICRI-SC) at TU Darmstadt. He received his PhD in Computer Science with the focus on privacy protecting cryptographic protocols and systems from the University of Saarland in Saarbrücken, Germany. Prior to academia, he worked in Research and Development of Telecommunications enterprises, and Ericson Telecommunications amongst others. He has been leading and involved in a variety of national and international research and development projects on design and implementation of Trustworthy Computing Platforms and Trusted Computing, Security Hardware, and Applied Cryptography. He has been serving as general or program chair as well as program committee member of major conferences and workshops in Information Security and Privacy. He is Editor-In-Chief of IEEE Security and Privacy Magazine, and on the editorial board of ACM Books. He served 5 years on the editorial board of the ACM Transactions on Information and System Security (TISSEC), and was guest editor of the IEEE Transactions on Computer-Aided Design (Special Issue on Hardware Security and Trust).

PANELISTS

John C. Havens is the Executive Director of The IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems. The IEEE Global AI Ethics Initiative has two primary outputs – the creation and iteration of a body of work known as Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Artificial Intelligence and Autonomous Systems and the identification and recommendation of ideas for Standards Projects focused on prioritizing ethical considerations in AI/AS. Currently there are eleven approved Standards Working Groups in the IEEE P7000™ series. Guided by over two hundred fifty thought leaders, The IEEE Global AI Ethics Initiative's mission is to ensure every stakeholder involved in the design and development of autonomous and intelligent systems is educated, trained, and empowered to prioritize ethical considerations so that these technologies are advanced for the benefit of humanity. John is also a regular contributor on issues of technology and well-being to Mashable, The Guardian, HuffPo and TechCrunch and is author of the books, *Heartificial Intelligence: Embracing Our Humanity To Maximize Machines* and *Hacking Happiness: Why Your Personal Data Counts and How Tracking it Can Change the World* (both published by TarcherPerigee, an imprint of Penguin Random House). John was an EVP of a Top Ten PR Firm, a VP of a tech startup, and an independent consultant where he has worked with clients such as Gillette, P&G, HP, Wal-Mart, Ford, Allstate, Monster, Gallo Wines, and Merck. He is also the founder of The Happathon

Project, a non-profit utilizing emerging technology and positive psychology to increase human well-being. John has spoken at TEDx, at SXSW Interactive (six times), and as a global keynote speaker for clients like Cisco, Gillette, IEEE, and NXP Semiconductors. John was also a professional actor on Broadway, TV and Film for fifteen years.

Heather Patterson is a Senior Research Scientist at Intel Labs, where she explores the ethics, politics, and social dynamics of emerging technologies. Trained as a cognitive scientist (Ph.D., University of Washington 2006) and privacy and technology lawyer (J.D., University of California, Berkeley 2012), her current focus is on building transparency, privacy, and accountability into technical systems in order to honor user information flow preferences and build trust. Dr. Patterson also holds an affiliate privacy scholar position at New York University's Information Law Institute.

Dr. Arthur J. Redfern is Manager of the Machine Leaning Lab, Texas Instruments, USA. He received a B.S. in 1995 from the University of Virginia and a M.S. and Ph.D. in 1996 and 1999, respectively, from the Georgia Institute of Technology, all in electrical engineering. Following his thesis work on nonlinear systems modeled by the Volterra series, Arthur joined Texas Instruments. His activities at TI have spanned the areas of machine learning (convolutional neural network based automotive and industrial applications, software libraries and hardware design), high performance computing (software libraries), signal processing for analog systems (ADCs, amplifiers, DACs, design optimization, speakers and touch screens) and communication system design (DSL, DTV and SerDes). He has over 20 papers published in refereed conferences and journals and has been granted over 20 US patents.

Dr. Howard Shrobe is a Principal Research Scientist at MIT's Computer Science and Artificial Intelligence Laboratory. He received his BS in Math from Yale College in 1968 and his MS (75) and PhD (78) from MIT. He has been a member of the research staff since 1978, but has also served as Technical Director and VP of Technology at Symbolics, Inc. (which made an advanced computer for AI research in the 1980's and 1990's). He also served as a program manager at DARPA sponsoring research in software engineering, AI, and computer security. He has served as Associate Director of the MIT AI lab (a predecessor of CSAIL) and of CSAIL. He currently is the Director of CyberSecuirty@CSAIL, a partnership between CSAIL and a group of corporate affiliates.

Dr. Cliff Wang is the Director of the Computing Sciences division at US Army Research Office. He graduated from North Carolina State University with a PhD in computer engineering in 1996. He has been carrying out research in the area of computer vision, medical imaging, high speed networks, and most recently information security. Dr. Wang authored/co-edited 15 books in the area of information security and holds 4 US patents on information security system development. Since 2003, Dr. Wang has been managing the extramural research portfolio on information assurance at the US Army Research Office. In 2007 he was selected as the director of the computing sciences division at ARO while at the same time managing his program in cyber security. For the past ten years, Dr. Wang managed over $200M in research funding which led to significant technology breakthroughs. Dr. Wang also holds an adjunct faculty position at both the Department of Computer Science and the Department of Electrical and Computer Engineering at North Carolina State University. He is a fellow of IEEE.

Dr. Susanne Wetzel is the NSF Program Director for the Secure and Trustworthy Cyberspace (SaTC) program. She recently joined the National Science Foundation (NSF) as Program Director for the Secure and Trustworthy Cyberspace (SaTC) program. She is also a Professor in the Computer Science Department at Stevens Institute of Technology, where she leads a broad research program in cybersecurity and algorithmic number theory. Dr. Wetzel has contributed to research advances in secure multi-party computation (with applications in bartering, reconciliation, electronic voting, and auctions), wireless security, privacy, biometrics, security economics, and lattice-based cryptography. She developed and directed the department's undergraduate degree program in cybersecurity which graduated its first class in Spring 2011. Until joining NSF, Dr. Wetzel also headed the Stevens' Cybercorps®: Scholarship for Service program. Her work in cybersecurity education and research has been supported by grants from NSF, DHS, and DoD. Dr. Wetzel received her Diploma in Computer Science from the University of Karlsruhe (Germany) and her Ph.D. in Computer Science from the Saarland University (Germany).

MAIN CONFERENCE AGENDA, TUESDAY, OCTOBER 31, 2017

TIME	TRACK 1 Dallas A1 Ballroom	TRACK 2 Dallas Ballroom A2	TRACK 3 Dallas Ballroom A3	TRACK 4 Dallas Ballroom D1	TRACK 5 Dallas Ballroom D2	TUTORIAL Dallas Ballroom D3
7:30-9:00	Breakfast & Registration					
9:00-9:15	**Chairs' Welcome, Dallas Ballroom BC**					
9:15-10:30	**Keynote by Prof. David Wagner (UC Berkeley) "Security and Machine Learning"**					
10:30-10:45	Coffee Break					
10:45-12:15	**1A: Multi-Party Computation** **DUPLO: Unifying Cut-and-Choose for Garbled Circuits** *Vladimir Kolesnikov (Bell Labs); Jesper Buus Nielsen (Aarhus University); Mike Rosulek and Ni Trieu (Oregon State University); Roberto Trifiletti (Aarhus University)* **Authenticated Garbling and Efficient Maliciously Secure Two-Party Computation** *Xiao Wang (University of Maryland); Samuel Ranellucci (University of Maryland/George Mason University); Jonathan Katz (University of Maryland)* **Global-Scale Secure Multiparty Computation** *Xiao Wang (University of Maryland); Samuel Ranellucci (University of Maryland/George Mason University); Jonathan Katz (University of Maryland)*	**2A: Human Authentication** **Hearing Your Voice Is Not Enough: An Articulatory Gesture Based Liveness Detection for Voice Authentication** *Linghan Zhang, Sheng Tan, and Jie Yang (Florida State University* **VibWrite: Towards Finger-input Authentication on Ubiquitous Surfaces via Physical Vibration** *Jian Liu, Chen Wang, and Yingying Chen (Rutgers University); Nitesh Saxena (University of Alabama at Birmingham)* **Presence Attestation: The Missing Link In Dynamic Trust Bootstrapping** *Zhangkai Zhang (Beihang University); Xuhua Ding (Singapore Management University); Gene Tsudik (University of California, Irvine); Jinhua Cui (Singapore Management University); Zhoujun Li (Beihang University)*	**3A: Adversial Machine Learning** **Evading Classifiers by Morphing in the Dark** *Hung Dang, Yue Huang, and Ee-Chien Chang (National University of Singapore)* **MagNet: a Two-Pronged Defense Against Adversarial Examples** *Dongyu Meng (ShanghaiTech University); Hao Chen (University of California, Davis)* **DolphinAttack: Inaudible Voice Commands** *Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu (Zhejiang University)*	**4A: Browsers** **Hindsight: Understanding the Evolution of UI Vulnerabilities in Mobile Browsers** *Meng Luo, Oleksii Starov, Nima Honarmand, and Nick Nikiforakis (Stony Brook University)* **Deterministic Browser** *Yinzhi Cao, Zhanhao Chen, Song Li, and Shujiang Wu (Lehigh University)* **Most Websites Don't Need to Vibrate: A Cost-Benefit Approach to Improving Browser Security** *Peter Snyder, Cynthia Taylor, and Chris Kanich (University of Illinois at Chicago)*	**5A: Cryptocurrency** **Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin** *Yujin Kwon, Dohyun Kim, and Yunmok Son (KAIST); Eugene Vasserman (Kansas State University); Yongdae Kim (KAIST)* **Betrayal, Distrust, and Rationality: Smart Counter-Collusion Contracts for Verifiable Cloud Computing** *Changyu Dong, Yilei Wang, Amjad Aldweesh, Patrick McCorry, and Aad van Moorsel (Newcastle University)* **Zero-Knowledge Contingent Payments Revisited: Attacks and Payments for Services** *Matteo Campanelli and Rosario Gennaro (City College of New York); Steven Goldfeder (Princeton University); Luca Nizzardo (IMDEA Software Institute and Universidad Politécnica de Madrid)*	**Tutorial (10:45-12:15)** **Cache Side Channels: State-of-the-Art and Research Opportunities** *Yinqian Zhang (Ohio State University)*
12:15-1:45	Lunch Break					

MAIN CONFERENCE AGENDA, TUESDAY, OCTOBER 31, 2017

TIME	TRACK 1 Dallas Ballroom A1	TRACK 2 Dallas Ballroom A2	TRACK 3 Dallas Ballroom A3	TRACK 4 Dallas Ballroom D1	TRACK 5 Dallas Ballroom D2	TUTORIAL Dallas Ballroom D3
1:45-3:15	**1B: Multi-Party Computation** **Pool: Scalable On-Demand Secure Computation Service Against Malicious Adversaries** *Ruiyu Zhu and Yan Huang (Indiana University); Darion Cassel (Carnegie Mellon University)* **A Framework for Constructing Fast MPC Over Arithmetic Circuits with Malicious Adversaries and an Honest-Majority** *Yehuda Lindell and Ariel Nof (Bar-Ilan University)* **Efficient, Constant-Round and Actively Secure MPC: Beyond the Three-Party Case** *Nishanth Chandran (Microsoft Research India); Juan Garay (Texas A&M University); Payman Mohassel (Visa Research); Satyanarayana Vusirikala (Microsoft Research India)*	**2B: Passwords** **Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat** *Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor (Carnegie Mellon University); Serge Egelman (University of California, Berkeley); Alain Forget (Google)* **Why Do Developers Get Password Storage Wrong? A Qualitative Usability Study** *Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, Marco Herzog, Sergej Dechand, and Matthew Smith (University of Bonn)* **The TypTop System: Personalized Typo-tolerant Password Checking** *Rahul Chatterjee (Cornell Tech); Joanne Woodage (Royal Holloway, University of London); Yuval Pnueli (Technion - Israel Institute of Technology); Anusha Chowdhury (Cornell University); Thomas Ristenpart (Cornell Tech)*	**3B: Investigating Attacks** **Rise of the HaCRS: Augmenting Autonomous Cyber Reasoning Systems with Human Assistance** *Yan Shoshitaishvili (Arizona State University); Michael Weissbacher (Northeastern University); Lukas Dresel, Christopher Salls, Ruoyu Wang, Christopher Kruegel, and Giovanni Vigna (University of California, Santa Barbara)* **Neural Network-based Graph Embedding for Cross-Platform Binary Code Similarity Detection** *Xiaojun Xu (Shanghai Jiao Tong University); Chang Liu (University of California, Berkeley); Qian Feng (Samsung Research America); Heng Yin (University of California, Riverside); Le Song (Georgia Institute of Technology); Dawn Song (University of California, Berkeley)* **RAIN: Refinable Attack Investigation with On-demand Inter-Process Information Flow Tracking** *Yang Ji, Sangho Lee, Evan Downing, Weiren Wang, Mattia Fazzini, Taesoo Kim, Alessandro Orso, and Wenke Lee (Georgia Institute of Technology)*	**4B: Privacy Policies** **Synthesis of Probabilistic Privacy Enforcement** *Martin Kucera, Petar Tsankov, Timon Gehr, Marco Guarnieri, and Martin Vechev (ETH Zürich)* **A Type System for Privacy Properties** *Véronique Cortier (Loria, CNRS/Inria); Niklas Grimm (TU Wien); Joseph Lallemand (Loria, CNRS/Inria); Matteo Maffei (TU Wien)* **Generating Synthetic Decentralized Social Graphs with Local Differential Privacy** *Zhan Qin (State University of New York at Buffalo); Yin Yang (College of Science and Engineering, Hamad Bin Khalifa University); Ting Yu (Qatar Computing Research Institute, Hamad Bin Khalifa University); Xiaokui Xiao (Nanyang Technological University); Issa Khalil (Qatar Computing Research Institute, Hamad Bin Khalifa University); Kui Ren (State University of New York at Buffalo)*	**5B: Blockchains** **Revive: Rebalancing Off-Blockchain Payment Networks** *Rami Khalil and Arthur Gervais (ETH Zürich)* **Concurrency and Privacy with Payment-Channel Networks** *Giulio Malavolta (Friedrich-Alexander University Erlangen Nuernberg); Pedro Moreno-Sanchez and Aniket Kate (Purdue University); Matteo Maffei (TU Wien); Srivatsan Ravi (University of Southern California)* **Bolt: Anonymous Payment Channels for Decentralized Currencies** *Matthew Green and Ian Miers (Johns Hopkins University)*	**Tutorial (1:45-5:15)** **Cliptography: Post-Snowden Cryptography** *Qiang Tang (New Jersey Institute of Technology), Moti Yung (Snap, Inc,/ Columbia University)*
3:15-3:45	Coffee Break					

