Statement of Research

Kassem M. Fawaz (kassemfawaz.com)

I design and build security and privacy protection systems that have theoretical foundations, and are practical and usable. My Ph.D. research bridges the gap between the theoretical and practical aspects of security and privacy in mobile systems and, more recently, the Internet of Things (IoT).

Background and Current Work

The internet of things (IoT) promises new applications that will improve our quality of life. With the number of connected devices, sensors, and actuators expected to hit 50 billion in 2020 [1], fitness devices, thermostats, door locks, heart pacemakers, cars, and appliances are becoming connected. As these devices touch different aspects of our lives, they, unfortunately, accompany unprecedented threats to us and our environments. These threats are no longer limited to the cyber-space but will extend to the physical space.

While users repeatedly express concern about the associated security and privacy threats, they lack the effective and practical tools to mitigate these threats. My research lies at the intersection of three areas of security and privacy research: *user-centric*, *theoretical*, and *practical* security and privacy. My research builds on the analysis of real-world threats from data collection campaigns. I frequently evaluate my proposed systems by utilizing user studies and surveys. Over the past few years, I have collected data about more than 200 different devices and 1160 mobile apps from hundreds of users; I have run user studies and surveys that included more than 700 individuals. My proposed systems utilize theoretical tools and models to provide security and privacy guarantees. My research incorporates concepts from renewal theory, probabilistic analysis, information disclosure and differential privacy. Recently, I started exploring game-theoretic constructs to develop a theory on cyber-deception. Finally, I made my proposed systems practical to deploy by implementing them on real-world platforms using only commercial-off-the-shelf (COTS) hardware.

The systems I built span several platforms and environments. They address privacy and security issues for Bluetooth Low Energy (BLE-Guardian), voice assistant systems (VAuth), location-aware apps (LP-Guardian and LP-Doctor), indoor mobility tracking environments (PR-LBS), and Android smartphones (Linkdroid). I have published papers describing these systems at the top security, privacy and networking venues (USENIX Security'16, PETS'16, ACM CoNext'16, USENIX Security'15, ACM CCS'14). My work has resulted in several patented technologies [2, 3], and has been incorporated into commercial platforms, such as Qualcomm's recent Smart Protect Technology. I have also coauthored grant proposals to Google and the NSF that funded some of my research. Besides the security and privacy area, I made several research contributions to software systems as well as wireless communications and networks.

Secure Interactions with the Internet of Things

There are two interaction surfaces in the IoT: *device-to-device* (D2D) through dedicated wireless protocols and *human-to-device* (H2D) through user input mechanisms. To inflict damage in an IoT environment, an attacker has to first breach these interaction surfaces. An attacker can then gain unauthorized access to the IoT devices, leading to an array of security and privacy threats. I investigate the security and privacy threats of two representative technologies for D2D and H2D interactions: Bluetooth Low Energy (BLE) and voice-based input.

BLE-Guardian [4]: My study of more than 200 types of BLE-equipped devices has revealed that the BLE protocol, despite its privacy provisions, fails to address the most basic threat of all – hiding the device's presence from curious adversaries. To combat these threats, I proposed BLE-Guardian, a novel device-agnostic system that protects access to BLE-equipped devices. BLE-Guardian efficiently invokes friendly jamming to allow only authorized clients to discover, scan, and connect to the user's BLE-equipped devices. It is effective in combating security and privacy threats, has low overhead, and incurs minimal or no disruption to the legitimate BLE devices. BLE-Guardian achieves its objectives with minimum requirements from an external radio that offers only the basic capabilities of reception and transmission on the 2.4GHz band. BLE-Guardian is currently a patent-pending technology. It has attracted the interest of Hewlett Packard Enterprise which is working on its commercialization and is in negotiations with potential customers.

