SaTS '24: The 2nd ACM Workshop on Secure and Trustworthy Superapps

Zhiqiang Lin
The Ohio State University
Columbus, USA
zlin@cse.ohio-state.edu

Luyi Xing
Indiana University Bloomington
Bloomington, USA
luyixing@iu.edu

Abstract

Mobile super apps are revolutionizing mobile computing by offering diverse services through integrated "miniapps", creating comprehensive ecosystems akin to app stores like Google Play and Apple's App Store. While these platforms, such as WeChat, Alipay, and TikTok, enhance user convenience and functionality, they also raise significant security and privacy concerns due to the vast amounts of user data they handle. In response, the Workshop on Secure and Trustworthy Superapps (SaTS 2024) aims to address these critical issues by fostering collaboration among researchers and practitioners to explore solutions that protect users and enhance security within the super app landscape.

CCS Concepts

• **Security and privacy → Systems security**.

Keywords

Super App; Mobile; Web; Security

ACM Reference Format:
Zhiqiang Lin and Luyi Xing. 2024. SaTS '24: The 2nd ACM Workshop on Secure and Trustworthy Superapps. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3658644.3691542

1 Introduction

Mobile super apps represent a transformative shift in mobile computing. These platforms, offering a wide array of services through integrated "miniapps," have experienced rapid growth in recent years. Miniapps, functioning similarly to native apps, enable super apps to build comprehensive ecosystems, much like Google Play or the Apple App Store. This ecosystem not only expands the super app's capabilities but also provides users with enhanced convenience and seamless functionality.

However, the rise of popular super apps like WeChat, Alipay, TikTok, and Grab has led to the generation, storage, and transmission of vast amounts of user data. The integration of numerous services within a single platform amplifies security and privacy risks, drawing the attention of users, researchers, and regulators alike. These challenges underline the growing need for robust privacy protections and secure practices within the super app landscape.

In response to these developments, the Workshop on Secure and Trustworthy Superapps (SaTS 2024), co-located with ACM CCS 2024, offers a timely platform for addressing the pressing security and privacy challenges posed by super apps. As these apps become essential tools for communication, entertainment, and commerce, they also introduce significant risks. SaTS 2024 aims to bring together researchers and practitioners to discuss these issues and explore solutions that benefit the security community, industry, and society. The workshop's primary goal is to highlight these concerns and create a collaborative environment for knowledge sharing and problem-solving.

2 Workshop Format

SaTS '24 is a full-day workshop held alongside ACM CCS 2024, featuring a diverse range of contributions, including research papers, short/work-in-progress papers, and invited talks. The event brings together authors, organizers, and participants, creating an engaging space for knowledge exchange and collaboration. In particular, SaTS '24 offers a platform for two distinct categories of papers:

- Regular Papers (up to 8 pages): These papers present original research that has not been previously published or submitted concurrently elsewhere.
- Short Papers or Work-in-Progress Papers (up to 4 pages): This category accommodates papers that focus on fostering discussion, collaboration, and the sharing of preliminary research activities, work in progress, and industrial innovations.

The event is further enhanced by three keynote talks from experts, covering topics from miniapp standardization, data protection and access control, and malicious software in the ecosystems, offering broader context and sparking discussions. These talks deepen the workshop's insights and highlight ways to address challenges and opportunities in secure and trustworthy superapps.

3 Topics of Interest

Topics of interest include (but are not limited to) the following.

- Privacy-preserving techniques for mobile super apps (including their miniapps)
- Security analysis of mobile super app ecosystems
- Authentication and authorization mechanisms for super apps
- Data protection and secure storage in super apps
- Privacy policies, compliance, and regulations for mobile super apps
- User behavior and privacy risk analysis

CCS '24, October 14–18, 2024, Salt Lake City, UT, USA

ACM ISBN 979-8-4007-0636-3/24/10
https://doi.org/10.1145/3658644.3691542

- Surveillance and censorship in mobile super apps
- Anonymity and pseudonymity in miniapp communication
- Security and privacy issues in third-party integrations
- Secure payment systems in mobile super apps
- Case studies and real-world experiences with mobile super app security and privacy

In addition, topics of interest include, but are not limited to other emerging paradigms in mobile and ubiquitous computing.