MAIN CONFERENCE AGENDA, TUESDAY, OCTOBER 31, 2017

TIME	TRACK 1 Dallas Ballroom A1	TRACK 2 Dallas Ballroom A2	TRACK 3 Dallas Ballroom A3	TRACK 4 Dallas Ballroom D1	TRACK 5 Dallas Ballroom D2	TUTORIAL Dallas Ballroom D3
3:45-5:15	**1C: Oblivious RAM** **S3ORAM: A Computation-Efficient and Constant Client Bandwidth Blowup ORAM with Shamir Secret Sharing** *Thang Hoang, Ceyhun D. Ozkaptan, and Attila A. Yavuz (Oregon State University); Jorge Guajardo (Robert Bosch Research and Technology Center); Tam Nguyen (Oregon State University)* **Deterministic, Stash-Free Write-Only ORAM** *Daniel S. Roche, Adam J. Aviv, Seung Geol Choi, and Travis Mayberry (United States Naval Academy)* **Scaling ORAM for Secure Computation** *Jack Doerner and abhi shelat (Northeastern University)*	**2C: World Wide Web Of Wickedness** **Don't Let One Rotten Apple Spoil the Whole Barrel: Towards Automated Detection of Shadowed Domains** *Daiping Liu (University of Delaware); Zhou Li (ACM Member); Kun Du (Tsinghua University); Haining Wang (University of Delaware); Baojun Liu and Haixin Duan (Tsinghua University)* **Herding Vulnerable Cats: A Statistical Approach to Disentangle Joint Responsibility for Web Security in Shared Hosting** *Samaneh Tajalizadehkhoob (Delft University of Technology); Tom van Goethem (KU Leuven, imec-DistriNet); Maciej Korczyński and Arman Noroozian (Delft University of Technology); Rainer Böhme (Innsbruck University); Tyler Moore (The University of Tulsa); Wouter Joosen (KU Leuven, imec-DistriNet); Michel van Eeten (Delft University of Technology)* **Hiding in Plain Sight: A Longitudinal Study of Combosquatting Abuse** *Panagiotis Kintis (Georgia Institute of Technology); Najmeh Miramirkhani (Stony Brook University); Charles Lever, Yizheng Chen, and Rosa Romero-Gómez (Georgia Institute of Technology); Nikolaos Pitropakis (London South Bank University); Nick Nikiforakis (Stony Brook University); Manos Antonakakis (Georgia Institute of Technology)*	**3C: Machine Learning Privacy** **Machine Learning Models that Remember Too Much** *Congzheng Song (Cornell University); Thomas Ristenpart and Vitaly Shmatikov (Cornell Tech)* **Deep Models Under the GAN: Information Leakage from Collaborative Deep Learning** *Briland Hitaj, Giuseppe Ateniese, and Fernando Perez-Cruz (Stevens Institute of Technology)* **Oblivious Neural Network Predictions via MiniONN Transformations** *Jian Liu, Mika Juuti, Yao Lu, and N. Asokan (Aalto University)*	**4C: From Verification to ABE** **Verifying Security Policies in Multi-agent Workflows with Loops** *Bernd Finkbeiner (CISPA, Saarland University); Christian Müller, Helmut Seidl, and Eugen Zalinescu (Technische Universität München)* **Attribute-Based Encryption in the Generic Group Model: Automated Proofs and New Constructions** *Miguel Ambrona (IMDEA Software Institute/Universidad Politécnica de Madrid); Gilles Barthe (IMDEA Software Institute); Romain Gay and Hoeteck Wee (ENS, Paris)* **FAME: Fast Attribute-based Message Encryption** *Shashank Agrawal (Visa Research); Melissa Chase (Microsoft Research)*	**5C: Using Blockchains** **Practical UC-Secure Delegatable Credentials with Attributes and Their Application to Blockchain** *Jan Camenisch (IBM Research - Zürich); Manu Drijvers (IBM Research - Zürich/ETH Zürich); Maria Dubovitskaya (IBM Research - Zürich)* **Solidus: Confidential Distributed Ledger Transactions via PVORM** *Ethan Cecchetti and Fan Zhang (Cornell University); Yan Ji (Cornell University); Ahmed Kosba (University of Maryland); Ari Juels (Cornell Tech, Jacobs Institute); Elaine Shi (Cornell University)* **Fairness in an Unfair World: Fair Multiparty Computation from Public Bulletin Boards** *Arka Rai Choudhuri, Matthew Green, Abhishek Jain, Gabriel Kaptchuk, and Ian Miers (Johns Hopkins University)*	**Tutorial (1:45-5:15)** **Cliptography: Post-Snowden Cryptography** *Qiang Tang (New Jersey Institute of Technology), Moti Yung (Snap. Inc,/ Columbia University)*
5:15-6:00	Break					
6:00-8:00	**WELCOME RECEPTION & POSTER SESSION**					

MAIN CONFERENCE AGENDA, WEDNESDAY, NOVEMBER 1, 2017

TIME	TRACK 1 Dallas Ballroom A1	TRACK 2 Dallas Ballroom A2	TRACK 3 Dallas Ballroom A3	TRACK 4 Dallas Ballroom D1	TRACK 5 Dallas Ballroom D2	TUTORIAL Dallas Ballroom D3
7:30-9:00	Breakfast & Registration					
9:00-10:30	**1D: Functional Encryption and Obfuscation** **5Gen-C: Multi-input Functional Encryption and Program Obfuscation for Arithmetic Circuits** *Brent Carmer (Oregon State University/Galois, Inc.); Alex J. Malozemoff (Galois, Inc.); Mariana Raykova (Yale University)* **Iron: Functional Encryption using ntel SGX** *Ben Fisch (Stanford University); Dhinakaran Vinayagamurthy (University of Waterloo); Dan Boneh (Stanford University); Sergey Gorbunov (University of Waterloo)* **Implementing BP-Obfuscation Using Graph-Induced Encoding** *Shai Halevi and Tzipora Halevi (IBM); Victor Shoup (IBM and New York University); Noah Stephens-Davidowitz (New York University)*	**2D: Vulnerable Mobile Apps** **AUTHSCOPE: Towards Automatic Discovery of Vulnerable Access Control in Online Services** *Chaoshun Zuo, Qingchuan Zhao, and Zhiqiang Lin (University of Texas at Dallas)* **Mass Discovery of Android Traffic Imprints through Instantiated Partial Execution** *Yi Chen (University of Chinese Academy of Sciences); Wei You and Yeonjoon Lee (Indiana University); Kai Chen (University of Chinese Academy of Sciences); XiaoFeng Wang (Indiana University); Wei Zou (University of Chinese Academy of Sciences* **Unleashing the Walking Dead: Understanding Cross-App Remote Infections on Mobile WebViews** *Tongxin Li (Peking University); Xueqiang Wang (Indiana University); Mingming Zha and Kai Chen (Chinese Academy of Sciences); XiaoFeng Wang and Luyi Xing (Indiana University); Xiaolong Bai (Tsinghua University); Nan Zhang (Indiana University); Xinhui Han (Peking University)*	**3D: Logical Side Channels** **May the Fourth Be With You: A Microarchitectural Side Channel Attack on Several Real-World Applications of Curve25519** *Daniel Genkin (University of Pennsylvania/University of Maryland); Luke Valenta (University of Pennsylvania); Yuval Yarom (University of Adelaide/Data61* **Stacco: Differentially Analyzing Side-Channel Traces for Detecting SSL/TLS Vulnerabilities in Secure Enclaves** *Yuan Xiao, Mengyuan Li, Sanchuan Chen, and Yinqian Zhang (The Ohio State University)* **Precise Detection of Side-Channel Vulnerabilities Using Quantitative Cartesian Hoare Logic** *Jia Chen, Yu Feng, and Isil Dillig (University of Texas at Austin)*	**4D: Crypto Primitives** **Better Than Advertised: Improved Collision-Resistance Guarantees for MD-Based Hash Functions** *Mihir Bellare, Joseph Jaeger, and Julia Len (University of California, San Diego)* **Generic Semantic Security Against a Kleptographic Adversary** *Alexander Russell (University of Connecticut); Qiang Tang (New Jersey Institute of Technology); Moti Yung (Snap, Inc./Columbia University); Hong-Sheng Zhou (Virginia Commonwealth University)* **Defending Against Key Exfiltration: Efficiency Improvements for Big-Key Cryptography via Large-Alphabet Subkey Prediction** *Mihir Bellare and Wei Dai (University of California, San Diego)*	**5D: Network Security** **Client-side Name Collision Vulnerability in the New gTLD Era: A Systematic Study** *Qi Alfred Chen (University of Michigan); Matthew Thomas and Eric Osterweil (Verisign Labs); Yulong Cao, Jie You, and Z. Morley Mao (University of Michigan)* **The Wolf of Name Street: Hijacking Domains Through Their Nameservers** *Thomas Vissers (KU Leuven, imec-DistriNet); Timothy Barron (Stony Brook University); Tom Van Goethem and Wouter Joosen (KU Leuven, imec-DistriNet); Nick Nikiforakis (Stony Brook University)* **Faulds: A Non-Parametric Iterative Classifier for Internet-Wide OS Fingerprinting** *Zain Shamsi (Texas A&M University); Daren B.H. Cline and Dmitri Loguinov (Texas A&M University)*	**Tutorial (9:00-10:30)**
10:30-11:00	Coffee Break					

MAIN CONFERENCE AGENDA, WEDNESDAY, NOVEMBER 1, 2017

TIME	TRACK 1 Dallas Ballroom A1	TRACK 2 Dallas Ballroom A2	TRACK 3 Dallas Ballroom A3	TRACK 4 Dallas Ballroom D1	TRACK 5 Dallas Ballroom D2	TUTORIAL Dallas Ballroom D3
11:00-12:30	**1E: Hardening Crypto** **T/Key: Second-Factor Authentication From Secure Hash Chains** *Dmitry Kogan, Nathan Manohar, and Dan Boneh (Stanford University)* **Practical Graphs for Optimal Side-Channel Resistant Memory-Hard Functions** *Joel Alwen (IST Austria); Jeremiah Blocki and Ben Harsha (Purdue University)* **Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation** *Shay Gueron (Haifa University/ AWS); Yehuda Lindell (Bar-Ilan University)*	**2E: Securing Mobile Apps** **The ART of App Compartmentalization: Compiler-based Library Privilege Separation on Stock Android** *Jie Huang, Oliver Schranz, Sven Bugiel, and Michael Backes (CISPA, Saarland University)* **Vulnerable Implicit Service: A Revisit** *Lingguang Lei (Chinese Academy of Sciences, Institute of Information Engineering/ George Mason University); Yi He (Tsinghua University); Kun Sun (George Mason University); Jiwu Jing and Yuewu Wang (Chinese Academy of Sciences, Institute of Information Engineering); Qi Li (Tsinghua University); Jian Weng (Jinan University)* **A Stitch in Time: Supporting Android Developers in Writing Secure Code** *Duc Cuong Nguyen (CISPA, Saarland University); Dominik Wermke (Leibniz University Hannover); Yasemin Acar (Leibniz University Hannover); Michael Backes (CISPA, Saarland University); Charles Weir (Security Lancaster, Lancaster University); Sascha Fahl (Leibniz University Hannover)*	**3E: Physical Side Channels** **Exploiting a Thermal Side Channel for Power Attacks in Multi-Tenant Data Centers** *Mohammad A. Islam and Shaolei Ren (University of California, Riverside); Adam Wierman (California Institute of Technology)* **Watch Me, But Don't Touch Me! Contactless Control Flow Monitoring via Electromagnetic Emanations** *Yi Han, Sriharsha Etigowni, Hua Liu, Saman Zonouz, and Athina Petropulu (Rutgers University)* **Viden: Attacker Identification on In-Vehicle Networks** *Kyong-Tak Cho and Kang G. Shin (University of Michigan)*	**4E: Adversarial Social Networking** **Practical Attacks Against Graph-based Clustering** *Yizheng Chen, Yacin Nadji, and Athanasios Kountouras (Georgia Institute of Technology); Fabian Monrose (University of North Carolina at Chapel Hill); Roberto Perdisci (University of Georgia); Manos Antonakakis (Georgia Institute of Technology); Nikolaos Vasiloglou (Symantec)* **Automated Crowdturfing Attacks and Defenses in Online Review Systems** *Yuanshun Yao, Bimal Viswanath, Jenna Cryan, Haitao Zheng, and Ben Y. Zhao (University of Chicago)* **POISED: Spotting Twitter Spam Off the Beaten Paths** *Shirin Nilizadeh (University of California, Santa Barbara); François Labrèche (École Polytechnique de Montréal); Alireza Sadighian (École Polytechnique de Montréal); Ali Zand (University of California, Santa Barbara); José Fernandez (École Polytechnique de Montréal); Christopher Kruegel (University of California, Santa Barbara); Gianluca Stringhini (University College London); Giovanni Vigna (University of California, Santa Barbara)*	**5E: Privacy-Preserving Analytics** **Practical Secure Aggregation for Privacy-Preserving Machine Learning** *Keith Bonawitz, Vladimir Ivanov, and Ben Kreuter (Google); Antonio Marcedone (Cornell University); H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth (Google)* **Use Privacy in Data-Driven Systems: Theory and Experiments with Machine Learnt Programs** *Anupam Datta, Matthew Fredrikson, Gihyuk Ko, Piotr Mardziel, and Shayak Sen (Carnegie Mellon University)* **A Practical Encrypted Data Analytic Framework With Trusted Processors** *Fahad Shaon, Murat Kantarcioglu, Zhiqiang Lin, and Latifur Khan (University of Texas at Dallas)*	**Tutorial (11:00-12:30)** **Identity-related Threats, Vulnerabilities, and Risks Mitigation in Online Social Networks** *Leila Bahri (Royal Institute of Technology, Sweden)*
12:30-2:00	Lunch Break					