VAuth [5]: I proposed VAuth, a practical system that provides continuous authentication for voice-enabled IoT devices. As a wearable security token, it supports on-going authentication by matching the user's voice with a supplementary channel that provides physical assurance. In particular, VAuth collects the body surface vibrations of a user via a COTS accelerometer and continuously matches them to the voice commands received by the voice-enabled IoT device. This way, the IoT device only executes a command that originates from the authorized speaker's voice. VAuth defends against threats to voice-enabled devices from impersonation, replay, wireless and mangling voice attacks. It does not require any changes to the existing voice recognition engine of a voice-enabled device. We have filed a provisional patent application to the USPTO that covers VAuth, and we are currently pursuing its commercialization.

Data Privacy Protection

Since the smartphone was introduced, a revolution started; users discovered the convenience of getting driving directions before asking for them, and the comfort of a connected thermostat adjusting the temperature on their way home. These and other context-aware services are enabled by the wealth of collected sensory data and inferred personal habits – a trend that will not slow down with the rise of the IoT computing paradigm. This convenience, however, comes at a considerable security and privacy cost.

Devices, apps and advertisement libraries access the user's data to provide services as well as revenue-generating ads. Data access over time introduces privacy threats that include behavioral tracking, profiling, or even revealing the user's identity. In my thesis, I have proposed several online privacy enhancing mechanisms that reduce the privacy threats from exposing user's data. These mechanisms stand on theoretical privacy criteria, are practical and balance between the user's privacy and utility.

Location Privacy [6, 7]: Most location privacy protection mechanisms, proposed in the literature, do not handle the privacy threats as posed by location-aware apps. To fill this gap in location privacy research, I propose *LP-Guardian* [6], the first *app-aware* framework for location privacy protection on Android platforms, including, but not limited to, smartphones. LP-Guardian anonymizes the user's location before the app can access it. It guarantees that the observed mobility pattern of a certain user is indistinguishable among a theoretical set of individuals. An adversary cannot attribute the observed location information to the real user.

In a follow-up project, I investigated the deployment challenges facing location privacy protection mechanisms. They all require changes either to the underlying platform or the infrastructure making them untenable to be deployed. Therefore, users are left with the location access control of mobile operating systems. My analysis of the location privacy threats posed by 1160 apps for 150 users, over two years, indicated that OSes' location access controls lack granularity and threat awareness. I proposed *LP-Doctor* [7], a lightweight, user-level and open-source Android tool which enables users to be aware of the underlying location privacy threats and exercise fine-grained location access control. LP-Doctor picks a novel privacy criterion that limits information leakage from the location data released to different apps. A user study of 227 participants indicated LP-Doctor's ease of deployability and usability. This work was funded by a Google Faculty Award.

PR-LBS [8]: While LP-Guardian and LP-Doctor focus on outdoor location privacy, indoor environments exhibit different dynamics between users and service providers. Motivated by a survey of 200 shoppers, I proposed PR-LBS (Privacy vs. Reward for Location Based Service), a system that balances the users' privacy concerns and the benefits of sharing location data in indoor location tracking environments. PR-LBS includes three novel online location release mechanisms that achieve differential privacy guarantees and ensure that the user engages in a fair location-service exchange with the service provider. PR-LBS is a general framework; it acts as a broker between users and service providers when the service provider monitors user's mobility through tracking her wearable devices. PR-LBS is currently a patent-pending technology.

LinkDroid [9]: While users presume that their data and app usage behavior are confined within the individual apps, it is not the case in practice. Consistent identifiers, inter-process communication, and third party libraries packed within apps enable an adversary to aggregate user's behavior across independent apps. With my collaborator, I modeled this phenomenon as a dynamic linkability graph (DLG) which abstracts links between different apps. Monitoring the evolution of DLG for 13 users over 47 days revealed that two random apps, installed on the same device, are linkable with a probability of 0.81. To mitigate the linkability threat, I designed and implemented LinkDroid, an Android patch that monitors the DLG at run-time and feeds dummy information to the apps when possible. LinkDroid greatly reduces the linkability privacy threat with a minimal performance overhead and impact on the apps' functionality. We are currently extending LinkDroid to IoT gateways that process personal data streams originating from different IoT devices.

