9th ACM Conference on Data and Application Security and Privacy

CODASPY 2019

March 25 – 27, 2019
Dallas, TX, USA

ACM SPECIAL INTEREST GROUP ON SECURITY, AUDIT & CONTROL

http://www.codaspy.org/

Sponsored by:

ACM SIGSAC

In cooperation with:

UT DALLAS
The University of Texas at Dallas

Table of Contents

Foreword

It is our great pleasure to welcome you to the ninth edition of the *ACM Conference on Data and Application Security and Privacy (CODASPY 2019)*, which follows the successful eight editions held in February/March 2011-2018. This conference series has been founded to foster novel and exciting research in this arena and to help generate new directions for further research and development. The initial concept was established by the two co-founders, Elisa Bertino and Ravi Sandhu, and sharpened by subsequent discussions with a number of fellow data security and privacy researchers. Their enthusiastic encouragement persuaded the co-founders to move ahead with the always daunting task of creating a high-quality conference.

Data and applications that manipulate data are crucial assets in today's information age. With the increasing drive towards availability of data and services anytime and anywhere, security and privacy risks have increased. Vast amounts of privacy-sensitive data are being collected today by organizations for a variety of reasons. Unauthorized disclosure, modification, usage or denial of access to these data and corresponding services may result in high human and financial costs. Important applications such as homeland security, social networking and social computing provide value by aggregating input from numerous individual users, and the mobile devices they carry. The emerging area of Internet of Things also poses serious privacy and security challenges. To achieve efficiency and effectiveness in traditional domains such as healthcare, there is a drive to make these records electronic and highly available. The need for organizations to share information effectively is underscored by rapid innovations in the business world that require close collaboration across traditional boundaries. Security and privacy in these and other arenas can be meaningfully achieved only in context of the application domain. Data and applications security and privacy has rapidly expanded as a research field with many important challenges to be addressed.

In response to the call for papers of CODASPY 2019, 119 papers were submitted from Africa, Asia, Europe, South America and North America. The program committee selected 28 full-length research papers (23.5% acceptance rate). These papers cover a variety of topics, including security issues in web, cloud, IoT, and mobile devices, privacy, access control, authentication, malware, code analysis, and hardware and system security. The program includes a poster paper session presenting exciting work in progress. The program is complemented by two keynote speeches by Anupam Joshi and Engin Kirda as well as a special distinguished lecture by Elisa Bertino. This year's edition also features three workshops: the ACM International Workshop on Security and Privacy Analytics, the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, and the ACM Workshop on Automotive Cybersecurity, and a panel on the research challenges at the intersection on AI, Big Data and Cyber Security.

The organization of a conference like CODASPY requires the collaboration of many individuals. First of all, we would like to thank the authors for submitting to the conference and the keynote speakers for graciously accepting our invitation. We express our gratitude to the program committee members and external reviewers for their efforts in reviewing the papers, engaging in active online discussion during the selection process and providing valuable feedback to authors. We also would like to thank Yuan Cheng (web and publicity chair), Ravi Sandhu (workshop chair), Rhonda Walls (local arrangement chair), Hongxin Hu (poster chair) and the committee of the poster track, Murtuza Jadliwala (proceedings chair), and Latifur Khan (panel chair). Finally, we would like to thank our sponsors, ACM SIGSAC and The University of Texas at Dallas, for supporting this conference.

We hope that you will find this program interesting and that the conference will provide you with a valuable opportunity to interact with other researchers and practitioners from institutions around the world. Enjoy!

Murat Kantarcioglu, *The University of Texas at Dallas, USA*
Ram Krishnan, *The University of Texas at San Antonio, USA*
CODASPY'19 Program Co-Chairs

Bhavani Thuraisingham, *The University of Texas at Dallas, USA*
Gail-Joon Ahn, *Arizona State University, USA*
CODASPY'19 General Co-Chairs

Conference Organization and Steering Committee

General Co-Chairs: Bhavani Thuraisingham, *The University of Texas at Dallas, USA*
Gail-Joon Ahn, *Arizona State University, USA*

Program Co-Chairs: Murat Kantarcioglu, *The University of Texas at Dallas, USA*
Ram Krishnan, *The University of Texas at San Antonio, USA*

Poster Chair: Hongxin Hu, *Clemson University, USA*

Workshop Chair: Ravi Sandhu, *The University of Texas at San Antonio, USA*

Panel Chair: Latifur Khan, *The University of Texas at Dallas, USA*

Publicity and Web Chair: Yuan Cheng, *California State University, Sacramento, USA*

Local Arrangement Chair: Rhonda Walls, *The University of Texas at Dallas , USA*

Proceedings Chair: Murtuza Jadliwala, *The University of Texas at San Antonio, USA*

Research Award Chair: Bhavani Thuraisingham, *The University of Texas at Dallas, USA*

Steering Committee: Elisa Bertino (co-chair), *Purdue University*
Ravi Sandhu (co-chair), *The University of Texas at San Antonio, USA*
Gail-Joon Ahn, *Arizona State University, USA*
Alexander Pretschner, *Technische Universität München*

Program and Poster Committee

Program Committee:

Irfan Ahmed (Virginia Commonwealth University)
Gail-Joon Ahn (Arizona State University)
Cuneyt Gurcan Akcora (The University of Texas at Dallas)
Vijay Atluri (Rutgers University)
Elisa Bertino (Purdue University)
Prosunjit Biswas (The University of Texas at San Antonio)
Barbara Carminati (University of Insubria)
Reza Curtmola (New Jersey Institute of Technology)
Naranke Dulay (Imperial College London)
Manuel Egele (Boston University)
Elena Ferrari (University of Insubria)
Philip W. L. Fong (University of Calgary)
Debin Gao (Singapore Management University)
Brahim Hamid (IRIT- University of Toulouse)
Hannes Hartenstein (Karlsruhe Institute of Technology)
Wei Jiang (University of Missouri-Columbia)
Martin Johns (TU Braunschweig)
Alexandros Kapravelos (North Carolina State University)
Yves Le Traon (University of Luxembourg)
Adam J. Lee (University of Pittsburgh)
Qi Li (Tsinghua University)
Dan Lin (University of Missouri)
Brad Malin (Vanderbilt University)
Fabio Martinelli (IIT-CNR)
Amirreza Masoumzadeh (University at Albany – SUNY)
Martín Ochoa (Universidad del Rosario)
Jaehong Park (University of Alabama in Huntsville)
Alexander Pretschner (Technical University of Munich)
Indrajit Ray (Colorado State University)
Vassil Roussev (University of New Orleans)
Erkay Savas (Sabanci University)
Huasong Shan (JD.com American Technologies Corporation)
Anna Squicciarini (The Pennsylvania State University)
NataliaStakhanova (University of New Brunswick)
Hassan Takabi (University of North Texas)
Mahesh Tripunitara (University of Waterloo)
Jaideep Vaidya (Rutgers University)
Wendy Hui Wang (Stevens Institute of Technology)
Roland Yap (National University of Singapore)
Ting Yu (Qatar Computing Research Institute)
Chuan Yue (Colorado School of Mines)
Junyuan Zeng (The University of Texas at Dallas)
Yajin Zhou (Zhejiang University)

Poster Committee:

Long Cheng (Clemson University)
Yuan Cheng (California State University, Sacramento)
Hongda Li (Clemson University)
Carlos Rubio (Arizona State University)
Ziming Zhao (Rochester Institute of Technology)

Additional Reviewers:

Kevin Allix
Adam Bowers
Aleieldin Salem
Alexandra Dirksen
Alexandre Bartel
Ali Allami
Amani Abu Jabal
Anand Mudgerikar
Andrea Saracino
Ankush Singla
Antonio La Marra
Athanasios Rizos
Bo Zhang
Cengiz Örencik
Chao Yan
Christian Rondanini
Christina Michailidou
David Klein
Francesco Mercaldo
Ganbayar Uuganbayar
Giacomo Giorgi
Gokhan Sagirlar
Gregory Duck
Hafiz Asif
Hasini Gunasinghe
Hong Hu
Husheng Zhou
Jan Grashöfer
Jize Du
Julien Polge
Jun Han
Ken Goss
Leila Bahri
Ludovic Mouline
Marc Leinweber
Marius Musch
Matthew Sanders
Matthias Grundmann
Médéric Hurier
Min Suk Kang
Mohsen Ahmadvand
Nitish Uplavikar
Oliver Stengele
Padmavathi Iyer
Pietro Colombo
Prasanna Umar
Qingchuan Zhao
Sebastian Banescu
Severin Kacianka
Shagufta Mehnaz
Shruti Tople
Simon Koch
Sufatrio Sufatrio
Sushama Karumanchi
Tegawende Bissyande
Thomas Hutzelmann
Till Neudecker
Weiping Pei
Weiyi Xia
Wenhao Wang
Yi Qin
Yifei Wang
Younes Karimi
Zhiju Yang
Zhiyu Wan

Hyatt Regency North Dallas Richardson
1st Floor Main Meeting Space

Event	CODASPY 2019	Reception/ Poster Session & Banquet	IWSPA Workshop	SDN-NFV Workshop	AutoSec Workshop
Room	*Salon D*	*Salon EFG*	*Longhorn II*	*Longhorn III*	*Longhorn IV*

Special Distinguished Lecture

Elisa Bertino
Professor, Purdue University
Date: Monday, March 25th, 2019
Time: 9:00 – 10:00am
Room: Salon D

Security and Privacy in the IoT

The Internet of Things (IoT) paradigm refers to the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with servers, centralized systems, and/or other connected devices based on a variety of communication infrastructures. IoT makes it possible to sense and control objects creating opportunities for more direct integration between the physical world and computer-based systems. IoT will usher automation in a large number of application domains, ranging from manufacturing and energy management (e.g. SmartGrid), to healthcare management and urban life (e.g. SmartCity). However, because of its fine-grained, continuous and pervasive data acquisition and control capabilities, IoT raises concerns about security and privacy. Deploying existing security solutions to IoT is not straightforward because of device heterogeneity, highly dynamic and possibly unprotected environments, and large scale. In this talk, after outlining key challenges in IoT security and privacy, we present initial approaches to securing IoT data, including firewall techniques to prevent IoT devices to be compromised and used by botnets.

Biography:

Elisa Bertino is professor of Computer Science at Purdue University. Prior to joining Purdue, she was a professor and department head at the Department of Computer Science and Communication of the University of Milan. She has been a visiting researcher at the IBM Research Laboratory (now Almaden) in San Jose, at the Microelectronics and Computer Technology Corporation, at Rutgers University, and at Telcordia Technologies. Her main research interests include security, privacy, database systems, distributed systems, and sensor networks. Her recent research focuses on digital identity management, biometrics, IoT security, security of 4G and 5G cellular network protocols, and policy infrastructures for managing distributed systems. Prof. Bertino has published more than 700 papers in all major refereed journals, and in proceedings of international conferences and symposia. She has given keynotes, tutorials and invited presentations at conferences and other events. She is a Fellow member of ACM, IEEE, and AAAS. She received the 2002 IEEE Computer Society Technical Achievement Award "For outstanding contributions to database systems and database security and advanced data management systems" and the 2005 IEEE Computer Society Tsutomu Kanai Award for “Pioneering and innovative research contributions to secure distributed systems”.

Conference Keynote 1

Engin Kirda
Professor, Northeastern University
Date: Monday, March 25th, 2019
Time: 10:00 – 11:00am
Room: Salon D

Using AI to Detect Advanced Threats – Done Right

In industry today, almost everyone claims that they are using some form of "AI" to detect complex attacks. In this talk, I will take a critical look at some of the claims that many security companies are making in this domain. I will then describe some of the work we are doing at Lastline (which is an academically-rooted company) in using AI to detect attacks in the right context and in the right way.

Biography:

Engin Kirda holds the post of professor of computer science at Northeastern University in Boston. Before that, he held faculty positions at Institute Eurecom in the French Riviera and the Technical University of Vienna, where he co-founded the Secure Systems Lab that is now distributed over five institutions in Europe and the United States. Professor Kirda's research has focused on malware analysis (e.g., Anubis, Exposure, and Fire) and detection, web application security, and practical aspects of social networking security. He co-authored more than 150 peer-reviewed scholarly publications and served on the program committees of numerous well-known international conferences and workshops. Professor Kirda was the program chair of the International Symposium on Recent Advances in Intrusion Detection (RAID) in 2009, the program chair of the European Workshop on Systems Security (Eurosec) in 2010 and 2011, the program chair of the well-known USENIX Workshop on Large Scale Exploits and Emergent Threats in 2012, the program chair of the security flagship conference Network and Distributed System Security Symposium (NDSS) in 2015, and co-chair of USENIX Security in 2017. In the past, Professor Kirda has consulted for the European Commission on emerging threats, and gave a Congressional Briefing in Washington D.C. on advanced malware attacks and cyber-security. He also spoke at SXSW Interactive 2015 about "Malware in the Wild" and at Blackhat 2015. Besides his roles at Northeastern, Professor Kirda is a co-founder of Lastline, Inc, a Silicon-Valley based company that specializes in the detection and prevention of advanced cyber-attacks.

Conference Keynote 2

Anupam Joshi
Professor, University of Maryland, Baltimore County
Date: Tuesday, March 26th, 2019
Time: 9:00 – 10:00am
Room: Salon D

Using AI to Detect Attacks and Manage Access Control

As attacks have become more complex and involved, the cognitive bandwidth of a SoC analyst has become a bottleneck. This talk explores using AI to augment the capabilities of an analyst. Specifically, while data mining and machine learning have been used extensively to detect attacks, there has been limited exploration of other AI techniques such as knowledge extraction, representation, and reasoning in security. This talk explores how traditional information sources (host and network based sensors) can be combined with information extracted from threat intelligence to detect attacks. We focus on the threat intelligence and access control for IoT elements of this body of work.

Biography:

Anupam Joshi is the Oros Family Professor and Chair of Computer Science and Electrical Engineering Department at the University of Maryland, Baltimore County (UMBC). He is the Director of UMBC's Center for Cybersecurity, and one of the USM leads for the National Cybersecurity FFRDC. He is a Fellow of IEEE.

Dr. Joshi obtained a B.Tech degree from IIT Delhi in 1989, and a Masters and Ph.D. from Purdue University in 1991 and 1993 respectively. His research interests are in the broad area of networked computing and intelligent systems. His primary focus has been on data management and security/privacy in mobile/pervasive computing environments, and policy driven approaches to security and privacy. He is also interested in Semantic Web and Data/Text/Web Analytics, especially their applications to (cyber) security. He has published over 275 technical papers with an h-index of 78 and over 23000 citations (per Google scholar), been granted nine patents, and has obtained research support from National Science Foundation (NSF), NASA, Defense Advanced Research Projects Agency (DARPA), US Dept of Defense (DoD), NIST, IBM, Microsoft, Qualcom, Northrop Grumman, and Lockheed Martin amongst others.

Workshop Keynote

Jeremy Daily
Associate Professor, University of Tulsa
Date: Wednesday, March 27th, 2019
Time: 9:30 – 10:30am
Room: Longhorn III/IV

Cybersecurity Aspects of Heavy Vehicle Digital Forensics

As vehicles become more computerized and cybersecurity concerns transcend traditional information technologies, new challenges related to incident response and digital forensics arise for heavy vehicles. The presentation is focused on highlighting observations related to the cybersecurity of heavy vehicles from the perspective of a mechanical engineer reconstructing traffic crashes. This intersection of cyber-physical incident response will only grow in importance with the race towards autonomy and higher levels of computer control of the vehicles. As autonomous vehicles are involved in crashes, digital forensics and physical reconstructions will go hand-in-hand to determine crash causation. However, experts in cybersecurity and digital forensics rarely work with experts in traffic crash reconstruction. This presentation tries to bridge that domain gap by providing interesting results from tests and research that would benefit both domains.

Biography:

After some time working in electronic maintenance in the U.S. Air Force, Jeremy Daily graduated with his Ph.D. from Wright State University after studying mechanical engineering. He went to work at the University of Tulsa researching traffic crash reconstruction techniques where he started a crash reconstruction research consortium (TU- CRRC). As part of that consortium, Dr. Daily traveled all over the United States and performed crash tests to gather data relating digital information onboard vehicles with the physical observations and measurements from a crash scene. Around 2010, Dr. Daily started a U.S. Department of Justice project with colleagues from the computer science department (John Hale and Mauricio Papa). The project was to develop digital forensic techniques for the process control systems onboard heavy trucks. This research resulted in a patent that was awarded in 2018. After the patent application was submitted, Dr. Daily took a sabbatical and founded Synercon Technologies in 2013 with some of his graduating students. After raising venture capital to build digital forensic tools for heavy trucks, the business turned profitable in a couple years and Synercon Technologies was sold in December of 2018. Meanwhile, the heavy vehicle industry recognized the need to understand cybersecurity concerns for their vehicles. In 2017, Dr. Daily co-founded (with Karl Heimer) the CyberTruck Challenge, a non-profit dedicated to creating a community of interest regarding heavy vehicle cybersecurity issues and helping develop the next generation of talent to face these issues. Currently, Dr. Daily teaches in the mechanical engineering department and conducts externally funded research related to heavy vehicle cybersecurity.

CODASPY Main Conference, Monday, March 25th, 2019

8:45-9:00a	Day 1 - Welcome (Salon D)
	Session Chair: Murat Kantarcioglu, The University of Texas at Dallas
9:00-10:00a	**Special Distinguished Lecture** ***Security and Privacy in the IoT*** Elisa Bertino (Purdue University)
10:00-11:00a	**Conference Keynote I** ***Using AI to Detect Advanced Threats – Done Right*** Engin Kirda (Northeastern University)
11:00-11:30a	Break
	Session 1 Mobile Security
	Session Chair: Kevin Butler, University of Florida
11:30a-1:10p	**Developing TrustZone User Interface for Mobile OS Using Delegation Integration Model** *Kailiang Ying (Syracuse University), Priyank Thavai (Syracuse University) and Wenliang Du (Syracuse University)*
	Understanding the Responsiveness of Mobile App Developers to Software Library Updates *Tatsuhiko Yasumatsu (Waseda University), Takuya Watanabe (NTT Secure Platform Laboratories / Waseda University), Fumihiro Kanei (NTT), Eitaro Shioji (NTT), Mitsuaki Akiyama (NTT), and Tatsuya Mori (Waseda University / RIKEN AIP)*
	ACMiner: Extraction and Analysis of Authorization Checks in Android's Middleware *Sigmund Albert Gorski III (North Carolina State University), Benjamin Andow (North Carolina State University), Adwait Nadkarni (William and Mary Univ.), Sunil Manandhar (William and Mary Univ.), William Enck (North Carolina State University), Eric Bodden (Paderborn University) and Alexandre Bartel (University of Luxembourg)*
	REAPER: Real-time App Analysis for Augmenting the Android Permission System *Michalis Diamantaris (FORTH), Elias P. Papadopoulos (FORTH), Evangelos P. Markatos (FORTH), Sotiris Ioannidis (FORTH) and Jason Polakis (University of Illinois at Chicago)*
1:10-2:10p	Lunch (Salon EFG)
	Session 2 IOT/Smart Device Security
	Session Chair: Maribel Fernandez, King's College London
2:10-3:50p	**Verifiable Round-Robin Scheme for Smart Homes** *Nisha Panwar (University of California, Irvine), Shantanu Sharma (University of California, Irvine), Guoxi Wang (University of California, Irvine), Sharad Mehrotra (University of California, Irvine) and Nalini Venkatasubramanian (University of California, Irvine)*
	Dynamic Groups and Attribute-Based Access Control for Next-Generation Smart Car *Maanak Gupta (The University of Texas at San Antonio), James Benson (The University of Texas at San Antonio), Farhan Patwa (The University of Texas at San Antonio) and Ravi Sandhu (The University of Texas at San Antonio)*
	A Study of Data Store-based Home Automation *Kaushal Kafle (William & Mary University), Kevin Moran (William & Mary University), Sunil Manandhar (William & Mary University), Adwait Nadkarni (William & Mary University)and Denys Poshyvanyk (William & Mary University)*
	Detection of Threats to IoT Devices Using Scalable VPN-forwarded Honeypots *Amit Tambe (Singapore University of Technology and Design), Yan Lin Aung (Singapore University of Technology and Design), Ragav Sridharan (Singapore University of Technology and Design), Martin Ochoa (Universidad del Rosario), Nils Ole Tippenhauer (Center for It-Security, Privacy & Accountability (CISPA)), Asaf Shabtai (Ben Gurion University of the Negev), and Yuval Elovici (Singapore University of Technology and Design)*
3:50-4:20p	Break

	Session 3 Data Security and Privacy
	Session Chair: Vassil Roussev, University of New Orleans
4:20-6:00p	**Deep Neural Networks Classification over Encrypted Data** *Ehsan Hesamifard (University of North Texas), Hassan Takabi (University of North Texas) and Mehdi Ghasemi (University of Saskatchewan)*
	Attribute Compartmentation and Greedy UCC Discovery for High-Dimensional Data Anonymization *Nikolai Jannik Podlesny (Hasso-Plattner-Institute), Anne V.D.M. Kayem (Hasso-Plattner-Institute), and Christoph Meinel (Hasso-Plattner-Institute)*
	Curie: Policy-based Secure Data Exchange *Z. Berkay Celik (The Pennsylvania State University), Abbas Acar (Florida International University), Hidayet Aksu (Florida International University), Ryan Sheatsley (The Pennsylvania State University), A. Selcuk Uluagac (Florida International University), and Patrick McDaniel (The Pennsylvania State University)*
	Result-Based Detection of Insider Threats to Relational Databases *Asmaa Sallam (Purdue University), and Elisa Bertino (Purdue University)*
6:00-6:30p	Break
6:30p	Session 4 **RECEPTION AND POSTER SESSION (SALON EFG)**
	Session Chair: Hongxin Hu, Clemson University

CODASPY Main Conference, Tuesday, March 26th, 2019

	Day 2 (Salon D)
	Session Chair: Bhavani Thuraisingham, The University of Texas at Dallas
9:00-10:00a	**Conference Keynote II** ***Using AI to Detect Attacks and Manage Access Control*** Anupam Joshi (University of Maryland, Baltimore County)
10:00-10:30	Break
	Session 5 Access Control and Information Flow
	Session Chair: Murat Kantarcioglu, The University of Texas at Dallas
10:30a-12:10p	**Specification and Analysis of ABAC Policies via the Category-based Metamodel** *Maribel Fernandez (King's College London), Ian Mackie (LIX) and Bhavani Thuraisingham (The University of Texas at Dallas)*
	Results in Workflow Resiliency: Complexity, New Formulation, and ASP Encoding *Philip W. L. Fong (University of Calgary)*
	Efficient and Precise Information Flow Control for Machine Code through Demand-Driven Secure Multi-Execution *Tobias Pfeffer (TU Berlin), Thomas Göthel (TU Berlin), and Sabine Glesner (TU Berlin)*
	PoLPer: Process-Aware Restriction of Over-Privileged Setuid Calls in Legacy Applications *Yuseok Jeon (Purdue University), Junghwan Rhee (NEC Laboratories America), Chung Hwan Kim (NEC Laboratories America), Zhichun Li (NEC Laboratories America), Mathias Payer (Purdue University), Byoungyoung Lee (Seoul National University) and Zhenyu Wu (NEC Laboratories America)*
12:10-1:10p	Lunch (Salon EFG)
1:10-2:50p	**Panel: AI + Cyber Security + Big Data** (Salon D) *Latifur Khan, Moderator (The University of Texas at Dallas), Rakesh Verma (University of Houston), Anoop Singhal, (NIST), Cuneyt Akcora (The University of Texas at Dallas), Hongxin Hu (Clemson University)*
2:50-3:20p	Break
	Session 6 Hardware Assisted Data Security
	Session Chair: Rakesh Verma, University of Houston
3:20-5:00p	**Extracting Secrets from Encrypted Virtual Machines** *Mathias Morbitzer (Fraunhofer), Manuel Huber (Fraunhofer), and Julian Horsch (Fraunhofer)*
	Careful-Packing: A Practical and Scalable Anti-Tampering Software Protection Enforced by Trusted Computing *Flavio Toffalini (Singapore University of Technology and Design), Martín Ochoa (Universidad del Rosario), Jun Sun (Singapore University of Technology and Design), and Jianying Zhou (Singapore University of Technology and Design)*
	Behind Enemy Lines: Exploring Trusted Data Stream Processing on Untrusted Systems *Cory Thoma (University of Pittsburgh), Adam J. Lee (University of Pittsburgh), and Alexandros Labrinidis (University of Pittsburgh)*
	A Practical Intel SGX Setting for Linux Containers in the Cloud *Dave Tian (University of Florida), Joseph Choi (University of Florida), Grant Hernandez (University of Florida), Patrick Traynor (University of Florida), and Kevin Butler (University of Florida)*
5:00-6:00p	Break
6:00p	Banquet (Salon EFG)

CODASPY Main Conference, Wednesday, March 27th, 2019

	Day 3 (Salon D)
	Session 7 Web Security and Privacy
	Session Chair: Ram Krishnan, The University of Texas at San Antonio
8:30-10:10a	**Limitless HTTP in an HTTPS World: Inferring the Semantics of the HTTPS Protocol Without Decryption** *Blake Anderson (Cisco), Andrew Chi (The University of North Carolina at Chapel Hill), Scott Dunlop (Cisco) and David McGrew (Cisco)*
	Client Diversity Factor in HTTPS Webpage Fingerprinting *Hasan Alan (The University of North Carolina at Chapel Hill) and Jasleen Kaur (The University of North Carolina at Chapel Hill)*
	Adversarial Author Attribution in Open-source Projects *Alina Matyukhina (University of New Brunswick), Natalia Stakhanova (University of New Brunswick), Mila Dalla Preda (University of Verona), and Celine Perley (University of New Brunswick)*
	Understanding and Predicting Private Interactions in Underground Forums *Zhibo Sun (Arizona State University), Carlos E. Rubio-Medrano (Arizona State University), Ziming Zhao (Arizona State University), Tiffany Bao (Arizona State University), Adam Doupé (Arizona State University), and Gail-Joon Ahn (Arizona State University)*
10:10-10:30a	Break
	Session 8 System Security and Authentication
	Session Chair: Hassan Takabi, University of North Texas
10:30a-12:10p	**BootKeeper: Validating Software Integrity Properties on Boot Firmware Images** *Ronny Chevalier (CentraleSupélec), Stefano Cristalli (University of Milan), Christophe Hauser (University of Southern California), Yan Shoshitaishvili (Arizona State University), Ruoyu Wang (University of California, Santa Barbara), Christopher Kruegel (University of California, Santa Barbara), Giovanni Vigna (University of California, Santa Barbara), Danilo Bruschi (University of Milan) and Andrea Lanzi (University of Milan)*
	MimosaFTL: Adding Secure and Practical Ransomware Defense Strategy to Flash Translation Layer *Peiying Wang (Institute of Information Engineering,Chinese Academy of Sciences), Shijie Jia (Institute of Information Engineering,Chinese Academy of Sciences), Bo Chen (Michigan Technological University), Luning Xia (Institute of Information Engineering,Chinese Academy of Sciences) and Peng Liu (The Pennsylvania State University)*
	BlAnC: Blockchain-based Anonymous and Decentralized Credit Networks *Gaurav Panwar (New Mexico State University), Satyajayant Misra (New Mexico State University), and Roopa Vishwanathan (New Mexico State University)*
	SKA-CaNPT: Secure Key Agreement Using Cancelable and Noninvertible Biometrics Based on Periodic Transformation *Laleh Eskandarian (Sabancı University), Dilara Akdoğan (Sabancı University), Duygu Karaoğlan Altop (Sabancı University), and Albert Levi (Sabancı University)*
12:10p	Take-out Lunch

Workshop on Security and Privacy Analytics (IWSPA) on Wed., March 27th, 2019

8:45-9:00a	Welcome (Longhorn II)
	Session 2: Tutorial
9:00-10:10a	**Tutorial: Clustering for Security Challenges** *Rakesh Verma (University of Houston) and Srivathsan Srinivasagopalan (AT&T Cybersecurity)*
10:10-10:30a	Break
	Session 3: Clustering Tutorial Wrap-up/Privacy Preserving Data Mining Tutorial
10:30a-12:10p	**Privacy Preserving Data Mining** *Lila Ghemri (Texas Southern University)*
12:10-1:10p	Lunch
	Session 4
1:10-2:50p	**On Improving the Effectiveness of Adversarial Training** *Yi Qin (Colorado School of Mines), Ryan Hunt (Colorado School of Mines), and Chuan Yue (Colorado School of Mines)*
	Spears Against Shields: Are Defenders Winning the Phishing War? *Ayman El Aassal (University of Houston) and Rakesh Verma (University of Houston)*
	Using Randomness to Improve Robustness of Tree-based Models Against Evasion Attacks *Fan Yang (University of Maryland Baltimore County), Zhiyuan Chen (University of Maryland Baltimore County), and Aryya Gangopadhyay (University of Maryland Baltimore County)*
2:50-3:20p	Break
	Session 5
3:20-4.40p	**Efficientk-means Using Triangle Inequality on Spark for CyberSecurity Analytics** *Ambika Shrestha Chitrakar (Norwegian University of Science and Technology) and Slobodan Petrovic (Norwegian University of Science and Technology)*
	Computing the Identification Capability of SQL Queries for Privacy Comparison *Muhammad Imran Khan (Insight-centre for Data Analytics), Simon N. Foley (IMT Atlantique), and Barry O'Sullivan (Insight-centre for Data Analytics, University College Cork)*
	Dark Web Content Analysis and Visualization *Sugiu Takaaki (Tokyo Denki University) and Inomata Atsuo (Tokyo Denki University)*

Workshop on Security in Software Defined Networks & Network Function Virtualization (SDN-NFV) on Wed., March 27th, 2019

9:20-9:30a	Welcome (Longhorn III)
	Session 2: Keynote
9:30-10:30a	**Workshop Keynote** ***Cybersecurity Aspects of Heavy Vehicle Digital Forensics*** Jeremy Daily (University of Tulsa)
10:30-11:00a	Break
	Session 3: SDN/NFV-enabled Security Mechanism
	Session Chair: Hongda Li
11:00a-12:00p	**PIQ: Persistent Interactive Queries for Network Security Analytics (F)** *Oliver Michel (University of Colorado Boulder), John Sonchack (University of Pennsylvania), Eric Keller (University of Colorado Boulder), Jonathan M. Smith (University of Pennsylvania)*
	A Blockchain Future for Secure Clinical Data Sharing: A Position Paper (S) *Yan Luo (UMASS Lowell), Hao Jin (UMASS Lowell), Peilong Li (Elizabethtown College)*
	Securing Large-scale Data Transfers in Campus Networks: Experiences, Issues, and Challenges (S) *Deepak Nadig (University of Nebraska-Lincoln), Byrav Ramamurthy (University of Nebraska-Lincoln)*
12:00-1:30p	Lunch
	Session 4: SDN/NFV Security Architecture
	Session Chair: Peilong Li
1:30-2:35p	**A Formal Access Control Model for SE-Floodlight Controller (F)** *Abdullah Al-Alaj (The University of Texas at San Antonio); Ravi Sandhu (The University of Texas at San Antonio); Ram Krishnan (The University of Texas at San Antonio)*
	SDNSOC: Object Oriented SDN Framework (F) *Ankur Chowdhary (Arizona State University); Dijiang Huang (Arizona State University); Gail-Joon Ahn (Arizona State University); Myong Kang (United States Naval Research Laboratory); Anya Kim (United States Naval Research Laboratory); Alexander Velazquez (United States Naval Research Laboratory)*
	Enabling Dynamic Network Access Control with Anomaly-based IDS and SDN (S) *Hongda Li (Clemson University); Feng Wei (Clemson University); Hongxin Hu (Clemson University)*

Full Paper (F); Short Paper (S)

Workshop on Automotive Cybersecurity (AutoSec) on Wednesday, March 27th, 2019

9:20-9:30a	Welcome (Longhorn IV)
	Session 2: Keynote
9:30-10:30a	**Workshop Keynote** ***Cybersecurity Aspects of Heavy Vehicle Digital Forensics*** Jeremy Daily (University of Tulsa)
10:30-11:00a	Break
	Session 3: Secure Vehicle System Designs
11:00a-12:10p	**TOUCAN A proTocol tO secUre Controlled Area Network** *Giampaolo Bella (Università di Catania), Pietro Biondi (Università di Catania), Gianpiero Costantino (IIT-CNR) and Ilaria Matteucci (IIT-CNR)*
	Automotive Intrusion Detection Based on Constant CAN Message Frequencies Across Vehicle Driving Modes *Clinton Young (Iowa State University), Habeeb Olufowobi (Howard University), Gedare Bloom (Howard University) and Joseph Zambreno (Iowa State University)*
	Defending AUTOSAR Safety Critical Systems Against Code Reuse Attacks *Ahmad Nasser (University of Michigan) and Di Ma (University of Michigan)*
12:10-1:10p	Lunch
1:10-2:10p	**Tutorial: The Dawn of Systems Security Research in Connected and Automated Vehicles** *Qi Alfred Chin (University of California, Irvine)*
2:10 - 2:30p	Break
	Session 4: Anomaly Detection for Controller Area Network
2:30-3:40p	**Anomaly Detection for Mixed Transmission CAN Messages Using Quantized Intervals and Absolute Difference of Payloads** *Takuma Koyama (NTT), Toshiki Shibahara (NTT), Keita Hasegawa (NTT), Yasushi Okano (NTT), Masashi Tanaka (NTT) and Yoshihito Oshima (NTT)*
	Anomaly Detection Approach Using Adaptive Cumulative Sum Algorithm for Controller Area Network *Habeeb Olufowobi (Howard University), Uchenna Ezeobi (Howard University), Eric Muhati (Howard University), Gaylon Robinson (Howard University), Clinton Young (Iowa State University), Joseph Zambreno (Iowa State University) and Gedare Bloom (Howard University)*
	Towards a CAN IDS Based on a Neural Network Data Field Predictor *Krzysztof Pawelec (Pennsylvania State University), Robert Bridges (Oak Ridge National Laboratory) and Frank Combs (Oak Ridge National Laboratory)*
3:40-4:00p	Break
	Session 5: Miscellaneous
4:00-5:05p	**Route Derivation Using Distances and Turn Directions** *Marian Waltereit (University of Duisburg-Essen), Maximilian Uphoff (University of Duisburg-Essen) and Torben Weis (University of Duisburg-Essen)*
	Hardware-in-loop based Automotive Embedded Systems Cybersecurity Evaluation Testbed *Qadeer Ahmed (Ohio State University), Pradeep Sharma Oruganti (Ohio State University) and Matt Appel (Ohio State University)*
	TangleCV: Decentralized Technique for Secure Message Sharing in Connected Vehicles *Heena Rathore (Hiller Measurements), Abhay Samant (Hiller Measurements), Murtuza Jadliwala (UTSA) and Amr Mohamed (Qatar University)*

Accepted Posters

Differentially Private Event Detection on Data Streams
Maryam Fanaeepour (Duke University); Ashwin Machanavajjhala (Duke University)

Custom-made Anonymization by Data Analysis Program Provided by Recipient
Wakana Maeda (Fujitsu Laboratories Ltd.); Yuji Yamaoka (Fujitsu Laboratories Ltd.)

ABACaaS: Attribute-Based Access Control as a Service
Augustee Meshram (IIT); Saptarshi Das (IIT); Shamik Sural (IIT, Kharagpur); Jaideep Vaidya (Rutgers University); Vijay Atluri (Rutgers University)

Toward Efficient Spammers Gathering in Twitter Social Networks
Yihe Zhang (University of Louisiana at Lafayette); Hao Zhang (Oracle Inc); Xu Yuan (University of Louisiana at Lafayette)

Large Scale PoC Experiment with 57,000 People to Accumulate Patterns for Lifestyle Authentication
Ryosuke Kobayashi (Mitsubishi Electric Information Systems Corporation); Nobuyuki Saji (Infocorpus, Inc.); Nobuo Shigeta (The University of Tokyo); Rie Yamaguchi (The University of Tokyo)

Scaling Cryptographic Techniques by Exploiting Data Sensitivity at a Public Cloud
Sharad Mehrotra (University of California, Irvine); Shantanu Sharma (University of California, Irvine); Jeffrey Ullman (Stanford University)

Experiments on Malware Clustering
Houtan Faridi (University of Houston); Srivathsan Srinivasagopalan (AlienVault); Rakesh Verma (University of Houston)

Continuous Mining for Periodic Patterns in Time Series of Proximate Relational Queries
Asmaa Sallam (Purdue University); Elisa Bertino (Purdue University)

Posters on Accepted Research Papers

Dynamic Groups and Attribute-Based Access Control for Next-Generation Smart Car
Maanak Gupta (The University of Texas at San Antonio); James Benson (The University of Texas at San Antonio); Farhan Patwa (The University of Texas at San Antonio); Ravi Sandhu (The University of Texas at San Antonio)

Careful-Packing: A Practical and Scalable Anti-Tampering Software Protection Enforced by Trusted Computing
Flavio Toffalini (Singapore University of Technology and Design); Martín Ochoa (Universidad del Rosario); Jun Sun (Singapore University of Technology and Design); Jianying Zhou (Singapore University of Technology and Design)

Deep Neural Networks Classification over Encrypted Data
Ehsan Hesamifard (University of North Texas); Hassan Takabi (University of North Texas); Mehdi Ghasemi (University of Saskatchewan)

A Study of Data Store-based Home Automation
Kaushal Kafle (William & Mary University); Kevin Moran (William & Mary University); Sunil Manandhar (William & Mary University); Adwait Nadkarni (William & Mary University); Denys Poshyvanyk (William & Mary University)

Behind Enemy Lines: Exploring Trusted Data Stream Processing on Untrusted Systems
Cory Thoma (University of Pittsburgh); Adam J. Lee (University of Pittsburgh); Alexandros Labrinidis (University of Pittsburgh)

Understanding the Responsiveness of Mobile App Developers to Software Library Updates
Tatsuhiko Yasumatsu (Waseda University); Takuya Watanabe (NTT Secure Platform Labs / Waseda University); Fumihiro Kanei (NTT Secure Platform Labs); Eitaro Shioji (NTT Secure Platform Labs); Mitsuaki Akiyama (NTT Secure Platform Labs); and Tatsuya Mori (Waseda University / RIKEN AIP)

Curie: Policy-based Secure Data Exchange
Z. Berkay Celik (The Pennsylvania State University); Abbas Acar (Florida International University); Hidayet Aksu (Florida International University); Ryan Sheatsley (The Pennsylvania State University); A. Selcuk Uluagac (Florida International University); Patrick McDaniel (The Pennsylvania State University)

A Practical Intel SGX Setting for Linux Containers in the Cloud
Dave Tian (University of Florida); Joseph Choi (University of Florida); Grant Hernandez (University of Florida); Patrick Traynor (University of Florida); Kevin Butler (University of Florida)

Adversarial Author Attribution in Open-source Projects
Alina Matyukhina (University of New Brunswick); Natalia Stakhanova (University of New Brunswick); Mila Dalla Preda (University of Verona); Celine Perley (University of New Brunswick)

Efficient and Precise Information Flow Control for Machine Code Through Demand-Driven Secure Multi-Execution
Tobias Pfeffer (TU Berlin), Thomas Göthel (TU Berlin), and Sabine Glesner (TU Berlin)

Local Attractions

Dallas Museum of Art [MUSEUM]

1717 N Harwood St; Dallas, TX 75201
Price: Free Operating Hours: Tuesday - Sunday 11am - 5pm, to 9pm Thursday;

This museum is a high-caliber world tour of decorative art from all cultures and time periods. Among the many treasures are Edward Hopper's enigmatic Lighthouse Hill, Frederic Church's lush masterpiece The Icebergs and Rodin's Sculptor and His Muse. Other highlights include exquisite pre-Columbian pottery, carvings and tapestries from Oceania, and a villa modeled on Coco Chanel's Mediterranean mansion (where you can see paintings by Winston Churchill).

Nasher Sculpture Center

2001 Flora St.; Dallas, TX 75201
Operating Hours: Tuesday – Sunday, 11 am – 5 pm;

Located in the heart of the Dallas Arts District, the Nasher Sculpture Center is home to one of the finest collections of modern and contemporary sculptures in the world. The Nasher Sculpture Center presents rotating exhibitions of works from the Nasher family collection as well as special exhibitions drawn from other museums and private collections. In addition to indoor gallery space, the Center contains an auditorium, education and research facilities, a cafe and a store.

GeO-Deck at Reunion Tower [LANDMARK]

300 Reunion Blvd E; Dallas, TX 75207
Operating Hours: 10 am - 10 pm;

To get a sky-high panoramic view of the city, head over to Reunion Tower and take the elevator 470ft up (vertigo sufferers beware) to the top of the impressive GeO-Deck. From the viewing platform you can see the grassy banks of the Trinity River and the distant horizon beyond. Reunion Tower: The city's unofficial architectural symbol rises 50 stories, topped off by a three-level spherical dome with flashing lights. Its iconic observation deck offers 360-degree views of the city.

George W Bush Presidential Library & Museum [MUSEUM]

2943 SMU Blvd; Dallas, TX 75205
Price: adult - $21; Operating Hours: Monday - Saturday 9 am - 5 pm , Sunday 12 pm - 5 pm;

DART: light rail Mockingbird
Opened on the campus of Southern Methodist University (SMU) in 2013, this vast facility documents the presidency of George W Bush. Like other presidential libraries it has two missions: to allow research and to present a record of the president to the public. Exhibits include all manner of gifts Bush received while president. Its most interactive feature is the Decision Points Theater which allows you to see how Bush made decisions around events such as 9/11 and the invasion of Iraq. The approach is genial throughout.

Sixth Floor Museum [MUSEUM]

411 Elm St; Dallas, TX 75202
Price: adult/child - $18/14; Operating Hours: Tuesday - Sunday 10 am - 6 pm, Monday 12 pm - 6 pm;

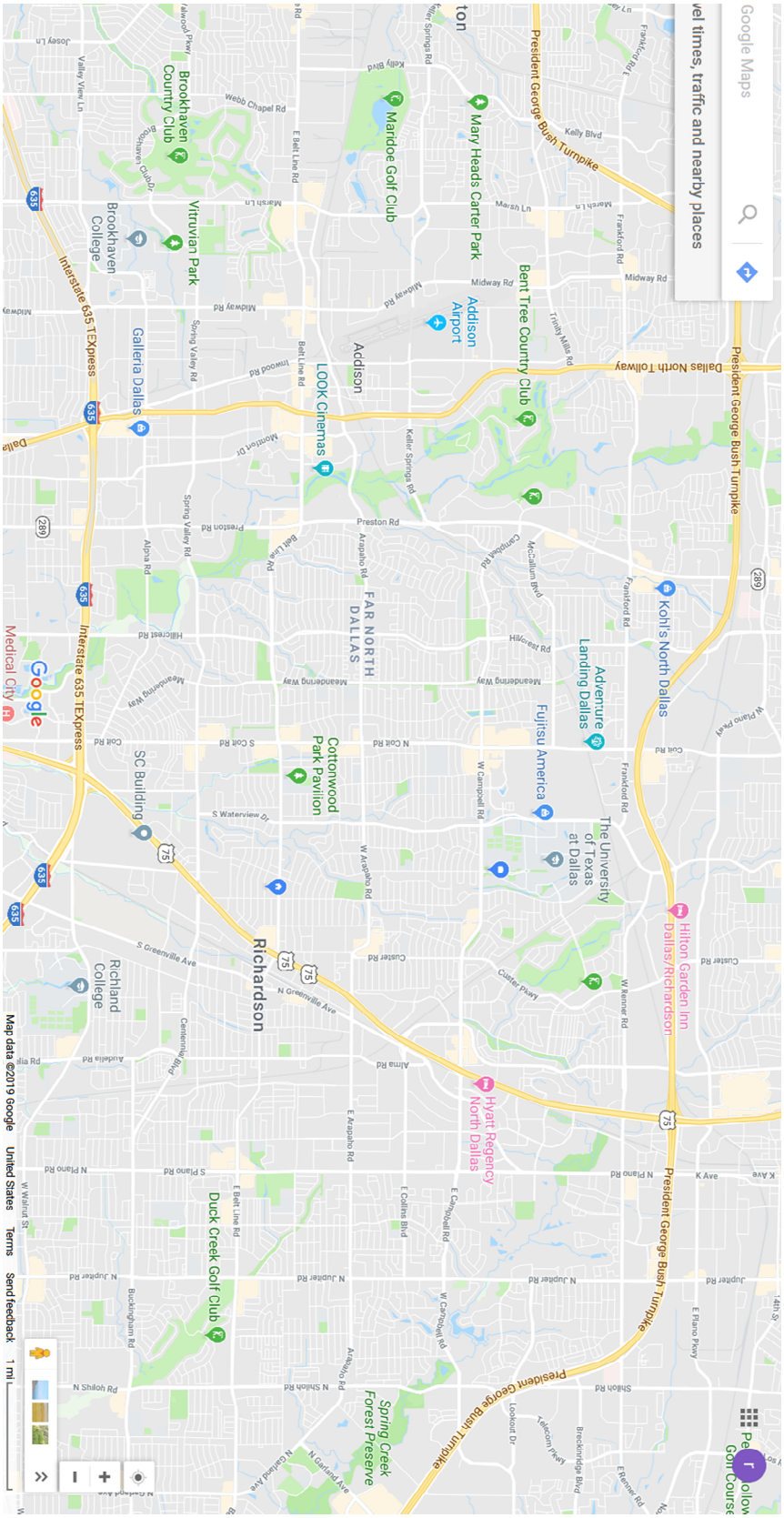
DART: light rail West End Rather than downplay the assassination of John F Kennedy, Dallas gives visitors a unique opportunity to delve into the world-altering events that sent the country reeling in 1963. Fascinating multimedia exhibits inside the former Texas School Book Depository (plus the included audio guide) give an excellent historical context of the president's time, as well as his life and legacy.

Dallas Arboretum

8525 Garland Rd.; Dallas, TX 75218
Price: adult/child - $17/12; Operating hours: Daily 9 am – 5 pm

The Dallas Arboretum is one of the premier places to visit in the Dallas area, and one of the top botanical gardens in America. Dallas Blooms is one of the largest floral festivals in the Southwest, with over 100 varieties of spring-blooming bulbs exploding with color and 500,000 tulips, plus hundreds of thousands of other spring flowers that will dazzle you.

Richardson Area Map



Notes

ACM CODASPY 2019

Notes

ACM CODASPY 2019