MAIN CONFERENCE AGENDA, WEDNESDAY, NOVEMBER 1, 2017

TIME	TRACK 1 Dallas Ballroom A1	TRACK 2 Dallas Ballroom A2	TRACK 3 Dallas Ballroom A3	TRACK 4 Dallas Ballroom D1	TRACK 5 Dallas Ballroom D2	TUTORIAL Dallas Ballroom D3
2:00-3:30	**1F: Private Set Intersection** **Malicious-Secure Private Set Intersection via Dual Execution** *Peter Rindal and Mike Rosulek (Oregon State University)* **Fast Private Set Intersection from Homomorphic Encryption** *Hao Chen and Kim Laine (Microsoft Research); Peter Rindal (Oregon State University)* **Practical Multi-party Private Set Intersection from Symmetric-Key Techniques** *Vladimir Kolesnikov (Bell Labs); Naor Matania and Benny Pinkas (Bar-Ilan University); Mike Rosulek and Ni Trieu (Oregon State University)*	**2F: Insights from Log (in)s** **Detecting Structurally Anomalous Logins Within Enterprise Networks** *Hossein Siadati and Nasir Memon (New York University)* **DeepLog: Anomaly Detection and Diagnosis from System Logs Through Deep Learning** *Min Du, Feifei Li, Guineng Zheng, and Vivek Srikumar (University of Utah)* **Predicting the Risk of Cyber Incidents** *Leyla Bilge, Yufei Han, and Matteo Dell'Amico (Symantec Research Labs)*	**3F: Crypto Pitfalls** **Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2** *Mathy Vanhoef and Frank Piessens (KU Leuven, imec-DistriNet)* **CCCP: Closed Caption Crypto Phones to Resist MITM Attacks, Human Errors and Click-Through** *Maliheh Shirvanian and Nitesh Saxena (University of Alabama at Birmingham)* **No-Match Attacks and Robust Partnering Definitions — Defining Trivial Attacks for Security Protocols is Not Trivial** *Yong Li (Huawei Technologies Düsseldorf); Sven Schäge (Ruhr-Universität Bochum)*	**4F: Private Queries** **Querying for Queries: Indexes of Queries for Efficient and Expressive IT-PIR** *Syed Mahbub Hafiz and Ryan Henry (Indiana University)* **PeGaSus: Data-Adaptive Differentially Private Stream Processing** *Yan Chen and Ashwin Machanavajjhala (Duke University); Michael Hay (Colgate University); Gerome Miklau (University of Massachusetts Amherst)* **Composing Differential Privacy and Secure Computation: A Case Study on Scaling Private Record Linkage** *Xi He and Ashwin Machanavajjhala (Duke University); Cheryl Flynn and Divesh Srivastava (AT&T Labs-Research)*	**5F: Understanding Security Fails** **Where the Wild Warnings Are: Root Causes of Chrome HTTPS Certificate Errors** *Mustafa Emre Acer, Emily Stark, and Adrienne Porter Felt (Google); Sascha Fahl (Leibniz University Hannover); Radhika Bhargava (Purdue University); Bhanu Dev (International Institute of Information Technology Hyderabad); Matt Braithwaite, Ryan Sleevi, and Parisa Tabriz (Google)* **Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials** *Kurt Thomas (Google); Frank Li (University of California, Berkeley); Ali Zand, Jake Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, and Dan Margolis (Google); Vern Paxson (University of California, Berkeley); Elie Bursztein (Google)* **Certified Malware: Measuring Breaches of Trust in the Windows Code-Signing PKI** *Doowon Kim, Bum Jun Kwon, and Tudor Dumitraş (University of Maryland)*	**Tutorial (1:45-5:00)** **Web Tracking Technologies and Protection Mechanisms** *Nataliia Bielova (Inria, France)*
3:30-4:00	Coffee Break					

MAIN CONFERENCE AGENDA, WEDNESDAY, NOVEMBER 1, 2017

TIME	TRACK 1 Dallas Ballroom A1	TRACK 2 Dallas Ballroom A2	TRACK 3 Dallas Ballroom A3	TRACK 4 Dallas Ballroom D1	TRACK 5 Dallas Ballroom D2	TUTORIAL Dallas Ballroom D3
4:00-5:00	**1G: Searchable Encryption** **Forward Secure Dynamic Searchable Symmetric Encryption with Efficient Updates** *Kee Sung Kim, Minkyu Kim, Dongsoo Lee, Je Hong Park, and Woo-Hwan Kim (National Security Research Institute)* **Forward and Backward Private Searchable Encryption from Constrained Cryptographic Primitives** *Raphael Bost (Direction Générale de l'Armement - Maitrise de l'Information/Université de Rennes 1); Brice Minaud (Royal Holloway, University of London); Olga Ohrimenko (Microsoft Research, Cambridge)*	**2G: Bug Hunting Risks and Rewards** **Economic Factors of Vulnerability Trade and Exploitation: Empirical evidence from a prominent Russian cybercrime market** *Luca Allodi (Eindhoven University of Technology)* **Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research** *Alexander Gamero-Garrido, Stefan Savage, Kirill Levchenko, and Alex C. Snoeren (University of California, San Diego)*	**3G: Crypto Standards** **Identity-Based Format-Preserving Encryption** *Mihir Bellare (University of California, San Diego); Viet Tung Hoang (Florida State University)* **Standardizing Bad Cryptographic Practice - A teardown of the IEEE standard for protecting electronic-design intellectual property** *Animesh Chhotaray, Adib Nahiyan, Thomas Shrimpton, Domenic J Forte, and Mark Tehranipoor (University of Florida)*	**4G: Voting** **New Techniques for Structural Batch Verification in Bilinear Groups with Applications to Groth-Sahai Proofs** *Gottfried Herold (ENS Lyon); Max Hoffmann (Ruhr-Universität Bochum); Michael Klooß (Karlsruhe Institute of Technology); Carla Ràfols (UPF Barcelona); Andy Rupp (Karlsruhe Institute of Technology)* **Practical Quantum-Safe Voting from Lattices** *Rafael del Pino, Vadim Lyubashevsky, Gregory Neven, and Gregor Seiler (IBM Research - Zürich)*	**5G: Hardening Hardware** **A Touch of Evil: High-Assurance Cryptographic Hardware from Untrusted Components** *Vasilios Mavroudis and Andrea Cerulli (University College London); Petr Svenda (Masaryk University); Dan Cvrcek and Dusan Klinec (EnigmaBridge); George Danezis (University College London)* **Provably-Secure Logic Locking: From Theory To Practice** *Muhammad Yasin, Abhrajit Sengupta, Mohammed Thari Nabeel, Mohammed Ashraf (New York University); Jeyavijayan JV Rajendran (University of Texas at Dallas); Ozgur Sinanoglu (New York University)*	**Tutorial (1:45-5:00)** **Web Tracking Technologies and Protection Mechanisms** *Nataliia Bielova (Inria, France)*
5:00-5:15	Break					
5:15-6:45	**Discussion Panel, Dallas Ballroom BC**					
6:45-7:00	Break					
7:00-9:00	**Award Ceremony and Banquet**					

MAIN CONFERENCE AGENDA, THURSDAY, NOVEMBER 2, 2017

TIME	TRACK 1 Dallas Ballroom A1	TRACK 2 Dallas Ballroom A2	TRACK 3 Dallas Ballroom A3	TRACK 4 Dallas Ballroom D1	TRACK 5 Dallas Ballroom D2	TUTORIAL Dallas Ballroom D3
7:30-9:00	Breakfast & Registration					
9:00-10:30	**1H: Crypto Attacks** **The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli** *Matus Nemec (Masaryk University/ Ca' Foscari University of Venice); Marek Sys and Petr Svenda (Masaryk University); Dusan Klinec (Masaryk University/EnigmaBridge); Vashek Matyas (Masaryk University)* **Algorithm Substitution Attacks from a Steganographic Perspective** *Sebastian Berndt and Maciej Liskiewicz (University of Luebeck)* **On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs** *Shahin Tajik, Heiko Lohrke, Jean-Pierre Seifert, and Christian Boit (Technische Universität Berlin)*	**2H: Code Reuse Attacks** **The Dynamics of Innocent Flesh on the Bone: Code Reuse Ten Years Later** *Victor van der Veen, Dennis Andriesse, Manolis Stamatogiannakis (Vrije Universiteit Amsterdam); Xi Chen (Vrije Universiteit Amsterdam/Microsoft); Herbert Bos, and Cristiano Giuffrida (Vrije Universiteit Amsterdam)* **Capturing Malware Propagations with Code Injections and Code-Reuse Attacks** *David Korczynski (University of Oxford); Heng Yin (University of California, Riverside)* **Code-reuse Attacks for the Web: Breaking Cross-Site Scripting Mitigations via Script Gadgets** *Sebastian Lekies and Krzysztof Kotowicz (Google); Samuel Groß (SAP SE); Eduardo Vela (Google); Martin Johns (SAP SE)*	**3H: Web Security** **Rewriting History: Changing the Archived Web from the Present** *Ada Lerner (Wellesley College); Tadayoshi Kohno, and Franziska Roesner (University of Washington)* **Deemon: Detecting CSRF with Dynamic Analysis and Property Graphs** *Giancarlo Pellegrino (CISPA, Saarland University); Martin Johns (SAP SE); Simon Koch, Michael Backes, and Christian Rossow (CISPA, Saarland University)* **Tail Attacks on Web Applications** *Huasong Shan and Qingyang Wang (Louisiana State University); Calton Pu (Georgia Institute of Technology)*	**4H: Formal Verification** **A Comprehensive Symbolic Analysis of TLS 1.3** *Cas Cremers (University of Oxford); Marko Horvat (The Max Planck Institute For Software Systems); Jonathan Hoyland, Sam Scott, and Thyla van der Merwe (Royal Holloway, University of London)* **HACL*: A Verified Modern Cryptographic Library** *Jean-Karim Zinzindohoué(Inria Paris); Karthikeyan Bhargavan (Inria Paris); Jonathan Protzenko (Microsoft Research); Benjamin Beurdouche (Inria Paris)* **Jasmin: High-Assurance and High-Speed Cryptography** *José Bacelar Almeida (HASLab -- INESC TEC/Universidade do Minho); Manuel Barbosa (HASLab -- INESC TEC/DCC FC Universidade do Porto); Gilles Barthe (IMDEA Software Institute); Arthur Blot (ENS Lyon); Benjamin Grégoire (Inria); Vincent Laporte (IMDEA Software Institute); Tiago Oliveira and Hugo Pacheco (HASLab -- INESC TEC/ Universidade do Minho); Benedikt Schmidt (IMDEA Software Institute); Pierre-Yves Strub (Ecole Polytechnique)*		**Tutorial (9:00-12:30)** **SGX Security and Privacy** *Taesoo Kim (Georgia Tech), Zhiqiang Lin (UT Dallas), Chia-Che Tsai (UC Berkeley/Texas A&M University)*
10:30-11:00	Coffee Break					

MAIN CONFERENCE AGENDA, THURSDAY, NOVEMBER 2, 2017

TIME	TRACK 1 Dallas Ballroom A1	TRACK 2 Dallas Ballroom A2	TRACK 3 Dallas Ballroom A3	TRACK 4 Dallas Ballroom D1	TRACK 5 Dallas Ballroom D2	TUTORIAL Dallas Ballroom D3
11:00-12:30	**1I: Post-Quantum** **Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives** *Melissa Chase (Microsoft Research); David Derler (Graz University of Technology); Steven Goldfeder (Princeton University); Claudio Orlandi (Aarhus University); Sebastian Ramacher (Graz University of Technology); Christian Rechberger (Graz University of Technology/Denmark Technical University); Daniel Slamanig (AIT Austrian Institute of Technology); Greg Zaverucha (Microsoft Research)* **To BLISS-B or Not to be - Attacking strongSwan's Implementation of Post-Quantum Signatures** *Peter Pessl (Graz University of Technology); Leon Groot Bruinderink (Technische Universiteit Eindhoven); Yuval Yarom (University of Adelaide/Data61)* **Side-Channel Attacks on BLISS Lattice-Based Signatures: Exploiting Branch Tracing Against strongSwan and Electromagnetic Emanations in Microcontrollers** *Thomas Espitau (UPMC); Pierre-Alain Fouque (Université de Rennes 1); Benoît Gérard (DGA.MI); Mehdi Tibouchi (NTT Secure Platform Laboratories)*	**2I: Information Flow** **Nonmalleable Information Flow Control** *Ethan Cecchetti and Andrew Myers (Cornell University); Owen Arden (University of California, Santa Cruz)* **Cryptographically Secure Information Flow Control on Key-Value Stores** *Lucas Waye, Pablo Buiras (Harvard University); Owen Arden (University of California, Santa Cruz); Alejandro Russo (Chalmers University of Technology); Stephen Chong (Harvard University)* **Object Flow Integrity** *Wenhao Wang, Xiaoyang Xu, and Kevin Hamlen (University of Texas at Dallas)*	**3I: Personal Privacy** **BBA+: Improving the Security and Applicability of Privacy-Preserving Point Collection** *Gunnar Hartung (Karlsruhe Institute of Technology); Max Hoffmann (Ruhr-Universität Bochum); Matthias Nagel and Andy Rupp (Karlsruhe Institute of Technology)* **walk2friends: Inferring Social Links from Mobility Profiles** *Michael Backes (CISPA, Saarland University); Mathias Humbert (Swiss Data Science Center, ETH/EPFL); Jun Pang (University of Luxembourg); Yang Zhang (CISPA, Saarland University)* **Back to the Drawing Board: Revisiting the Design of Optimal Location Privacy-Preserving Mechanisms** *Simon Oya (University of Vigo); Carmela Troncoso (IMDEA Software Institute); Fernando Pérez-González (University of Vigo)*	**4I: Verifying Crypto** **Certified Verification of Algebraic Properties on Low-Level Mathematical Constructs in Cryptographic Programs** *Ming-Hsien Tsai, Bow-Yaw Wang, and Bo-Yin Yang (Academia Sinica)* **A Fast and Verified Software Stack for Secure Function Evaluation** *José Bacelar Almeida (HASLab -- INESC TEC/Universidade do Minho); Manuel Barbosa (HASLab -- INESC TEC/DCC FC Universidade do Porto); Gilles Barthe (IMDEA Software Institute); François Dupressoir (University of Surrey); Benjamin Grégoire (INRIA Sophia-Antipolis); Vincent Laporte (IMDEA Software Institute); Vitor Pereira (HASLab -- INESC TEC/DCC FC Universidade do Porto)* **Verified Correctness and Security of mbedTLS HMAC-DRBG** *Katherine Q. Ye (Princeton University/Carnegie Mellon University); Matthew Green (Johns Hopkins University); Naphat Sanguansin and Lennart Beringer (Princeton University); Adam Petcher (Oracle); Andrew W. Appel (Princeton University)*	**5I: Communication Privacy** **How Unique is Your .onion? An Analysis of the Fingerprintability of Tor Onion Services** *Rebekah Overdorf (Drexel University); Marc Juarez and Gunes Acar (KU Leuven); Rachel Greenstadt (Drexel University); Claudia Diaz (KU Leuven)* **The Waterfall of Liberty: Decoy Routing Circumvention that Resists Routing Attacks** *Milad Nasr, Hadi Zolfaghari, and Amir Houmansadr (University of Massachusetts Amherst)* **Compressive Traffic Analysis: A New Paradigm for Scalable Traffic Analysis** *Milad Nasr, Amir Houmansadr, and Arya Mazumdar (University of Massachusetts Amherst)*	**Tutorial (9:00-12:30)** **SGX Security and Privacy** *Taesoo Kim (Georgia Tech), Zhiqiang Lin (UT Dallas), Chia-Che Tsai (UC Berkeley/Texas A&M University)*
12:30-2:00	Lunch Break					

MAIN CONFERENCE AGENDA, THURSDAY, NOVEMBER 2, 2017

TIME	TRACK 1 Dallas Ballroom A1	TRACK 2 Dallas Ballroom A2	TRACK 3 Dallas Ballroom A3	TRACK 4 Dallas Ballroom D1	TRACK 5 Dallas Ballroom D2	TUTORIAL Dallas Ballroom D3
2:00-3:30	**1J: Outsourcing** **Full Accounting for Verifiable Outsourcing** *Riad S. Wahby (Stanford University); Ye Ji (New York University); Andrew J. Blumberg (University of Texas at Austin); abhi shelat (Northeastern University); Justin Thaler (Georgetown University); Michael Walfish and Thomas Wies (New York University)* **Ligero: Lightweight Sublinear Arguments Without a Trusted Setup** *Scott Ames (University of Rochester); Carmit Hazay (Bar-Ilan University); Yuval Ishai (Technion/ University of California, Los Angeles); Muthuramakrishnan Venkitasubramaniam (University of Rochester)* **Homomorphic Secret Sharing: Optimizations and Applications** *Elette Boyle (IDC Herzliya); Geoffroy Couteau (ENS, Paris); Niv Gilboa (Ben Gurion University); Yuval Ishai (Technion/University of California, Los Angeles); Michele Orru (ENS, Paris)*	**2J: Fun with Fuzzing** **DIFUZE:Interface Aware Fuzzing for Kernel Drivers** *Jake Corina, Aravind Machiry, Christopher Salls (University of California, Santa Barbara); Yan Shoshitaishvili (Arizona State University); Shuang Hao (University of Texas at Dallas); Christopher Kruegel, and Giovanni Vigna (University of California, Santa Barbara)* **SemFuzz: Semantics-based Automatic Generation of Proof-of-Concept Exploits** *Wei You (Indiana University); Peiyuan Zong and Kai Chen (Chinese Academy of Sciences, Institute of Information Engineering); XiaoFeng Wang (Indiana University); Xiaojing Liao (William and Mary); Pan Bian and Bin Liang (Renmin University of China)* **SlowFuzz: Automated Domain-Independent Detection of Algorithmic Complexity Vulnerabilities** *Theofilos Petsios, Jason Zhao, Angelos D. Keromytis, and Suman Jana (Columbia University)*	**3J: Problematic Patches** **Checking Open-Source License Violation and 1-day Security Risk at Large Scale** *Ruian Duan, Ashish Bijlani, Meng Xu, Taesoo Kim, and Wenke Lee (Georgia Institute of Technology)* **Keep me Updated: An Empirical Study of Third-Party Library Updatability on Android** *Erik Derr, Sven Bugiel (CISPA, Saarland University); Sascha Fahl (Leibniz University Hannover); Yasemin Acar (Leibniz University Hannover); Michael Backes (CISPA, Saarland University)* **A Large-Scale Empirical Study of Security Patches** *Frank Li and Vern Paxson (University of California, Berkeley)*	**4J: Flash Security** **DEFTL: Implementing Plausibly Deniable Encryption in Flash Translation Layer** *Shijie Jia and Luning Xia (Chinese Academy of Sciences, Institute of Information Engineering); Bo Chen (Michigan Technological University); Peng Liu (The Pennsylvania State University, College of Information Sciences and Technology)* **FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware** *Jian Huang (Georgia Institute of Technology); Jun Xu,Xinyu Xing, and Peng Liu (The Pennsylvania State University); Moinuddin K. Qureshi (Georgia Institute of Technology)* **FirmUSB: Vetting USB Device Firmware Using Domain Informed Symbolic Execution** *Grant Hernandez, Farhaan Fowze, Dave Jing Tian, Tuba Yavuz, and Kevin Butler (University of Florida)*		**Tutorial (2:00-5:00)** **Private Information Retrieval** *Ryan Henry (Indiana University)*
3:30-4:00	Coffee Break					

MAIN CONFERENCE AGENDA, THURSDAY, NOVEMBER 2, 2017

TIME	TRACK 1 Dallas Ballroom A1	TRACK 2 Dallas Ballroom A2	TRACK 3 Dallas Ballroom A3	TRACK 4 Dallas Ballroom D1	TRACK 5 Dallas Ballroom D2	TUTORIAL Dallas Ballroom D3
4:00-5:30	**1K: Secure Computation** **TinyOLE: Efficient Actively Secure Two-Party Computation from Oblivious Linear Function Evaluation** *Nico Döttling (University of California, Berkeley); Satrajit Ghosh, Jesper Buus Nielsen, Tobias Nilges, and Roberto Trifiletti (Aarhus University)* **Distributed Measurement with Private Set-Union Cardinality** *Ellis Fenske (Tulane University); Akshaya Mani (Georgetown University); Aaron Johnson (U.S. Naval Research Lab); Micah Sherr (Georgetown University)* **Efficient Public Trace-and-Revoke from Standard Assumptions** *Shweta Agrawal (IIT Madras); Sanjay Bhattacherjee (Turing Lab, ASU, ISI Kolkata); Duong Hieu Phan (XLIM U. Limoges, CNRS, France); Damien Stehle (ENS Lyon, Laboratoire LIP U. Lyon, CNRS, ENSL, INRIA, UCBL); Shota Yamada (National Institute of Advanced Industrial Science and Technology AIST, Japan)*	**2K: Fuzzing Finer and Faster** **Designing New Operating Primitives to Improve Fuzzing Performance** *Wen Xu, Sanidhya Kashyap, Changwoo Min, and Taesoo Kim (Georgia Institute of Technology)* **Directed Greybox Fuzzing** *Marcel Böhme, Van-Thuan Pham, Manh-Dung Nguyen, and Abhik Roychoudhury (National University of Singapore)* **IMF: Inferred Model-based Fuzzer** *HyungSeok Han and Sang Kil Cha (KAIST)*	**3K: Program Analysis** **PtrSplit: Supporting General Pointers in Automatic Program Partitioning** *Shen Liu, Gang Tan, and Trent Jaeger (The Pennsylvania State University)* **HexType: Efficient Detection of Type Confusion Errors for C++** *Yuseok Jeon (Purdue University); Priyam Biswas, Scott Carr, Byoungyoung Lee, and Mathias Payer (Purdue University)* **FreeGuard: A Faster Secure Heap Allocator** *Sam Silvestro, Hongyu Liu, and Corey Crosser (University of Texas at San Antonio); Zhiqiang Lin (University of Texas at Dallas); Tongping Liu (University of Texas at San Antonio)*	**4K: Secure Enclaves** **JITGuard: Hardening Just-in-time Compilers with SGX** *Tommaso Frassetto, David Gens, Christopher Liebchen, and Ahmad-Reza Sadeghi (Technische Universität Darmstadt)* **Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX** *Wenhao Wang (Indiana University); Guoxing Chen (The Ohio State University); Xiaorui Pan (Indiana University); Yinqian Zhang (The Ohio State University); XiaoFeng Wang (Indiana University); Vincent Bindschaedler (University of Illinois at Urbana-Champaign); Haixu Tang (Indiana University); Carl A. Gunter (University of Illinois at Urbana-Champaign)* **A Formal Foundation for Secure Remote Execution of Enclaves** *Pramod Subramanyan and Rohit Sinha (University of California, Berkeley); Ilia Lebedev and Srinivas Devadas (Massachusetts Institute of Technology); Sanjit Seshia (University of California, Berkeley)*		**Tutorial (2:00-5:00)** **Private Information Retrieval** *Ryan Henry (Indiana University)*
5:30-5:45	Break					
5:45-6:30	**Business Meeting, Dallas Ballroom BC**					

POSTERS

A Comprehensive Study of Forged Certificates in the Wild
Mingxin Cui, Zigang Cao, Gang Xiong and Junzheng Shi (Institute of Information Engineering, CAS)

A PU Learning-based System for Potential Malicious URL Detection
Ya-Lin Zhang (Nanjing University), Longfei Li (Ant Financial), Jun Zhou (Ant Financial), Xiaolong Li (Ant Financial), Zhi-Hua Zhou (Nanjing University), Yujing Liu (Ant Financial) and Yuanchao Zhang (Ant Financial)

A Unified Framework of Differentially Private Synthetic Data Release with Generative Adversarial Network
Pei-Hsuan Lu and Chia-Mu Yu (National Chung Hsing University)

AFL-based Fuzzing for Java with Kelinci
Rody Kersten, Kasper Luckow, and Corina Pasareanu (CMU)

An Empirical Measurement Study on Multi-tenant Deployment Issues of CDNs
Zixi Cai, Zigang Cao, Gang Xiong, Zhen Li and Wei Xia (Institute of Information Engineering, CAS)

BGPCoin: A Trustworthy Blockchain-based Resource Management Solution for BGP Security
Qianqian Xing, Wang Baosheng and Xiaofeng Wang (National University of Defense Tech)

Covert Channel Based on the Sequential Analysis in Android Systems
Jun-Won Ho, Kyungrok Won and Jee Sun Kim (Seoul Women's University)

Cyber Attack Prediction of Threats from Unconventional Resources (CAPTURE)
Ahmet Okutan, Gordon Werner, Katie McConky and S. Jay Yang (Rochester Institute of Technology)

Detection of CPS Program Anomalies by Enforcing Cyber-Physical Execution Semantics
Long Cheng, Ke Tian and Danfeng Yao (Virginia Tech)

Evaluating Reflective Deception as a Malware Mitigation Strategy
Thomas Shaw (University of Tulsa), Jim Arrowood (Haystack Security LLC), Michael Kvasnicka (University of Tulsa), Shay Taylor (University of Tulsa), Kyle Cook (University of Tulsa) and John Hale (University of Tulsa)

Finding Vulnerabilities in P4 Programs with Assertion-based Verification
Lucas M. Freire, Miguel C. Neves, Alberto E. Schaeffer-Filho and Marinho P. Barcellos (UFRGS)

Hidden in Plain Sight: A Filesystem for Data Integrity and Confidentiality
Anne Kohlbrenner (CMU), Frederico Araujo, Teryl Taylor and Marc Stoecklin (IBM T.J. Watson)

Improving Anonymity of Services Deployed over Tor by Changing Guard Selection
Abhishek Singh (University of Oslo)

Inaudible Voice Commands
Liwei Song and Prateek Mittal (Princeton University)

Intrusion Detection System for In-vehicle Networks Using Sensor Correlation and Integration
Huaxin Li, Li Zhao, Marcio Juliato, Shabbir Ahmed, Manoj Sastry and Liuyang Lily Yang (Intel Labs)

Is Active Electromagnetic Side-channel Attack Practical?
Satohiro Wakabayashi, Seita Maruyama, Tatsuya Mori, Shigeki Goto (Waseda University), Masahiro Kinugawa (National Institute of Technology, Sendai College) and Yu-Ichi Hayashi (Nara Institute of Science and Technology)

Neural Network-based Graph Embedding for Malicious Accounts Detection
Ziqi Liu, Chaochao Chen, Jun Zhou, Xiaoling Li, Feng Xu, Tao Chen (Ant Financial), and Le Song (Georgia Tech)

PenJ1939: An Interactive Framework for Design and Dissemination of Exploits for Commercial Vehicles
Subhojeet Mukherjee, Jacob Walker, Indrajit Ray and Indrakshi Ray (Colorado State University)

Practical Fraud Transaction Prediction
Longfei Li, Jun Zhou, Xiaolong Li and Tao Chen (Ant Financial)

PriReMat: A Distributed Tool for Privacy Preserving Record Linking in Healthcare
Diptendu Kar, Ibrahim Lazrig, Indrajit Ray and Indrakshi Ray (Colorado State University)

Probing Tor Hidden Service with Dockers
Jonghyeon Park and Youngseok Lee (Chungnam National University)

Rethinking Fingerprint Identification on Smartphones
Seungyeon Kim, Hoyeon Lee and Taekyoung Kwon (Yonsei University)

Rust SGX SDK: Towards Memory Safety in Intel SGX Enclave
Yu Ding, Ran Duan, Long Li, Yueqiang Cheng, Yulong Zhang, Tanghui Chen, Tao Wei (Baidu X-Lab) and Huibo Wang (UT Dallas)

Security Evaluation of a Classifier in High-Dimensional Network Data
Muhammad Ejaz Ahmed and Hyoungshick Kim (Sungkyunkwan University)

Semi-supervised Classification for Dynamic Android Malware Detection
Li Chen, Mingwei Zhang, Chih-Yuan Yang and Ravi Sahita (Intel Lab)

TitAnt: Active Detector for Implicit Fraudulent Transactions in Alipay
Shaosheng Cao, Xinxing Yang, Jun Zhou, Xiaolong Li, Kai Xiao, Yuan Qi (Ant Financial)

TOUCHFLOOD: A Novel Class of Attacks against Capacitive Touchscreens
Seita Maruyama, Satohiro Wakabayashi and Tatsuya Mori (Waseda University)

TouchTrack: How Unique Are Your Touch Gestures?
Rahat Masood (The University of New South Wales), Benjamin Zi Hao Zhao, Hassan Jameel Asghar and Mohamed Ali Kaafar (Data61 - CSIRO)

Towards Precise and Automated Verification of Security Protocols in Coq
Hernan Palombo, Hao Zheng and Jay Ligatti (University of South Florida)

Vulnerability Discovery with Function Representation Learning from Unlabeled Projects
Guanjun Lin, Jun Zhang, Wei Luo, Lei Pan (Deakin University) and Yang Xiang (Swinburne University)

Watch Out Your Smart Watch When Paired
Youngjoo Lee, Wonseok Yang and Taekyoung Kwon (Yonsei University)

Who Was Behind the Camera? Towards Some New Forensics
Jeff Yan (Lancaster University) and Aurélien Bourquard (MIT)

Why Are You Going That Way? Measuring Unnecessary Exposure of Network Traffic to Nation States
Jordan Holland and Max Schuchard (University of Tennessee)

X-Ray Your DNS
Amit Klein, Vladimir Kravtsov (Fraunhofer SIT), Alon Perlmuter, Haya Shulman and Michael Waidner (Fraunhofer SIT)

DEMO

Akatosh: Automated Cyber Incident Verification and Impact Analysis
Jared Smith, Elliot Greenlee and Aaron Ferber (Oak Ridge National Laboratory)

MPS: 1st International Workshop on Multimedia Privacy and Security
Monday, October 30th, Dallas Ballroom A1

Program Chairs: *Roger Hallman (SPAWAR Systems Center, USA), Kurt Rohloff (New Jersey Institute of Technology, USA), Victor Chang (Xi'an Jiaotong Liverpool University, China)*

7:30 – 9:00a Breakfast and Registration

9:00 - 10:00a Session 1: Privacy

Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks
Angeliki Aktypi, Jason Nurse, and Michael Goldsmith (University of Oxford, UK)

A Study on Autoencoder-based Reconstruction Method for Wi-Fi Location Data with Erasures
Tetsushi Ohki (Shizuoka University, Japan) and Akira Otsuka (Institute of Information Technology, Japan)

10:00 - 10:45a Coffee Break

10:45a - 12:00p Session 2: Keynote

Keynote: An NSF View of Multimedia Privacy and Security
Jeremy Epstein (National Science Foundation)

12:00 - 2:00p Lunch

2:00 - 3:00p Session 3: Image and Video Security

Attacking Automatic Video Analysis Algorithms: A Case Study of Google Cloud Video Intelligence API
Hossein Hosseini, Baicen Xiao, and Radha Poovendran (University of Washington, USA), Andrew Clark (Worcester Polytechnic Institute, USA)

Approximate Thumbnail Preserving Encryption
Byron Marohn (Intel; Portland State University, USA), Charles Wright and Wu-Chi Feng (Portland State University, USA), Mike Rosulek and Rakesh B. Bobba (Oregon State University)

3:00 - 3:45p Coffee Break

3:45 - 5:30p Session 4: Intrusion Detection and Prevention

Detecting Spying and Fraud Browser Extensions
Gaurav Varshney and Manoj Misra (Indian Institute of Technology, Roorkee, India), and Pradeep K. Atrey (State University of New York at Albany, USA)

Discussion Panel: Multimedia Security and Privacy with IoT and Social Networks
Moderated by Kurt Rohloff (New Jersey Institute of Technology, USA) and Roger Hallman (SPAWAR Systems Center Pacific, USA)

WPES: 16th Workshop on Privacy in the Electronic Society
Monday, October 30th, Dallas Ballroom A2

Program Chair: *Adam J. Lee (University of Pittsburg, USA)*

7:30 – 8:30a Breakfast and Registration

8:30 – 8:35a Opening

8:35 – 10:15a Session 1: Social Systems and Notifications

Blind De-anonymization Attacks Using Social Networks [Short]
Wei-Han Lee (Princeton University), Changchang Liu (Princeton University), Shouling Ji (Zhejiang University and Georgia Tech), Prateek Mittal (Princeton University), Ruby Lee (Princeton University)

AnNotify: A Private Notification Service
Ania Piotrowska (University College London), Jamie Hayes (University College London), Nethanel Gelernter (College of Management, Academic Studies), George Danezis (University College London), Amir Herzberg (Bar Ilan University)

Notify Assist: Balancing Privacy and Convenience in Delivery of Notifications on Android Smartphones [Short]
Raj Vardhan (McAfee), Ameya Sanzgiri (University at Buffalo), Dattatraya Kulkarni (McAfee), Piyush Joshi (McAfee)

SOMAR: Privacy-Preserving SOcial Media Advertising ARchitecture - Or: How Not To Leave Your Personal Data Around
Daniela Becker (Robert Bosch LLC, RTC, USA), Jorge Guajardo Merchan (Robert Bosch LLC, RTC, USA), Karl-Heinz Zimmermann (Hamburg University of Technology)

Is Bob Sending Mixed Signals?
Michael Schliep, Ian Kariniemi, and Nicholas Hopper (University of Minnesota)

10:15 – 10:45a Coffee Break

10:45 – 12:15p Session 2: Privacy Preservation

BIOS ORAM: Improved Privacy-preserving Data Access for Parameterized Outsourced Storage
Michael Goodrich (University of California, Irvine)

Mix-ORAM : Using Delegated Shuffles
Raphael Toledo (University College London), George Danezis (University College London), Isao Echizen (National Institute of Informatics)

Adaptive Statistical Learning with Bayesian Differential Privacy
Jun Zhao (Carnegie Mellon University)

SweetDroid: Toward a Context-Sensitive Privacy Policy Enforcement Framework for Android OS
Xin Chen (Didi Labs), Heqing Huang (IBM TJ Watson), Sencun Zhu (Penn State Univ.), Qing Li (Symantec Inc.), Quanlong Guan (Jinan University)

12:15 – 1:45p Lunch

1:45 – 3:15p Session 3: Privacy-preserving Computation

Private Set Projections & Variants
Xavier Carpent (UC Irvine), Sky Faber (UC Irvine), Tomas Sander (HPL Princeton), and Gene Tsudik (UC Irvine)

Public Accountability vs. Secret Laws: Can They Coexist? (A Cryptographic Proposal)
Shafi Goldwasser (MIT and Weizmann) and Sunoo Park (MIT)

WPES: 16th Workshop on Privacy in the Electronic Society
Monday, October 30th, Dallas Ballroom A2

Program Chair: *Adam J. Lee (University of Pittsburg, USA)*

A Framework of Privacy Preserving Anomaly Detection: Providing Traceability Without Big Brother
Hiromi Arai (NICT), Keita Emura (NICT), and Takuya Hayashi (Kobe University)

Using Secure Graph Algorithms for the Privacy-preserving Identification of Optimal Bartering Opportunities

Stefan Wueller (RWTH Aachen University), Michael Vu (RWTH Aachen University), Ulrike Meyer (RWTH Aachen University), and Susanne Wetzel (Stevens Institute of Technology)

3:15 – 3:45p Coffee Break

3:45 – 5:25p Session 4: Probing, Fingerprinting, and Other Deanonymization

Using EEG-Based BCI Devices to Subliminally Probe for Private Information [Short]
Mario Frank (UC Berkeley), Tiffany Hwu (UC Irvine), Sakshi Jain (LinkedIn Corporation), Robert T Knight (UC Berkeley), Ivan Martinovic (University of Oxford), Prateek Mittal (Princeton University), Daniele Perito (UC Berkeley), Ivo Sluganovic (University of Oxford), and Dawn Song (UC Berkeley)

Is Geo-Indistinguishability What You Are Looking For? [Short]
Simon Oya (University of Vigo), Carmela Troncoso (IMDEA Software Institute), and Fernando Perez-Gonzalez (University of Vigo)

Onions in the Crosshairs: When The Man Really Is Out to Get You
Aaron D. Jaggard, Paul Syverson (NRL)

Third-party Risks with Online Advertising - or - How Alice Can Buy Ads to Track Bob on a Budget
Paul Vines, Franziska Roesner, Tadayoshi Kohno (University of Washington)

Analysis of Fingerprinting Techniques for Tor Hidden Services
Andriy Panchenko (University of Luxembourg), Asya Mitseva (University of Luxembourg), Martin Henze (RWTH Aachen University), Fabian Lanze (Huf Secure Mobile GmbH), Klaus Wehrle (RWTH Aachen University), Thomas Engel (University of Luxembourg)

MTD: 4th Workshop on Moving Target Defense
Monday, October 30th, Dallas Ballroom A3

Program Chairs: *Hamed Okhravi (MIT Lincoln Laboratory, USA), Xinming Ou (University of South Florida, USA)*

7:30 - 8:50a Breakfast and Registration

8:50 - 9:00a Opening Remarks and Logistics

9:00 - 10:00a Keynote #1: (Session Chair: Hamed Okhravi)

Keynote: Science, Security and Academic Literature: Can We Learn from History?
Prof. Paul Van Oorschot (Carleton University)

10:00 - 10:15a Coffee Break

10:15a – 12:15p Session 1: New Moving Target Defenses

U-TRI: Unlinkability Through Random Identifier for SDN Network
Yulong Wang, Qingyu Chen, Junjie Yi, Jun Guo (Beijing University of Posts and Telecommunications)

Mixr: Flexible Runtime Rerandomization for Binaries
William Hawkins, Anh Nguyen-Tuong, Jason D. Hiser, Michele Co, Jack W. Davidson (University of Virginia)

Mutated Policies: Towards Proactive Attribute-based Defenses for Access Control
Carlos E. Rubio-Medrano, Josephine Lamp, Adam Doupé, Ziming Zhao, Gail-Joon Ahn (Arizona State University)

12:15 - 1:45p Lunch Break

1:45 - 2:45p Keynote # 2: (Session Chair: Hamed Okhravi)

Keynote: Moving Targets vs. Moving Adversaries: On the Effectiveness of System Randomization
Prof. Ahmad-Reza Sadeghi (Technische Universität Darmstadt)

2:45 – 3:45p Session 2: MTD Models and Evaluation

Performance Modeling of Moving Target Defenses
Warren Connell, Daniel Menasce, Massimiliano Albanese (George Mason University)

Evaluation of Deception-based Web Attacks Detection
Xiao Han (Orange Labs and Eurecom); Nizar Kheir (Thales); Davide Balzarotti (Eurecom)

3:45 - 4:00p Coffee Break

4:00 – 5:30p Session 3: MTD-based Detection, Games, and Algorithms

Detecting Stealthy Botnets in a Resource-Constrained Environment Using Reinforcement Learning
Sridhar Venkatesan, Massimiliano Albanese, Ankit Shah, Rajesh Ganesan, Sushil Jajodia (George Mason University)

Multi-Stage Attack Graph Security Games: Heuristic Strategies, with Empirical Game-Theoretic Analysis
Thanh H. Nguyen, Mason Wright, Michael P. Wellman, Satinder Singh (University of Michigan, Ann Arbor)

Online Algorithms for Adaptive Cyber Defense on Bayesian Attack Graphs
Zhisheng Hu, Minghui Zhu, Peng Liu (Pennsylvania State University)

5:30 – 6:00p Session 4: Short Papers

MTD: 4th Workshop on Moving Target Defense
Monday, October 30th, Dallas Ballroom A3

Program Chairs: *Hamed Okhravi (MIT Lincoln Laboratory, USA), Xinming Ou (University of South Florida, USA)*

Path Hopping: an MTD Strategy for Quantum-safe Communication
Reihaneh Safavi-Naini, Alireza Poostindouz (University of Calgary); Viliam Lisy (Czech Technical University)

If You Can't Measure It, You Can't Improve It: Moving Target Defense Metrics
Stjepan Picek (IEEE); Erik Hemberg, Una-May O'Reilly (MIT CSAIL)

6:00p Closing Remarks

MIST: 9th International Workshop on Managing Insider Security Threats
Monday, October 30th, Dallas Ballroom D1

Program Chairs: *Ilsun You (Soonchunhyang University, South Korea), Elisa Bertino (Purdue University, USA)*

7:30-9:00a Breakfast and Registration

8:40-8:45a Welcome Message General Co-Chair: Dr. Ilsun You (Soonchunhyang University, Republic of Korea)

8:45-10:00a Session 1 – Insider Threat Technologies 1 (Session Chair: Dr. Hassan Takabi (University of North Texas)

Insider Threat Event Detection in User-System Interactions
Pablo Moriano (Indiana University), Jared Pendleton (Cisco Systems, Inc.), Steve Rich (Cisco Systems, Inc.), and Jean Camp (Indiana University)

Using VisorFlow to Control Information Flow Without Modifying the Operating System Kernel or its Userspace
Matt Shockley, Chris Maixner, Ryan Johnson, Mitch Deridder, W. Michael Petullo (United States Military Academy)

Complexity of Insider Attacks to Databases
Gökhan Kul (University at Buffalo), Shambhu Upadhyaya (University at Buffalo), and Andrew Hughes (University at Buffalo)

10:00-10:20a Coffee Break

10:20-12:00p Session 2 - Insider Threat Technologies 2 (Session Chair: Dr. W. Michael Petullo (United States Military Academy)

A Multi-Modal Neuro-Physiological Study of Malicious Insider Threats
Yassir Hashem, Hassan Takabi, Ram Dantu, Rodney Nielsen (University of North Texas)

MalicIT: A Dataset of Malicious Insider Threat Behavior Based on a Gamified Competition
Athul Harilal, Flavio Toffalini, John Castellanos, Juan Guarnizo, Ivan Homoliak, Martin Ochoa (Singapore University of Technology and Design)

MemTri: A Memory Forensics Triage Tool Using Bayesian Network and Volatility
Antonis Michalas, Rohan Murray (University of Westminster)

A Subliminal Channel in EdDSA: Information Leakage with High-Speed Signatures
Alexander Hartl, Robert Annessi, Tanja Zseby (TU Wien)

12:00-2:00p Lunch Break

2:00-3:00p Session 3 – Keynote (Session Chair: Dr. Ilsun You (Soonchunhyang University, Republic of Korea)

Keynote: Research Challenges and Opportunities in Big Digital Forensic Data
Kim-Kwang Raymond Choo (The University of Texas at San Antonio)

3:00-3:30p Coffee Break

3:30-5:00p Session 4 – Short Paper Session (Session Chair: Dr. Kim-Kwang Raymond Choo (The University of Texas at San Antonio)
Socializing Drones for Inter-Service Operability in Ultra-Dense Wireless Networks Using Blockchain
Vishal Sharma, Ilsun You (Soonchunhyang University), Gökhan Kul (University at Buffalo)

MIST: 9th International Workshop on Managing Insider Security Threats
Monday, October 30th, Dallas Ballroom D1

Program Chairs: *Ilsun You (Soonchunhyang University, South Korea), Elisa Bertino (Purdue University, USA)*

Combining Homomorphic Encryption with Trusted Execution Environment: A Demonstration with Paillier Encryption and SGX
Nir Drucker, Shay Gueron (University of Haifa)

Behavior Prediction over Summarized Network Activities
Shih-Chieh Su (Qualcomm)

Insider Threat Mitigation Using Moving Target Defense and Deception
Hassan Takabi (University of North Texas) and Haadi Jafarian (University of Colorado Denver)

Criminal Minds: Reasoning Prime Suspect in Russian Hacking Scandal by Perspective of Insiders
Mookyu Park (Korea University), Junwoo Seo (Korea University), Kyoungmin Kim (Korea University), Moosung Park (Agency for Defense Development) and Kyungho Lee (Korea University)

PLAS: Programming Languages and Analysis for Security
Monday, October 30th, Dallas Ballroom D2

Program Chairs: *Nataliia Bielova (Inria, France), Marco Gaboardi (University at Buffalo, SUNY, USA)*

7:30 – 8:50a Breakfast and Registration

8:50 – 9:00a Welcome

9:00 – 10:00a Session 1: Invited Talk

Invited Talk: Languages for Oblivious Computation
Michael Hicks (University of Maryland, College Park

10:00 – 10:45a Coffee Break

10:45a – 12:00p Session 2: Program Analysis

CFG Construction Soundness in Control-Flow Integrity
Gang Tan, Trent Jaeger (Penn State University)

Using Precise Taint Tracking for Auto-sanitization
Tejas Saoji, Thomas H. Austin (San Jose State University), Cormac Flanagan (University of California, Santa Cruz)

Modular Synthesis of Heap Exploits
Dusan Repel, Johannes Kinder, Lorenzo Cavallaro (Royal Holloway, University of London)

12:00 – 1:30p Lunch Break

1:30 – 3:00p Session 3: Information Flow

Short Paper: Compiler Optimizations with Retrofitting Transformations: IsThere a Semantic Mismatch?
Jay Lim (Rutgers University), Vinod Ganapathy (Indian Institute of Science), Santosh Nagarakatte (Rutgers University)

Short Paper: Towards Information Flow Reasoning About Real-world C Code
Samuel Gruetter, Toby Murray (University of Melbourne)

Annotated Multisemantics to Prove Non-Interference Analyses
Gurvan Cabon, Alan Schmitt (Inria)

Design-time Quantification of Integrity in Cyber-physical Systems
Eric Rothstein Morris, Martin Ochoa, Carlos G. Murguia (Singapore University of Technology and Design)

3:00 – 3:45p Coffee Break

3:45 – 4:45p Session 4: Invited Talk

Invited Talk: Authorization Contracts
Stephen Chong (Harvard University)

4:45 – 6:00p Session 5: New Languages and Tools

Encoding DCC in Haskell
Maximilian Algehed, Alejandro Russo (Chalmers University of Technology)

A Sequent Calculus for Counterfactual Reasoning
McKenna McCall, Lay Kuan Loh,,Limin Jia (Carnegie Mellon University)

Simplicity: A New Language for Blockchains
Russell O'Connor (Blockstream)

TPDP - Theory and Practice of Differential Privacy
Monday, October 30th, Dallas Ballroom D3

Program Chair: *Jonathan Ullman (Northeastern University, USA)*

7:30 – 8:45a Breakfast and Registration

8:45 - 9:00a Welcome

9:00 - 9:45a Session 1
Invited Talk: TBD
Dan Kifer

9:45 - 10:00a Session 2

Accuracy First: Selecting a Differential Privacy Level for Accuracy-Constrained ERM
Katrina Ligett, Seth Neel, Aaron Roth, Bo Waggoner, and Zhiwei Steven Wu

10:00 - 10:45a Coffee Break

10:45 - 11:30a Session 3

Invited Talk: TBD
Xi He

11:30 - 12:00p Session 4

Ektelo: A Framework for Defining Differentially-Private Computations
Dan Zhang, Ryan McKenna, Ios Kotsogiannis, Gerome Miklau, Michael Hay, Ashwin Machanavajjhala

Finite Sample Differentially Private Confidence Intervals
Vishesh Karwa, Salil Vadhan

12:00 - 2:00p Lunch Break

2:00 - 2:45p Session 5

Invited Talk: Rényi Differential Privacy
Ilya Mironov

2:45 - 3:00p Session 6
Practical Locally Private Heavy Hitters
Raef Bassily, Kobbi Nissim, Uri Stemmer, Abhradeep Thakurta

3:00 - 3:45p Coffee Break

3:45 - 4:30p Session 7

Invited Talk: TBD
Thomas Steinke

4:30 - 5:00p Session 8

BLENDER: Enabling Local Search with a Hybrid Differential Privacy Model
Brendan Avent, Aleksandra Korolova, David Zeber, Torgeir Hovden, Benjamin Livshits

Differential Privacy on Finite Computers
Victor Balcer, Salil Vadhan

5:00 – 6:00p Poster Session

Accuracy First: Selecting a Differential Privacy Level for Accuracy-Constrained ERM,
Katrina Ligett, Seth Neel, Aaron Roth, Bo Waggoner, Zhiwei Steven Wu

Practical Locally Private Heavy Hitters, *Raef Bassily, Kobbi Nissim, Uri Stemmer, Abhradeep Thakurta*

BLENDER: Enabling Local Search with a Hybrid Differential Privacy Model,
Brendan Avent, Aleksandra Korolova, David Zeber, Torgeir Hovden, Benjamin Livshits

Differential Privacy on Finite Computers,
Victor Balcer, Salil Vadhan

Ektelo: A Framework for Defining Differentially-Private Computations
Dan Zhang, Ryan McKenna, Ios Kotsogiannis, Gerome Miklau, Michael Hay, Ashwin Machanavajjhala

Finite Sample Differentially Private Confidence Intervals, *Vishesh Karwa, Salil Vadhan*

Towards an Optimal Algorithm for Concentrated Differential Privacy, *Jaroslaw Blasiok, Mark Bun, Aleksandar, Thomas Steinke*

One-sided Privacy, *Stylianos Doudalis, Ios Kotsogiannis, Ashwin Machanavajjhala and Sharad Mehrotra*

Differential Privacy for Growing Databases, *Rachel Cummings, Gi Heung Robin Kim, Sara Krehbiel and Uthaipon Tao Tantipongpipat*

Composable and Versatile Privacy via Truncated CDP, *Mark Bun, Cynthia Dwork, Guy Rothblum and Thomas Steinke*

Privacy Loss in Apple's Implementation of Differential Privacy on MacOS 10.12, *Jun Tang, Aleksandra Korolova, Xiaolong Bai, Xueqiang Wang and Xiaofeng Wang*

Bootstrap Inference and Differential Privacy, *Thomas Brawner, James Honaker*

Hiding Data Deception Attacks in Differential-Privacy Noise, *Jairo Giraldo, Alvaro Cardenas, Murat Kantarcioglu, Jonathan Katz*

Vulnerability in Floating Point Implementation of Exponential Mechanism, *Matthew Burke*

On the Correct Use of the Gaussian Mechanism for Differential Privacy, *Jun Zhao*

Locally Differentially Private Heavy Hitter Identification, *Tianhao Wang, Ninghui Li, Somesh Jha*

Competitive Differentially Private Algorithms for Interactive Queries, *Aleksandar Nikolov, Jonathan Ullman*

CyberW: 1st Workshop for Women in Cyber Security
Monday, October 30th, Austin Ballroom 1

Program Chairs: *Danfeng (Daphne) Yao (Virginia Tech, USA), Elisa Bertino (Purdue University, USA*

7:30 – 8:30a Breakfast and Registration

8:30 – 8:35a Chairs' Welcome

8:35 – 9:15a Session 1: Inclusive Excellence (Session Chair: Elisa Bertino)

Why a Cyber Security Career for a Woman?
Bhavani Thuraisingham (The University of Texas at Dallas)

Truth, Social Justice (and the American Way?)
David Evans (University of Virginia)

9:15 – 10:15a Session 2: Security Challenges (Session Chair: Daphne Yao)

The Evolutionary Mess: Computing and Cybersecurity Come of Age
Stephanie Forrest (Arizona State University)

10:15 – 10:45a Coffee Break

10:45 – 11:30a Session 2 (cont.): Security Challenges

Research Challenges and Opportunities in IoT Security
Elisa Bertino (Purdue University)

11:30 – 12:15 Lightning Talks I (Martina Lindorfer)

12:15 – 1:45p Lunch

1:45 – 3:15p Session 3: Privacy, Society, and Me (Session Chair: Bhavani Thuraisingham)

Privacy in Today's World
Rebecca Wright (Rutgers University)

Privacy and Trust: Friend or Foe
Ling Liu (Georgia Tech)

3:15 – 3:45p Coffee Break

3:45 – 4:45p Session 4: Cybersecurity in Practice (Session Chair: Wendy Wang)

Human-Centric Cyber
Diane Staheli (MIT Lincoln Laboratory)

Security and Privacy in the Age of IoT
Alvaro A. Cardenas (The University of Texas at Dallas)

4:45 – 5:20p Lightning Talks II (Martina Lindorfer)

SafeConfig: Applying the Scientific Method to Active Cyber Defense Research
Friday, November 3rd, Dallas Ballroom A1

Program Chairs: *Erin Miller and Nick Multari (Pacific Northwest National Lab, USA), Anoop Singhal (National Institute of Standards and Technology, USA)*

7:30 – 9:00 Breakfast and Registration

9:00 - 9:05a Chairs' Welcome

9:05 – 10:00a Session 1
Invited Talk: Science Council: A Method for Incorporating Science Practices Into Cybersecurity Research
Dr. Bill Sanders

Cybersecurity Research
Dr. Erin Miller

10:00 – 10:45a Coffee Break

10:45a – 12:00p Session 2
Predicting Zero-day Malicious IP Addresses
Amirreza Niakanlahiji, Mir Mehedi Pritom, Bei-Tseng Chu and Ehab Al-Shaer

A Flexible Approach Towards Security Validation
Michael Atighetchi, Fusun Yaman, David Last, Captain Nicholas Paltzer, Meghan Caiazzo and Stephen Raio

A First Look: Using Linux Containers for Deceptive Honeypots
Alexander Kedrowitsch, Danfeng Yao, Gang Wang and Kirk Cameron

12:00 – 2:00p Lunch Break

2:00 – 3:00p Session 3
Towards Realistic Threat Modelling: Attack Commodification, Irrelevant Vulnerabilities, and Unrealistic Assumptions
Luca Allodi and Sandro Etalle

On the Detection of Adversarial Attacks Against Deep Neural Networks
Weiyu Wang and Quanyan Zhu

Invited Talk: Step One Towards Science of Security
Mahran Al-Zyoud, Laurie Williams, Jeffrey C. Carver

Invited Talk: Secure IoT Stream Data Management and Analytics with Intel SGX
Latifur Khan, Swarup Chandra; Vishal Karande

3:00 – 3:45p Coffee Break

3:45 – 4:15p Session 4
Invited Talk: Applying Cybersecurity Challenges to Medical and Vehicular Cyber Physical Systems
Daniel Massey

Invited Talk : From Security to Safety: An Evolution of Operating States
Jeffrey Picciotto

4:15 – 5:00p Session 5: Panel
Panel: Applying the Scientific Method to Active Cyber Defense Research
Latifur Khan, Daniel Massey, Jeffrey Picciotto, Erin Miller

CPS-SPC: 3rd Workshop on Cyber-Physical Systems Security & Privacy
Friday, November 3rd, Dallas Ballroom A2

Program Chairs: *Rakesh Bobba (Oregon State University, USA), Awais Rashid (Lancaster University, UK)*

7:30am – 8:00a Breakfast and Registration

8:30 – 8:45a Opening and Chairs' Welcome

8:45 – 10:00a Session 1: Intrusion and Anomaly Detection

A New Burst-based DFA Model for SCADA Anomaly Detection
Chen Markman and Avishai Wool (Tel-Aviv University); Alvaro Cardenas (The University of Texas at Dallas)

From System Specification to Anomaly Detection (and Back)
Davide Fauri, Daniel Ricardo Do, Jerry den Hartog and Sandro Etalle (Eindhoven University of Technology), Elisa Costante (Security Matters), and Stefano Tonetta (Fondazione Bruno Kessler)

Automatic Deployment of Specification-based Intrusion Detection in the BACnet Protocol
Herson Esquivel-Vargas and Andreas Peter (University of Twente); Marco Caselli (Siemens AG)

10:00 – 10:45a Coffee Break

10:45a – 12:00p Session 2: Attacks

Jumping the Air Gap: Modeling Cyber-Physical Attack Paths in the Internet-of-Things
Ioannis Agadakos (Stevens Institute of Technology), Chien-Ying Chen and Monowar Hasan (University of Illinois at Urbana-Champaign), Matteo Campanelli (The City College of New York), Prashant Anantharaman (Dartmouth College), Bogdan Copos, Tancrède Lepoint, Michael Locasto, Gabriela F. Ciocarlie, Ulf Lindqvist (SRI International)

Developing Models for Physical Attacks in Cyber-Physical Systems [Short Paper]
Carmen Cheh, Ken Keefe, Brett Feddersen, and William H. Sanders (University of Illinois at Urbana-Champaign), Binbin Chen, William G. Temple (Advanced Digital Sciences Center)

On the Significance of Process Comprehension for Conducting Targeted ICS Attacks
Marina Krotofil (Honeywell Industrial Cyber Security Lab), Benjamin Green (Lancaster University), Ali Abbasi (University of Twente)

12:00 – 1:30p Lunch Break

1:30 – 3:00p Session 3: Threat Analysis and Risk Assessment

CPSA: A Cyber-Physical Security Assessment Tool for Situational Awareness in Smart Grid
Neetesh Saxena, Victor Chukwuka, Leilei Xiong, Santiago Grijalva (Georgia Institute of Technology, USA)

Cyber Threat Analysis Framework for the Wind Energy Based Power System
Amarjit Datta and Mohammad Rahman (Tennessee Technological University)

Gamifying ICS Security Training and Research: Design, Implementation, and Results of S3
Daniele Antonioli, Hamid Reza Ghaeini, Sridhar Adepu, Martín Ochoa, and Nils Ole Tippenhauer (Singapore University of Technology and Design)

How Long is a Piece of String: Defining Key Phases and Observed Challenges Within ICS Risk Assessment [Short Paper]
Benjamin Green, Daniel Prince, Jerry Busby, and David Hutchison (Lancaster University)

3:00 – 3:45p Coffee Break

3:45 – 4:45p Session 4: Analysis and Verification

Remote Proofs of Video Freshness for Public Spaces
Junia Valente and Alvaro Cardenas (The University of Texas at Dallas)

Secure and Privacy-Preserving Average Consensus [Short Paper]
Minghao Ruan, Muaz Ahmad, and Yongqiang Wang (Clemson University)

Integrating Design and Data Centric Approaches to Generate Invariants for Distributed Attack Detection [Short Paper]
Muhammad Azmi Umer (DHA Suffa University, Karachi and Karachi Institute of Economics and Technology, Pakistan), Khurum Nazir Junejo (Karachi Institute of Economics and Technology, Pakistan), Aditya Mathur and Sridhar Adepu (Singapore University of Technology and Design)

4:45 – 5:00p Closing Remarks

FEAST: Forming an Ecosystem Around Software Transformation
Friday, November 3rd, Dallas Ballroom A3

Program Chairs: *Taesoo Kim (Georgia Tech, USA), Dinghao Wu (Penn State University, USA)*

7:30 – 9:00a Breakfast and Registration

9:00 – 10:45a Opening Session and Keynote

Keynote: ALLVM: Enabling Sophisticated Late-Stage Program Analysis and Transformation Across the System Stack
Vikram Sadanand Adve (Interim Head and Professor of Computer Science, University of Illinois at Urbana-Champaign)

10:00 – 10:45a Coffee Break

10:45a – 12:00p Session 1: Binary Rewriting and Transformation

Vertx: Automated Validation of Binary Transformations
Denis Gopan and David Melski (GrammaTech, Inc), Peter Ohmann (Xavier Univeristy)

Zipr++: Exceptional Binary Rewriting
Jason Hiser, Anh Nguyen-Tuong, William Hawkins, Matthew McGill, Michele Co, and Jack W. Davidson (University of Virginia)

RL-Bin, Robust Low-overhead Binary Rewriter
mir Majlesi-Kupaei, Danny Kim, and Rajeev Barua (University of Maryland), Kapil Anand and Khaled ElWazeer (SecondWrite LLC)

DAMGate: Dynamic Adaptive Multi-feature Gating in Program Binaries
Yurong Chen, Tian Lan, and Guru V. Venkataramani (George Washington University)

12:00p – 1:30p Lunch Break

1:30m – 3:00p Session 2: CPS, Mobile and Intel SGX

CPS Runtime Architecture and Automated Transformation of Applications
Lui Sha (UIUC)

ReDroid: Prioritizing Data Flows and Sinks for App Security Transformation
Ke Tian, Danfeng Yao, and Barbara G. Ryder (Virginia Tech), Gang Tan (Penn State University)

Binary Code Retrofitting and Hardening Using SGX
Shuai Wang, Qinkun Bao, Pei Wang, and Dinghao Wu (Penn State University), Wenhao Wang and XiaoFeng Wang (Indiana University at Bloomington)

2:30 - 3:00p Short Presentations and Discussion

3:00 - 3:45p Coffee Break

3:45 - 5:00p Session 3: Software and Protocol Debloating

New Directions for Container Debloating
Vaibhav Rastogi and Somesh Jha (University of Wisconsin-Madison), Chaitra Niddodi and Sibin Mohan (University of Illinois Urbana-Champaign)

An Initial Investigation of Protocol Customization
David Ke Hong, Qi Alfred Chen, and Z. Morley Mao (University of Michigan)

A Multi-OS Cross-Layer Study of Bloating in User Programs, Kernel and Managed Execution Environments
Anh Quach, Rukayat Erinfolami, David Demicco, and Aravind Prakash (Binghamton University)

ASHES: 1st Workshop on Attacks and Solutions in Hardware Security
Friday, November 3rd, Dallas Ballroom D1

Program Chairs: *Chip Hong Chang (Nanyang Technological University, Singapore), Ulrich Rührmair, Horst Görtz Institute for IT-Security and Ruhr University Bochum, Germany)*

7:30 – 8:50a Breakfast and Registration

8:50 – 9:00a Welcome

9:00 – 10:00a Keynote

Keynote: Secure Hardware and Cryptography: Contrasts, Synergies and Challenges
Srini Devadas (MIT)

10:00 – 10:25a Coffee Break

10:25 – 11:25a Keynote

Keynote: Hardware-Assisted Security: Promises, Pitfalls and Opportunities
Ahmad-Reza Sadeghi (TU Darmstadt)

11:25a – 12:15p Session 1: Solutions in Hardware Security

Boolean Circuit Camouflaging: Cryptographic Models, Limitations, Provable Results, and a Random Oracle Realization
Giovanni Di Crescenzo (Vencore Labs), Jeyavijayan Rajendran (Texas A&M University), Ramesh Karri (NYU), Nasir Memon (NYU) and Yevgenij Dodis (NYU)

Optimizing Cryptography in Energy Harvesting Applications
Charles Suslowicz , Archanaa S Krishnan and Patrick Schaumont (Virginia Tech)

12:15 – 2:00p Lunch

2:00 – 3:00p Keynote
Keynote: Data-driven Software Security and its Hardware Support
Ulfar Erlingsson (Google)

3:00 – 3:30p Coffee Break

3:30 – 4:10p Session 2: WaC & SoK

WaC: SpaceTEE – Secure and Tamper-Proof Computing in Space using CubeSats
Yan Michalevsky and Yonatan Winetraub (Stanford)

SoK: A Survey of Clone Detection Approaches in RFID-based Supply Chains
Hoda Maleki, Reza Rahaeimehr and Marten van Dijk (University of Connecticut)

4:10 – 5:00p Session 3: Attack in Hardware Security

EM Attack on BCH-based Error Correction for PUF-based Key Generation
Lars Tebelmann, Michael Pehl and Georg Sigl (TU München)

On the Feasibility and Performance of Rowhammer Attacks
Varnavas Papaioannou and Nicolas Courtois (University College London)

IoT S&P: 1st Workshop on Internet of Things Security and Privacy
Friday, November 3rd, Dallas Ballroom D2

Program Chairs: *Theophilus Benson (Duke University, USA), Srikanth Sundaresan (Princeton University, USA)*

7:30 – 8:50a Breakfast and Registration

8:50 – 9:00a Welcome Message

Technical Program Co-Chair: Dr. Theophilus Benson (Brown University, USA)

9:00 – 10:00a Session 1: Things We Need to Fix Now – I

Systematically Evaluating Security and Privacy for Consumer IoT Devices
Franco Loi, Arunan Sivanathan, Hassan Habibi Gharakheili, Adam Radford, and Vijay Sivaraman (University of New South Wales, Sydney, Australia

Plaintext Data Transmission in Consumer IoT Medical Devices
Daniel Wood, Noah Apthorpe, Nick Feamster (Princeton University)

Smart Solution, Poor Protection: An Empirical Study of Security and Privacy Issues in Developing and Deploying Smart Home devices
Hui Liu, Changyu Li (Shanghai Jiao Tong University), Xuancheng Jin (Xidian University), Juanru Li, Yuanyuan Zhang, and Dawu Gu (Shanghai Jiao Tong University)

10:00 – 10:30a Coffee Break

10:30 – 11:20a Session 2 - (Unusual) Things We Need to Fix Now - II

Security & Privacy of Smart Toys
Junia Valente and Alvaro Cardenas (The University of Texas at Dallas)

How to Practice Safe IoT: Sexual Intimacy in the Age of Smart Devices
Matthew Wynn, Kyle Tillotson, Ryan Kao and Alvaro Cardenas (The University of Texas at Dallas); Andrea Calderon (Universidad Nacional); Andres Murillo, Javier Camargo, Rafael Mantilla, and Brahian Rangel (Universidad de los Andes); and Sandra Rueda (Universidad de los Andes)

Understanding Security Threats in Consumer Drones Through the Lens of the Discovery Quadcopter Family
Junia Valente and Alvaro Cardenas (The University of Texas at Dallas)

11:20a – 12:15p Session 3: Defense Against the IoT Hacks

A Secure Event Logging System for Smart Home
Sepideh Avizheh, Tam Thanh Doan, Xi Liu and Reihaneh Safavi-Naini (University of Calgary)

Toward Usable Network Traffic Policies for IoT Devices in Consumer Networks
Nicholas DeMarinis and Rodrigo Fonseca (Brown University)

Enabling Multi-user Controls in Smart Home Devices
William Jang and Adil Chhabra (Amherst College); and Aarathi Prasad (Skidmore College)

12:15 – 2:00p Lunch Break

2:00 – 3:00p Session 4: Keynote (CC)

Keynote: Computer Security and Privacy for the Physical World
Earlence Fernandes (University of Washington, Seattle)

IoT S&P: 1st Workshop on Internet of Things Security and Privacy
Friday, November 3rd, Dallas Ballroom D2

Program Chairs: *Theophilus Benson (Duke University, USA), Srikanth Sundaresan (Princeton University, USA)*

3:00 – 4:00p Coffee Break and Session 5: Poster Session

Open-source Software-based Portable DoS Test Tool for IoT Devices
Keigo Nagara, Katsunori Aoki, Yutaka Matsubara and Hiroaki Takada (Nagoya University, Aichi, Japan)

Universal Radio Hacker: A Complete Suite for Investigating IoT Protocols
Johannes Pohl and Andreas Noack (University of Applied Sciences Stralsund)

Keep Pies Away from Kids: A Raspberry Pi Attacking Tool
Antonis Michalas and Ryan Murray (University of Westminster)

Source-End DDoS Defense in IoT Environments
Sam Mergendahl, Devkishen Sisodia and Jun Li (University of Oregon); Hasan Cam (Army Research Laboratory)

4:00 – 4:50p Session 6 – Defense Against the IoT Hacks

Low Cost Standard Public Key Cryptography Services for Wireless IoT Systems
Muslum Ozgur Ozmen and Attila A. Yavuz (Oregon State University)

Sounding the Bell for Improving Internet (of Things) Security
Theophilus Benson (Brown University) and Balakrishnan Chandrasekaran (Technische Universität Berlin)

A Lightweight Vulnerability Mitigation Framework for IoT Devices
Noy Hadar, Shachar Siboni, and Yuval Elovici (Cyber Security Research Center, Ben-Gurion University of the Negev)

4:50 – 5:00p Closing Remarks

CCSW: 9th Cloud Computing Security Workshop
Friday, November 3rd, Dallas Ballroom D3

Program Chairs: *Angelos Stavrou (George Mason University, USA), Ghassan Karame (NEC Laboratories Europe, Germany)*

7:30 – 9:00a Breakfast and Registration

9:00 – 09:15a Chairs' Welcome

09:15 – 10:15a Keynote
Keynote: TBD

10:15 – 10:45a Coffee Break

10:45 – 11:45a Session 1: Attacks and Defenses for Clouds

Numerical Evaluation of Cloud-Side Shuffling Defenses against DDoS Attacks on Proxied Multiserver Systems
Yuquan Shan (PSU), Goerge Kesidis (PSU), Daniel Fleck (GMU)

Short Paper: The vAMP Attack: Taking Control of Cloud Systems Via the Unified Packet Parse
Kashyap Thimmaraju, Bhargava Shastry, Tobias Fiebig, Felicitas Hetzelt, Jean-Pierre Seifert, Anja Feldmann,Stefan Schmid (TU BERLIN)

12:00 – 2:00p Lunch

2:00 – 3:20p Session 2: Secure and Privacy-preserving Computations

REX: a Searchable Symmetric Encryption Scheme Supporting Range Queries
Panagiotis Rizomiliotis, Eirini Molla, Stefanos Gritzalis (University of the Aegean)

Short Paper: Privacy-preserving Machine Learning in Cloud
Ehsan Hesamifard (UNT), Hassan Takabi (UNT), Mehdi Ghasemi (USASK)

Practical and Secure Outsourcing of Discrete Log Group Exponentiation to a Single Malicious Server
Giovanni Di Crescenzo (Vencore Labs), Matluba Khodjaeva, Delaram Kahrobaei, Vladimir Shpilrain (CUNY)

3:20 – 3:45p Coffee Break

3:45 – 4:30p Session 3: Blockchain Security

Short Paper: Towards Blockchain-based Auditable Storage and Sharing of IoT
Hossein Shafagh, Anwar Hithnawi, Lukas Burkhalter (ETH Zurich), Simon Duquennoy (Inria, France and RISE SICS, Sweden)

Short Paper: A Note on the Security of Equihash
Leo Alcock, Ling Ren (MIT)

AISec: 10th Workshop on Artificial Intelligence and Security
Friday, November 3rd, Austin Ballroom 1

Program Chairs: Battista Biggio (University of Cagliari, Italy), David Freeman (Facebook, Inc., USA), Brad Miller (Google Inc., USA), Arunesh Sinha (University of Michigan, Ann Arbor, USA)

7:30 – 8:50a Breakfast and Registration

8:50 – 9:00a Welcome Remarks

David Freeman (Facebook, Inc., USA)

9:00 – 10:00a Keynote
Keynote: Beyond Big Data: What Can We Learn from AI Models?
Aylin Caliskan (Princeton University, USA)

10:00 – 10:40a Coffee Break

10:40a – 12:00p Session 1: Deep Learning

Adversarial Examples Are Not Easily Detected: Bypassing Ten Detection Methods
Nicholas Carlini and David Wagner

ZOO: Zeroth Order Optimization-based Black-box Attacks to Deep Neural Networks Without Training Substitute Models
Pin-Yu Chen, Huan Zhang, Yash Sharma, Jinfeng Yi, Cho-Jui Hsieh

Towards Poisoning of Deep Learning Algorithms with Back-gradient Optimization
Luis Muñoz-González, Battista Biggio, Ambra Demontis, Andrea Paudice, Vasin Wongrassamee, Emil C. Lupu, Fabio Roli

Efficient Defenses Against Adversarial Attacks
Valentina Zantedeschi, Maria-Irina Nicolae, Ambrish Rawat

12:00 – 1:30p Lunch

1:30 – 2:00p Lightning Round

2:00 – 3:00p Session 2: Authentication and Intrusion Detection

Generating Look-alike Names For Security Challenges
Shuchu Han, Yifan Hu, Steven Skiena, Baris Coskun, Meizhu Liu, Hong Qin, Jaime Perez

In (Cyber)Space Bots Can Hear You Speak: Breaking Audio CAPTCHAs Using OTS Speech Recognition
Saumya Solanki, Gautam Krishnan, Varshini Sampath, Jason Polakis

Practical Machine Learning for Intrusion Detection for the Cloud: Challenges and the Way Forward
Ram Shankar Siva Kumar, Andrew Wicker, Matt Swann

3:00 – 3:45p Coffee Break

3:45 – 4:25p Session 3a: Defense Against Poisoning

Robust Linear Regression Against Training Data Poisoning

Chang Liu, Bo Li, Yevgeniy Vorobeychik, Alina Oprea

Mitigating Poisoning Attacks: Detecting Causative Attacks Using Data Provenance
Nathalie Baracaldo, Bryant Chen, Heiko Ludwig, Amir Safavi

4:25 – 5:05 Session 3b: Malware

Malware Classification and Class Imbalance via Stochastic Hashed LZJD
Edward Raff, Charles Nicholas

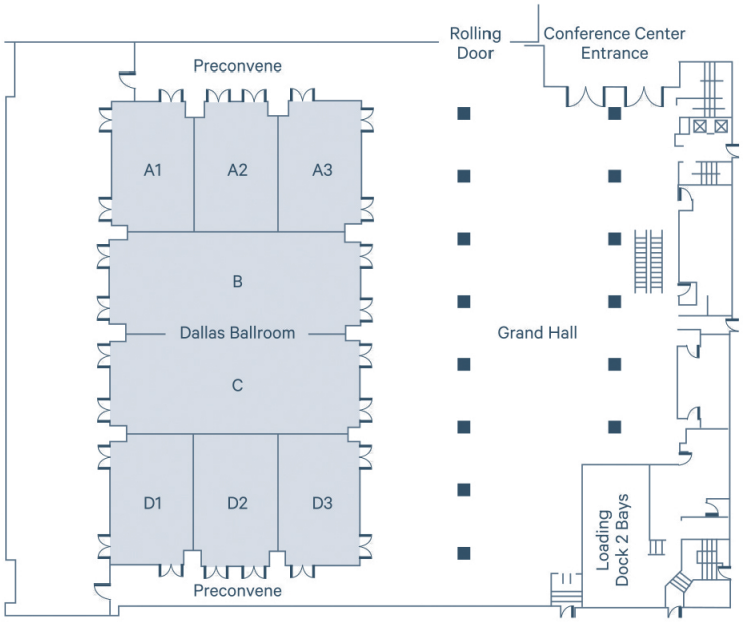
Learning the PE Header, Malware Detection with Minimal Domain Knowledge
Edward Raff, Jared Sylvester, Charles Nicholas

The 24th ACM Conference on Computer and Communications Security will be held in Dallas, Texas, USA from October 30, 2017 to November 3, 2017. Dallas is a major city in the state of Texas and is the largest urban center of the fourth most populous metropolitan area in the United States.

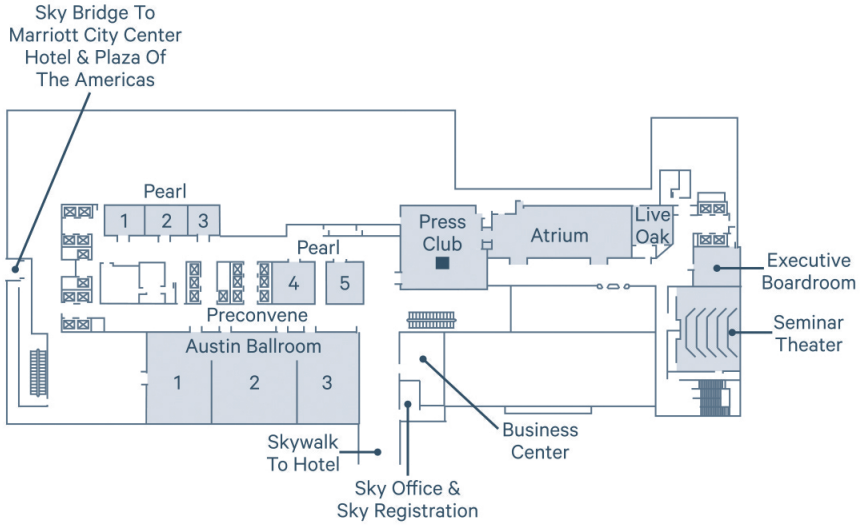
Address of the Conference Venue:

Hotel Sheraton Downtown Dallas
400 North Olive Street
Dallas, Texas 75201, USA

First Floor - Convention Center



Second Floor - Hotel



PLATINUM

Special Thanks To:

GOLD

SILVER

BRONZE

CCS Main Conference on Tuesday, October 31st, 2017

	Track 1	Track2	Track 3	Track 4	Track 5	Tutorials
	Dallas A1	Dallas A2	Dallas A3	Dallas D1	Dallas D2	Dallas D3
07:30-09:00	Breakfast & Registration					
09:00-10:30	**Chairs' Welcome @ Dallas BC** **Keynote** **"Security and Machine Learning"** **Prof. David Wagner (UC Berkeley)**					
10:30-10:45	Coffee Break					
10:45-12:15	1A: Multi-Party Computation	2A: Human Authentication	3A: Adversarial Machine Learning	4A: Browsers	5A: Cryptocurrency	Tutorial 1
12:15-1:45	Lunch Break					
1:45-3:15	1B: Multi-Party Computation	2B: Passwords	3B: Investigating Attacks	4B: Privacy Policies	5B: Blockchains	Tutorial 2
3:15-3:45	Coffee Break					
3:45-5:15	1C: Oblivious RAM	2C: World Wide Web of Wickedness	3C: Machine Learning Privacy	4C: From Verification to ABE	5C: Using Blockchains	Tutorial 2
5:15-6:00	Break					
6:00-8:00	**Welcome Reception & Poster Session**					

CCS Main Conference on Wednesday, November 1st, 2017

	Track 1	Track 2	Track 3	Track 4	Track 5	Tutorials
	Dallas A1	Dallas A2	Dallas A3	Dallas D1	Dallas D2	Dallas D3
07:30-09:00	Breakfast & Registration					
9:00-10:30	1D: Functional Encryption and Obfuscation	2D: Vulnerable Mobile Apps	3D: Logical Side Channels	4D: Crypto Primitives	5D: Network Security	
10:30-11:00	Coffee Break					
11:00-12:30	1E: Hardening Crypto	2E: Securing Mobile Apps	3E: Physical Side Channels	4E: Adversarial Social Networking	5E: Privacy-Preserving Analytics	Tutorial 3
12:30-2:00	Lunch Break					
2:00-3:30	1F: Private Set Intersection	2F: Insights from Log(in)s	3F: Crypto Pitfalls	4F: Private Queries	5F: Understanding Security Fails	Tutorial 4
3:30-4:00	Coffee Break					
4:00-5:00	1G: Searchable Encryption	2G: Bug-Hunting Risks and Rewards	3G: Crypto Standards	4G: Voting	5G: Hardening Hardware	Tutorial 4
5:00-5:15	Break					
5:15-6:45	**Panel @ Dallas Ballroom BC**					
6:45-7:00	Break					
7:00-9:00	**Award Ceremony & Banquet**					

CCS Main Conference on Thursday, November 2nd, 2017

	Track 1	Track 2	Track 3	Track 4	Track 5	Tutorials
	Dallas A1	Dallas A2	Dallas A3	Dallas D1	Dallas D2	Dallas D3
07:30-09:00	Breakfast & Registration					
09:00-10:30	1H: Crypto Attacks	2H: Code Reuse Attacks	3H: Web Security	4H: Formal Verification		Tutorial 5
10:30-11:00	Coffee Break					
11:00-12:30	1I: Post-Quantum	2I: Information Flow	3I: Personal Privacy	4I: Verifying Crypto	5I: Communication Privacy	Tutorial 5
12:30-2:00	Lunch Break					
2:00-3:30	1J: Outsourcing	2J: Fun with Fuzzing	3J: Problematic Patches	4J: Flash Security		Tutorial 6
3:30-4:00	Coffee Break					
4:00-5:30	1K: Secure Computation	2K: Fuzzing Finer and Faster	3K: Program Analysis	4K: Secure Enclaves		Tutorial 6
5:30-5:45	Break					
5:45-6:30	**Business Meeting @ Dallas Ballroom BC**					

ACM CCS 2017 | DALLAS, TEXAS