4 Workshop Organizers

Zhiqiang Lin is a Distinguished Professor of Engineering, and the director of Institute for Cybersecurity and Digital Trust (ICDT) at The Ohio State University. His research focuses on developing automated program analysis techniques for vulnerability discovery and malware analysis, as well as hardening systems and software using binary code rewriting, virtualization, and trusted execution environments. He has published over 150 papers on these and related topics. Recently, his team has been intensively studying the security and privacy of mobile super apps, and currently is ranked #2 worldwide in Tencent's security hall of fame He is an IEEE Fellow, and ACM Distinguished Member and has received numerous awards, including the NSF CAREER award, the AFOSR YIP award, Harrison Award for Excellence in Engineering Education, and Outstanding Teaching Award. He received his Ph.D. in Computer Science from Purdue University. He has been involved in organizing multiple conferences and workshops. This includes being program co-chairs for SECURECOMM'22, AsiaCCS'21, ISC'19, FEAST'10, local arrangement chair for CCS'17, and steering committee member for RAID and ISC.

Luyi Xing is an Associate Professor of Computer Science at Indiana University Bloomington. He is a recipient of NSF CAREER award (2021), Facebook Research Award (2021, Privacy Enhancing Technologies), 5 Facebook Whitehat awards (2012, 2013, 2020, 2021), Google Developer Data Protection award (2019), Microsoft Whitehat award (2019), Android Security Acknowledgements (2013 - 2016, 2018), Apple Security Acknowledgement (2015, 2019, 2020), among others. His research focus includes formal methods and guarantees for security and privacy-compliance in systems, in particular, IoT, cloud, mobile, and software supply chain. His research is known to impact security design of hundreds of operating system modules, applications, online/network services that almost everyone uses everyday, with the discovery of 50+ new types of vulnerabilities, uncovering new attack techniques and undermining modern security guarantees/assumptions. His works have been published almost exclusively at top-tier security venues. He is a co-founder and co-chair of the Workshop on Security and Privacy in Standardized IoT co-located with NDSS 2024 and 2025.

5 Committee

We highly appreciate the efforts of our Steering and Program Committees and would like to thank all members for their support.

Steering Committee

- Zhiqiang Lin (The Ohio State University)
- Luyi Xing (Indiana University Bloomington)
- Adam Doupe (Arizona State University)
- Nick Nikiforakis (Stony Brook University)
- Ben Stock (CISPA Helmholtz Center for Information Security)

Technical Program Committee Chairs

- Zhiqiang Lin (The Ohio State University)
- Luyi Xing (Indiana University Bloomington)

Technical Program Committee

- Adwait Nadkarni (William & Mary)
- Aurore Fass (CISPA Helmholtz Center for Information Security)
- Ding Li (Peking University)
- Daniel Luo (The Hong Kong Polytechnic University)
- Haoyu Wang (Huazhong University of Science and Technology)
- Jianyi Zhang (Beijing Electronic Science and Technology Institute)
- Omar Alrawi (Georgia Institute of Technology)
- Soteris Demetriou (Imperial College London)
- Wei You (Renmin University of China)
- Yanjie Zhao (Monash University)
- Yue Xiao (IBM Research)
- Yuan Zhang (Fudan University)
- Yue Zhang (The Ohio State University)
- Yuhong Nan (Sun Yat-sen University)
- Kaushal Kafle (University of South Florida)

Publicity Chair

- Yue Xiao (IBM Research)

6 Workshop Statistics

In its second edition, the workshop received a total of four submissions. All four submissions were accepted for inclusion in the workshop proceedings, comprising two full-length research papers and two works-in-progress papers. A noteworthy aspect of this edition was our deliberate choice to adopt a more inclusive stance on paper acceptance. This decision aligns with our primary objective of creating an environment that fosters open and inclusive discussions. By adopting a more inclusive acceptance policy, we aimed to embrace a diverse range of ideas and encourage active participation from all contributors. We are eager to build upon this foundation in future editions as we continue to foster insightful and inclusive discussions within our academic community.

7 Acknowledgement

We extend our sincere gratitude to the organizing committee of ACM CCS 2024 for graciously accepting and hosting our workshop, as well as for their invaluable support. We also appreciate all committee members for generously dedicating their time and expertise, which have greatly enriched the workshop's quality and impact. Last but not least, we would like to thank the authors and attendees for their contributions and participation. This work is partially supported by grants from the National Science Foundation (CNS-2330264 and CNS-2330265).