Future Research Agenda

Threats to the IoT devices and environments will continue to present unique challenges in the future, mainly due to device and service provider (SP) heterogeneity. A large and diverse set of manufacturers, developers, and SPs will dominate the IoT ecosystem, giving rise to different device architectures, communication technologies and paradigms, data types, and data sources and sinks. Therefore, we have to rethink security and privacy protection in this evolving era of heterogeneous IoT devices. Building on my research experience, I plan to undertake these challenges as follows.

Usable Security and Privacy: A major challenge related to the mass proliferation of IoT devices is that of usable security and privacy. Traditional notice and choice mechanisms fail to protect users' privacy. Users are increasingly frustrated and overwhelmed with complex privacy policies, unreachable privacy settings, and a multitude of emerging standards. I will explore utilizing Conversational Privacy Bots (*PriBots*) [10] as a new way of delivering notice and choice through a two-way dialogue between the user and a chatbot. PriBots will improve on state-of-the-art by offering users a more intuitive interface to inquire about their privacy settings, thus allowing them to control their privacy. In addition to investigating the potential applications of PriBots, I will undertake the different challenges of the underlying system including the user interface (UI) and natural language processing (NLP) aspects. Pribots will be part of a more general direction related to automated privacy. I will explore

mechanisms that make privacy decisions on the users' behalf that meet their needs while reducing unnecessary user interactions.

Privacy through Service Provider Diversity: The heterogeneity of SPs presents an opportunity for privacy protection. Particularly, I plan to explore a new research direction that is privacy protection through SP diversity, with the entailed theoretical and practical aspects. In the current mobile and IoT ecosystems, multiple SPs compete for users' data by offering similar services. For example, there are multiple navigation services, messaging platforms, cloud storage providers and IoT data analytics services. Interchanging between similar SPs to perform the same functionality achieves privacy protection by minimizing the data a single SP stores about a user. Moreover, data minimization is a good security practice for SPs; it limits their risk in the case of a security breach. To achieve privacy protection through SP diversity, several challenges need to be overcome that include modeling the privacy gains from diverse channels, interfacing different SPs with the protection mechanism, and designing high-fidelity user interfaces.

Device-aware Security: The trade-off between the IoT device's ability to perform its tasks and the required built-in security protection will be an important challenge, especially when considering power and/or computing constraints. I plan to pursue device-aware security and privacy protection mechanisms that adapt to each device's capabilities while ensuring a minimum protection level. For example, selective encryption techniques reduce computation overhead by encrypting only the sensitive parts of the data and adaptive machine learning classifiers reconfigure protection level depending on the device's capabilities.

Perimeter-based Security: Due to the closed nature of many IoT devices, we often cannot implement defenses directly on the device. This poses a challenge to IoT security. I plan to explore defense mechanisms that define the security state and enforce protection of IoT environments from a distance. First, defense mechanisms will utilize outside sensors in the same environment to estimate the security state of an inaccessible IoT device. For example, power sensor readings could reveal the operating characteristics of another connected device, wireless traffic could indicate malicious behavior, and vehicular sensors could reveal anomalies in the control systems. Second, the defense system will have to thwart an adversary without the privilege of running on the IoT device. BLE-Guardian and VAuth were the initial steps in this direction; their design philosophy could extend to other D2D interaction protocols, such as Zigbee, or H2D interfaces, such as gesture control. I have already coauthored an accepted NSF proposal (CNS-1646130) to pursue this problem in the next three years.

A Theory of Cyber-deception: It is not just the defender that aims to estimate the security state of the system(s) it is protecting, but the attacker targets the same objective. In this realm, I plan to explore a theory of cyber-deception. The defender will utilize a game-theoretic construct to strategically employ defensive actions that manipulate the attacker's estimation of the system's security state. Such actions may include disseminating fake information about the system components (software, devices or data). Such a cyber-deception theory will establish a methodology for the defender to *proactively* protect the assets in an enterprise or IoT deployment. I plan to address the related challenges of deployability, incomplete information about the attacker, and partial observations.

References

[1] D. Evans, "The Internet of Things," http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. [Online; accessed 23-Oct-2016].

[2] US Patent 9,147,072, "Method and System for Performing Behavioral Analysis Operations in a Mobile Device based on Application State", K. Fawaz, V. Sridhara, R. Gupta, M. