Message from the General Chair..................................................................................................................xi
Message from the Program Committee Co-Chairs......................................................................................xiv
Organizing Committee....................................................................................................................................xv
Program Committee.......................................................................................................................................xvii
External Reviewers...........................................................................................................................................xix

Hardware and Private Execution

HDFI: Hardware-Assisted Data-Flow Isolation ..............................................................................................1
    Chengyu Song, Hyungon Moon, Monjur Alam, Insu Yun, Byoungyoung Lee,
    Taesoo Kim, Wenke Lee, and Yunheung Paek

A2: Analog Malicious Hardware ...................................................................................................................18
    Kaiyuan Yang, Matthew Hicks, Qing Dong, Todd Austin, and Dennis Sylvester

Cache Storage Channels: Alias-Driven Attacks and Verified Countermeasures ...........................................38
    Roberto Guanciale, Hamed Nemati, Christoph Baumann, and Mads Dam

Shreds: Fine-Grained Execution Units with Private Memory ......................................................................56
    Yaohui Chen, Sebassujeen Reymondjohnson, Zhichuang Sun, and Long Lu

CaSE: Cache-Assisted Secure Execution on ARM Processors ......................................................................72
    Ning Zhang, Kun Sun, Wenjing Lou, and Y. Thomas Hou

Analyze Me

Back in Black: Towards Formal, Black Box Analysis of Sanitizers and Filters ..........................................91
    George Argyros, Ioannis Stais, Aggelos Kiayias, and Angelos D. Keromytis

LAVA: Large-Scale Automated Vulnerability Addition .............................................................................110
    Brendan Dolan-Gavitt, Patrick Hulin, Engin Kirda, Tim Leek, Andrea Mambretti,
    Wil Robertson, Frederick Ulrich, and Ryan Whelan

Prepose: Privacy, Security, and Reliability for Gesture-Based Programming ............................................122
    Lucas Silva Figueiredo, Benjamin Livshits, David Molnar, and Margus Veanes
SOK: (State of) The Art of War: Offensive Techniques in Binary Analysis ........................................... 138
  Yan Shoshitaishvili, Ruoyu Wang, Christopher Salls, Nick Stephens,
  Mario Polino, Andrew Dutcher, John Grosen, Siji Feng, Christophe Hauser,
  Christopher Kruegel, and Giovanni Vigna

Helping Johnny to Analyze Malware: A Usability-Optimized Decompiler
and Malware Analysis User Study ................................................................. 158
  Khaled Yakdan, Sergej Dechand, Elmar Gerhards-Padilla, and Matthew Smith

Oblivious and Snarky
A Practical Oblivious Map Data Structure with Secure Deletion and History
Independence ........................................................................................................ 178
  Daniel S. Roche, Adam Aviv, and Seung Geol Choi

TaoStore: Overcoming Asynchronicity in Oblivious Data Storage ........................................... 198
  Cetin Sahin, Victor Zakary, Amr El Abbadi, Huijia Lin, and Stefano Tessaro

Revisiting Square-Root ORAM: Efficient Random Access in Multi-party
Computation ........................................................................................................... 218
  Samee Zahur, Xiao Wang, Mariana Raykova, Adrià Gascón, Jack Doerner,
  David Evans, and Jonathan Katz

Cinderella: Turning Shabby X.509 Certificates into Elegant Anonymous
Credentials with the Magic of Verifiable Computation ........................................... 235
  Antoine Delignat-Lavaud, Cédric Fournet, Markulf Kohlweiss, and Bryan Parno

PhotoProof: Cryptographic Image Authentication for Any Set of Permissible
Transformations ........................................................................................................ 255
  Assa Naveh and Eran Tromer

Call Me on Usable Security
I Think They're Trying to Tell Me Something: Advice Sources and Selection
for Digital Security .............................................................................................. 272
  Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek

You Get Where You're Looking for: The Impact of Information Sources
on Code Security .................................................................................................. 289
  Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim,
  Michelle L. Mazurek, and Christian Stransky

Users Really Do Plug in USB Drives They Find ..................................................... 306
  Matthew Tischer, Zakir Durumeric, Sam Foster, Sunny Duan, Alec Mori,
  Elie Bursztein, and Michael Bailey

SoK: Everyone Hates Robocalls: A Survey of Techniques Against Telephone
Spam ....................................................................................................................... 320
  Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways</td>
<td>339</td>
</tr>
<tr>
<td><em>Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin R. B. Butler</em></td>
<td></td>
</tr>
<tr>
<td>Phoning it in</td>
<td>357</td>
</tr>
<tr>
<td>Following Devil's Footprints: Cross-Platform Analysis of Potentially Harmful Libraries on Android and iOS</td>
<td></td>
</tr>
<tr>
<td><em>Kai Chen, Xueqiang Wang, Yi Chen, Peng Wang, Yeonjoon Lee, XiaoFeng Wang, Bin Ma, Aohui Wang, Yingjun Zhang, and Wei Zou</em></td>
<td></td>
</tr>
<tr>
<td>TriggerScope: Towards Detecting Logic Bombs in Android Applications</td>
<td>377</td>
</tr>
<tr>
<td><em>Yanick Fratantonio, Antonio Bianchi, William Robertson, Engin Kirda, Christopher Kruegel, and Giovanni Vigna</em></td>
<td></td>
</tr>
<tr>
<td>Inferring User Routes and Locations Using Zero-Permission Mobile Sensors</td>
<td>397</td>
</tr>
<tr>
<td><em>Sashank Narain, Triet D. Vo-Huu, Kenneth Block, and Guevara Noubir</em></td>
<td></td>
</tr>
<tr>
<td>No Pardon for the Interruption: New Inference Attacks on Android Through Interrupt Timing Analysis</td>
<td>414</td>
</tr>
<tr>
<td><em>Wenrui Diao, Xiangyu Liu, Zhou Li, and Kehuan Zhang</em></td>
<td></td>
</tr>
<tr>
<td>SoK: Lessons Learned from Android Security Research for Appified Software Platforms</td>
<td>433</td>
</tr>
<tr>
<td><em>Yasemin Acar, Michael Backes, Sven Bugiel, Sascha Fahl, Patrick McDaniel, and Matthew Smith</em></td>
<td></td>
</tr>
</tbody>
</table>

**Key Exchange and Certificates**

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Confirmation in Key Exchange: A Formal Treatment and Implications for TLS 1.3</td>
<td>452</td>
</tr>
<tr>
<td><em>Marc Fischlin, Felix Günther, Benedikt Schmidt, and Bogdan Warinschi</em></td>
<td></td>
</tr>
<tr>
<td>Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication</td>
<td>470</td>
</tr>
<tr>
<td><em>Cas Cremers, Marko Horvat, Sam Scott, and Thyla van der Merwe</em></td>
<td></td>
</tr>
<tr>
<td>Multiple Handshakes Security of TLS 1.3 Candidates</td>
<td>486</td>
</tr>
<tr>
<td><em>Xinyu Li, Jing Xu, Zhenfeng Zhang, Dengguo Feng, and Honggang Hu</em></td>
<td></td>
</tr>
<tr>
<td>Downgrade Resilience in Key-Exchange Protocols</td>
<td>506</td>
</tr>
<tr>
<td><em>Karthikeyan Bhargavan, Christina Brzuska, Cédric Fournet, Matthew Green, Markulf Kohlweiss, and Santiago Zanella-Béguelin</em></td>
<td></td>
</tr>
<tr>
<td>Keeping Authorities &quot;Honest or Bust&quot; with Decentralized Witness Cosigning</td>
<td>526</td>
</tr>
<tr>
<td><em>Ewa Syta, Iulia Tamas, Dylan Visher, David Isaac Wolinsky, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, and Bryan Ford</em></td>
<td></td>
</tr>
</tbody>
</table>
Learning about Privacy

Synthesizing Plausible Privacy-Preserving Location Traces ..........................................................546
Vincent Bindschaedler and Reza Shokri

A Method for Verifying Privacy-Type Properties: The Unbounded Case ............................................564
Lucca Hirschi, David Baelde, and Stéphanie Delaune

Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks .........................................................582
Nicolas Papernot, Patrick McDaniel, Xi Wu, Somesh Jha, and Ananthram Swami

Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems ..................................................................................................................598
Anupam Datta, Shayak Sen, and Yair Zick

Vulnerabilities

Talos: Neutralizing Vulnerabilities with Security Workarounds for Rapid Response ........................................................618
Zhen Huang, Mariana D’Angelo, Dhaval Miyani, and David Lie

Security Analysis of Emerging Smart Home Applications ........................................................................636
Earlence Fernandes, Jaeyeon Jung, and Atul Prakash

Staying Secure and Unprepared: Understanding and Mitigating the Security Risks of Apple ZeroConf ..........................................................................................................................655
Xiaolong Bai, Luyi Xing, Nan Zhang, XiaoFeng Wang, Xiaojing Liao, Tongxin Li, and Shi-Min Hu

Don’t Go on the Web

MitM Attack by Name Collision: Cause Analysis and Vulnerability Assessment in the New gTLD Era .............................................................................................................................................675
Qi Alfred Chen, Eric Osterweil, Matthew Thomas, and Z. Morley Mao

Domain-Z: 28 Registrations Later Measuring the Exploitation of Residual Trust in Domains .........................................................................................................................691
Chaz Lever, Robert Walls, Yacin Nadji, David Dagon, Patrick McDaniel, and Manos Antonakakis

Seeking Nonsense, Looking for Trouble: Efficient Promotional-Infection Detection through Semantic Inconsistency Search .............................................................................................................707
Xiaojing Liao, Kan Yuan, XiaoFeng Wang, Zhongyu Pei, Hao Yang, Jianjun Chen, Haixin Duan, Kun Du, Eihal Alowaish, Sumayah Alrwais, Luyi Xing, and Raheem Beyah

The Cracked Cookie Jar: HTTP Cookie Hijacking and the Exposure of Private Information .................................................................................................................................724
Suphannee Sivakorn, Iasonas Polakis, and Angelos D. Keromytis
Cloak of Visibility: Detecting When Machines Browse a Different Web .................................................743

Luca Invernizzi, Kurt Thomas, Alexandros Kapravelos, Oxana Comanescu,
Jean-Michel Picod, and Elie Bursztein

Applied Cryptography

Verifiable ASICs ........................................................................................................................................759

Riad S. Wahby, Max Howald, Siddharth Garg, Abhi Shelat, and Michael Walfish

SoK: Verifiability Notions for E-Voting Protocols ..................................................................................779

Véronique Cortier, David Galindo, Ralf Küsters, Johannes Müller,
and Tomasz Truderung

pASSWORD tyPOS and How to Correct Them Securely .................................................................799

Rahul Chatterjee, Anish Athayle, Devdatta Akhawe, Ari Juels,
and Thomas Ristenpart

On the Practicality of Cryptographically Enforcing Dynamic Access Control Policies in the Cloud .................................................................819

William C. Garrison III, Adam Shull, Steven Myers, and Adam J. Lee

Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts .................................................................839

Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen,
and Charalampos Papamanthou

What? You Want More?

High-Speed Inter-Domain Fault Localization ..................................................................................859

Cristina Basescu, Yue-Hsun Lin, Haoming Zhang, and Adrian Perrig

Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints ................................................................................878

Pierre Laperdrix, Walter Rudametkin, and Benoit Baudry

Verena: End-to-End Integrity Protection for Web Applications .........................................................895

Nikolaos Karapanos, Alexandros Filios, Raluca Ada Popa, and Srdjan Capkun

SoK: Towards Grounding Censorship Circumvention in Empiricism .................................................914

Michael Carl Tschantz, Sadia Afroz, Anonymous, and Vern Paxson

Low-Level Attacks and Defenses

A Tough Call: Mitigating Advanced Code-Reuse Attacks at the Binary Level .................................................934

Victor van der Veen, Enes Göktas, Moritz Contag, Andre Pawoloski, Xi Chen,
Sanjay Rawat, Herbert Bos, Thorsten Holz, Elias Athanasopoulos,
and Cristiano Giuffrida