With technological advancements, our computers, mobile devices, and IoT devices (e.g., smart locks) have become our identities as they collect, store, and process sensitive personal information such as identity numbers, bank account credentials, and passwords. The amount of sensitive user information generated and handled by these technologies is enormous. Therefore, it is more important than ever to protect these devices with robust security and privacy mechanisms. In this manner, I have been actively conducting *system security* research with a special focus on practical and impactful perspectives. In my research, the fundamental building blocks are cryptographic constructions and machine learning (ML) techniques. I leverage state-of-the-art cryptographic tools and ML mechanisms, such as homomorphic encryption and differential privacy, to create privacy-aware and secure frameworks, while also harnessing ML techniques including traditional ML, deep learning, or federated learning for the development of robust intrusion detection systems.

Impact and Recognition. My contributions have been recognized in academic circles with over **1700 citations** to date. I have successfully presented my findings at top-tier security conferences, resulting in four top-tier publications and journals. Specifically, I published **four top-tier papers**, including three NDSS, one USENIX Security Symposium, and five journal articles, including IEEE TMC, and ACM TOPS. My research also resulted in NSF funding and patents. I was the leading researcher and instrumental in the writing of an NSF proposal "SaTC: TTP: Small: Collaborative: Privacy-Aware Wearable-Assisted Continuous Authentication Framework", which received half a million dollars in research funding. We also received a patent for our innovative approach to wearable-assisted authentication and my research has been highlighted several times in the media.

Prior and Ongoing Research

(1) Android Security: [NDSS '24]: Android is by far the most popular OS with over three billion active mobile devices. As in any software, uncovering vulnerabilities on Android devices and applying timely patches are both critical. Android Open Source Project (AOSP) has initiated efforts to improve the traceability of security updates through Security Patch Levels (SPLs) assigned to devices. While this initiative provided better traceability for the vulnerabilities, it has not entirely resolved the issues related to the timeliness and availability of security updates for end users. Recent studies on Android security updates have focused on the issue of delay during the security update roll-out, largely attributing this to factors related to fragmentation. However, these studies fail to capture the entire Android ecosystem as they primarily examine flagship devices or do not paint a comprehensive picture of the Android devices' lifecycle due to the datasets spanning over a short timeframe. To address this gap in the literature, we utilize a device-centric approach to analyze the security update behavior of Android devices. We obtained 367K official security update records from public sources, spanning from 2014 to 2023. Our dataset contains 599 unique devices from four major OEMs that are used in 97 countries and are associated with 109 carriers. We identify significant differences in the roll-out of security updates across different OEMs, device models/types, and geographical regions across the world. This paper has recently been accepted by NDSS 2024 [6][1].

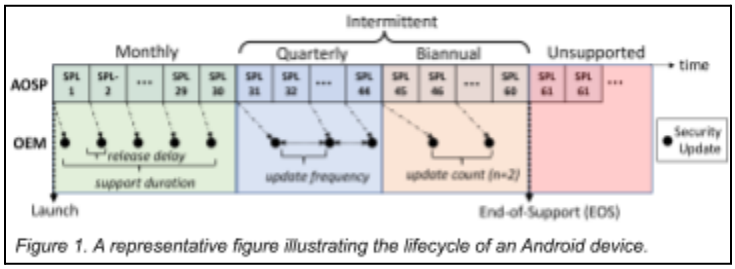

Figure 1. A representative figure illustrating the lifecycle of an Android device.

(2) (In)Security of Modern Web Applications: [USENIX Security '23]: File System Access (FSA) API enables web applications to interact with files on the users' local devices. Even though it can be used to develop rich web

[1] References refer the numbers in my CV.

applications, it greatly extends the attack surface, which can be abused by adversaries to cause significant harm. In this paper, for the first time in the literature, we extensively study this new attack vector that can be used to develop a powerful new ransomware strain over a browser. Using the FSA API and WebAssembly technology, we demonstrate this novel browser-based ransomware called RøB as a malicious web application that encrypts the user's files from the browser. We use RøB to perform impact analysis with different OSs, local directories, and antivirus solutions as well as to develop mitigation techniques against it. Our evaluations show that RøB can encrypt the victim's local files including cloud-integrated directories, external storage devices, and network-shared folders regardless of the access limitations imposed by the API. This paper was published in USENIX Security 2023 [7].

(3) Cryptojacking Malware: [NDSS '22]: Recently, cryptojacking malware has become an easy way of reaching and profiting from a large number of victims. Prior works have studied the cryptojacking detection systems focusing on both in-browser and host-based cryptojacking malware. However, none of the earlier works investigated different attack configurations and network settings in this context. For example, an attacker with an aggressive profit strategy may increase computational resources to the maximum utilization to benefit more in a short time, while a stealthy attacker may want to stay undetected longer time on the victim's device. The accuracy of the detection mechanism may differ for an aggressive and stealthy attacker. Not only profit strategies but also the cryptojacking malware type, the victim's device as well as various network settings where the network is fully or partially compromised may play a key role in the performance evaluation of the detection mechanisms. However, no prior works have investigated the impact of cryptojacking malware on IoT devices and compromised smart home networks. In this paper, we first propose an accurate and efficient IoT cryptojacking detection mechanism based on network traffic features, which can detect both in-browser and host-based cryptojacking. We tested our mechanism in various attack configurations and network settings. This paper was published in NDSS 2022 [10].

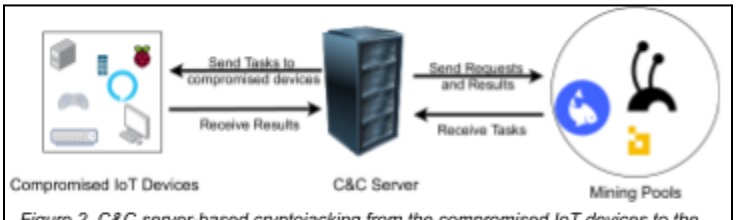

Figure 2. C&C server-based cryptojacking from the compromised IoT devices to the servers.

(4) Alternative Authentication Methods: [IEEE TMC '20]: The one-time login process in conventional authentication systems does not guarantee that the identified user is the actual user throughout the session. However, it is necessary to re-verify the user identity periodically throughout a login session, which is lacking in existing one-time login systems. Continuous authentication, which re-verifies the user identity without breaking the continuity of the session, can address this issue. However, existing methods for Continuous Authentication are either not reliable or not usable. In this work, we designed a novel, usable, and reliable Wearable-Assisted Continuous Authentication (WACA), which relies on sensor-based keystroke dynamics, and the authentication data is acquired through the built-in sensors of a wearable (e.g., smartwatch) while the user is typing. WACA is capable of identifying insider threats with very high accuracy and is also robust against powerful adversaries such as imitation and statistical attackers. This work was published in IEEE Transactions on Mobile Computing in 2020 [3].

(5) Privacy-Preserving Technologies:

[ACM CSUR '18]: Legacy encryption systems depend on sharing a key (public or private) among the peers involved in exchanging an encrypted message. However, this approach poses privacy concerns. The users or service providers with the key have exclusive rights on the data. Especially with popular cloud services, control over the privacy of sensitive data is lost. Even when the keys are not shared, the encrypted material is shared with a third party that does not necessarily need to access the content. Moreover, untrusted servers, providers, and cloud operators can keep identifying elements of users long after users end the relationship with the services. Indeed, Homomorphic Encryption

(HE), a special kind of encryption scheme, can address these concerns as it allows any third party to operate on the encrypted data without decrypting it in advance. Although this extremely useful feature of the HE scheme has been known for over 30 years, the first plausible and achievable Fully Homomorphic Encryption (FHE) scheme, which allows any computable function to perform on the encrypted data, was introduced by Craig Gentry in 2009. Even though this was a major achievement, different implementations so far demonstrated that FHE still needs to be improved significantly to be practical on every platform. Therefore, I have written a highly-cited, impactful survey article, which was published in ACM Computing Surveys (CSUR), focusing on HE and FHE schemes. This paper has received almost 1000 citations since its publication in 2018 [5].

(6) IoT-Smart Home Security and Privacy:

[WiSec '20]: A myriad of IoT devices such as bulbs, switches, and speakers in a smart home environment allow users to easily control the physical world around them and facilitate their living styles through the sensors already embedded in these devices. Sensor data contains a lot of sensitive information about the user and devices. However, an attacker inside or near a smart home environment can potentially exploit the innate wireless medium used by these devices to exfiltrate sensitive information from the encrypted payload (i.e., sensor data) about the users and their activities, invading user privacy. With this in mind, in this work, we introduced a novel multi-stage privacy attack against user privacy in a smart environment. It was realized by utilizing machine learning for detecting and identifying the types of IoT devices, their states, and ongoing user activities in a cascading style. The attack effectively works on both encrypted and unencrypted communications. This paper was published at the ACM WiSec 2020 Conference and has so far received 297 citations in 3 years [14].

Figure 3. Local adversary model considered in this work.

Future Research

(1) Malicious Smart Contracts:

[Ongoing]: Blockchain technology has seen great interest recently. Smart contracts running on the blockchain further advanced this technology by enabling a whole new class of applications called Decentralized Finance (DeFi). However, the premature nature of this technology also attracted attackers, and the attackers used traditional techniques like phishing as well as new techniques like a honeypot or wallet drainer smart contracts to scam the users. The objective of this work is to examine the problem of fraudulent activities involving cryptocurrencies that are widely spread in the context of blockchain technology and smart contracts. By conducting an extensive study and scrutinizing data, the initiative aims to pinpoint the usual trends and susceptibilities that scammers utilize in blockchain systems and smart contracts. Subsequently, the project will suggest and execute efficient approaches and preventive measures to alleviate and preclude cryptocurrency scams in blockchain environments and smart contracts.

(2) Sustainable and Robust Machine Learning:

[Ongoing]: WebAssembly (Wasm) has emerged as a paradigm shift in web development, providing performance-enhancing capabilities for web applications. It is designed as a compilation target for high-level languages and is widely adopted across popular modern browsers and platforms. Its increasing popularity has attracted malicious actors to abuse this technology by distributing malware via WebAssembly modules, leading to its execution on the

client side. Existing protection mechanisms are inadequate as they typically focus only on cryptojacking malware, rely on the source code, or do not account for obfuscation techniques. In this paper, we address the shortcomings of existing defense mechanisms and propose OWASM, a platform-independent deep learning-based detector for malicious obfuscated WebAssembly modules. We trained OWASM on a dataset of more than 9000 unique WebAssembly malicious and benign samples that consider various obfuscation techniques at the source code level. We empirically validate the homogeneity and smooth distribution of our datasets via different dimensionality reduction techniques. Our comprehensive evaluation of OWASM demonstrates an overall detection accuracy of 96.66% with an average F1 score of 96.17%. Compared to prior machine learning and non-machine learning detectors, OWASM shows the best overall performance with low computational costs

[Ongoing]: Android is the most popular mobile operating system worldwide, offering a wide array of mobile applications, from social media platforms and healthcare applications to productivity tools. Unfortunately, these applications might contain potentially malicious code that can infect mobile users. In particular, the malware authors develop sophisticated attack vectors with new malicious functionalities that can bypass detection mechanisms. Consequently, the current Android malware detection systems which mostly rely on advanced learning models exhibit significant performance degradation. In fact, the characteristics of Android malware along with the samples drift over time swiftly, making detection systems unsustainable and our understanding of the malware and technology obsolete. To address these concerns in this project, we propose to design a novel framework - SAMURAI - Sustainable Android Malware Detection via Unlearning with Robustness against Adversarial Inputs. SAMURAI consists of (1) identifying detector models that exhibit aging behaviors (i.e., fails to detect novel Android malware over time), (2) retrieving the root causes of poor performance through statistical and data distribution analysis, (3) updating the model via model-agnostic unlearning, and (4) improving the model's robustness through adversarial training and defensive-knowledge distillation techniques.

Proposals Contributions

I have actively contributed to the following NSF proposals:

- **Privacy-Aware Wearable-Assisted Authentication:**
  Title: "SaTC: TTP: Small: Collaborative: Privacy-Aware Wearable-Assisted Continuous Authentication Framework"
  Role: Primary Researcher and contributed to writing the application
  Status: Grant successfully awarded.
- **Cryptojacking Threat and Mitigation:**
  Title: "SaTC: CORE: Small: Emerging Cryptojacking Threat and Mitigation Methods"
  Role: Primary Researcher and contributed to writing the application
  Status: Submitted.
- **AI Integration into Cybersecurity Education:**
  Title: "EAGER: SaTC-EDU: Designing and Evaluating Curricular Modules for Inclusive Integration of Artificial Intelligence into Cybersecurity"
  Role: Contributed to writing the application
  Status: Grant received.
- **Access Control in Smart Settings:**
  Title: "Collaborative Research: EAGER: Understanding User Needs for Access Control Systems in Smart Settings"
  Role: Contributed to writing the application
  Status: Grant received.