October 30–November 3, 2017
Dallas, TX, USA

Association for Computing Machinery

Advancing Computing as a Science & Profession

CCS'17

Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security

Sponsored by:

ACM SIGSAC

Association for
Computing Machinery

Advancing Computing as a Science & Profession

The Association for Computing Machinery
2 Penn Plaza, Suite 701
New York, New York 10121-0701

Notice to Past Authors of ACM-Published Articles

ACM intends to create a complete electronic archive of all articles and/or other material previously published by ACM. If you have written a work that has been previously published by ACM in any journal or conference proceedings prior to 1978, or any SIG Newsletter at any time, and you do NOT want this work to appear in the ACM Digital Library, please inform permissions@acm.org, stating the title of the work, the author(s), and where and when published.

ISBN: 978-1-4503-4946-8

Additional copies may be ordered prepaid from:

ACM Order Department
PO Box 30777
New York, NY 10087-0777, USA

Phone: 1-800-342-6626 (USA and Canada)
+1-212-626-0500 (Global)
Fax: +1-212-944-1318
E-mail: acmhelp@acm.org
Hours of Operation: 8:30 am – 4:30 pm ET

Printed in the USA.

ACM CCS 2017 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 area 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
CCS 2017 General Chair
The University of Texas at Dallas
Richardson, Texas

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 academic, 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 on-line 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 3 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 on-line 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	**Tal Maklin**	**Dongyan Xu**
University of Virginia	*Columbia University*	*Purdue University*

ACM CCS 2017 Program Committee Co-Chairs

Table of Contents

Session A5: Cryptocurrency

Session B1: Multi-Party Computation 2

Session B2: Passwords

Session B3: Investigating Attacks

Session B4: Privacy Policies

Session B5: Blockchains

Session C1: Oblivious RAM

Session C2: World Wide Web of Wickedness

Session C3: Machine Learning Privacy

Session C4: From Verification to ABE

Session C5: Using Blockchains

Session D1: Functional Encryption and Obfuscation

Session D2: Vulnerable Mobile Apps

Session D3: Logical Side Channels

Session D4: Crypto Primitives

Session D5: Network Security

Session E1: Hardening Crypto

Session E2: Securing Mobile Apps

Session E3: Physical Side Channels

Session E4: Adversarial Social Networking

Session E5: Privacy-Preserving Analytics

Session F1: Private Set Intersection

Session F2: Insights from Log(in)s

Session F3: Crypto Pitfalls

Session F4: Private Queries

Session F5: Understanding Security Fails

Session G1: Searchable Encryption

Session G2: Bug-Hunting Risks and Rewards

Session G3: Crypto Standards

Session G4: Voting

Session G5: Hardening Hardware

Session H1: Crypto Attacks

Session H2: Code Reuse Attacks

Session H3: Web Security

Session H4: Formal Verification

Session I1: Post-Quantum

Session I2: Information Flow

Session I3: Personal Privacy

Session I4: Verifying Crypto

Session I5: Communication Privacy

Session J1: Outsourcing

Session J2: Fun with Fuzzing

Session J3: Problematic Patches

Session J4: Flash Security

Session K1: Secure Computation

Session K2: Fuzzing Finer and Faster

Session K3: Program Analysis

Session K4: Secure Enclaves

Demonstration

Posters

Tutorials

Workshop Summaries

CCS 2017 Conference Organization

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)*

Workshops Chairs: Taesoo Kim *(Georgia Tech)*
Cliff Wang *(Army Research Office)*

Tutorial Chairs: Guofei Gu *(Texas A&M)*
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 Chairs: JV Rajendran *(The University of Texas at Dallas)*
Gail-Joon Ahn *(Arizona State 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 Chair: 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 Chair: 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/Chairs: Latifur Khan *(The University of Texas at Dallas)*
Meera Sridhar *(University of North Carolina at Charlotte)*

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 *(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)*

Program Committee *(continued):* Tudor Dumitraș *(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)*
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)*

Program Committee *(continued):* 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)*
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)*

Program Committee *(continued):* 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)*

Additional reviewers: Hadi Abdullah
Gergely Ács
David Adrian
Eman Alashwali
Joey Allen
Myrto Arapinis
Jean-Philippe Aumasson
Christian Badertscher
Xiaolong Bai
Qinkun Bao
Cristina Basescu
Aditya Basu
Carsten Baum
Ingolf Becker
Matt Bernhard
Shengjie Bi
Gergely Biczók
Jorje Blasco Alis
Logan Blue
Raphael Bost
Jasmin Bowers
Ferdinand Brasser
Ahmet S. Buyukkayhan
Frank Capobianco
Sunjay Cauligi
Pyrros Chaidos
Konstantinos Chatzikokolakis
Sze Yiu Chau
Ying Chen
Shang-Tse Chen
Haehyun Cho
Pak Ho Chung
Katriel Cohn Gordon
Christian Decker
Zakir Durumeric
Mohammad Etemad
Daniel Feher
Daniel Fett
Hao Fu
Yu Fu
Joshua Gancher
linus gasser
Linus Gasser
András Gazdag
David Gens
Ilias Giechaskiel
Thomas Gilray
Liang Gong

Additional reviewers *(continued)*: Sergey Gorbunov
Paul Grubbs
Wenbo Guo
Johann Großschädl
Trinabh Gupta
Syed Kamran Haider
Ariel Hamlin
Wajih Ul Hassan
Ben Heidorn
Ethan Heilman
Nadia Heninger
Tamás Holczer
Sanghyun Hong
Hongxin Hu
Hong Hu
Heqing Huang
Zhen Huang
Jun Ho Huh
Siam Hussain
Yong Ho Hwang
Ahmad Ibrahim
Moshen Imani
Yuval Ishai
Saman Jafari
Stanislaw Jarecki
Roberto Jordaney
Yigitcan Kaya
Ryo Kikuchi
Donguk Kim Beom
Doowon Kim
Heyn Kim
Markulf Kohlweiss
Eleftherios Kokoris Kogias Vlad Kolesnikov
Maria Konte
Lucas Kowalczyk
Steve Kremer
Bogdan Kulynych
BumJun Kwon
Yu-Tsung (Eddy) Lee
Yue Li
Tongxin Li
Xiaojing Liao
Christopher Liechen
Yehuda Lindell
Xiao Liu
Andreas Lochbihler
Wouter Lueks
Alex Malozemoff
Andrea Mambretti
Piotr Mardziel
Christian Matt
Xianghang Mi
Reza Mirzazade
Varun Mishra
Esfandiar Mohammadi
Pedro Moreno Sanchez
Johannes Müller
Kartik Nayak
Kirill Nikitin
Ben Niu
Rebekah Overdorf
Simón Oya
Jun Pang
Dimitrios Papadopoulos
Charalampos Papamanthou
Bryan Parno
Marcus Peinado
Leo Perrin
Travis Peters
Giuseppe Petracca
Tim Pierson
Benny Pinkas
Yu Pu
Apostolos Pyrgelis
Rui Qiao
Samuel Ranellucci
Daniel Rausch
Bradley Reaves
M. Sadegh Riazi
Silas Richelson
Marc Roeschlin
Kurt Rohloff

Additional reviewers *(continued)*:

Carlos Rubio Medrano
Ralf Sasse
Nolen Scaife
Guillaume Scerri
Guido Schmitz
Peter Scholl
Will Scott
Sovantharith Seng
Srinath Setty
Daniele Sgandurra
Junbum Shin
Victor Shoup
Payap Sirinam
Gary Soeller
Linhai Song
Ebrahim Songhori
Christoph Sprenger
Drew Springall
Rock Stevens
Octavian Suciu
Yuqiong Sun
Jianhua Sun
Pengfei Sun
Peter Yi
Ping Sun
Zhibo Sun
Stefano Tessaro
Aleksei Udovenko
Jonathan Ullman
Diego Valasquez
Ben VanderSloot
Luis Vargas
Daniel Votipka
Kyle Wallace
Shengye Wan
Boyang Wang
Pei Wang
Shuai Wang
Xiao Wang
Qinglong Wang
Weiren Wang
Li Wang
Xueqiang Wang
Wenhao Wang
Bogdan Warinschi
Daniel Wichs
Michelle Wong
David Wu
Xiaodi Wu
Eric Wustrow
Willem Wyndham
Weilin Xu
Zhang Xu
Dongpeng Xu
Carter Yagemann
Moosa Yahyazadeh
Yang Yang
Insu Yun
Santiago Zanella Béguelin
Danfeng Zhang
Ning Zhang
Tianwei Zhang
Xiaokuan Zhang
Kaixuan Zhang
Ziming Zhao
Yajin Zhou
Ruiyu Zhu
Ziyun Zhu

PLATINUM

Special Thanks To:

GOLD

SILVER

BRONZE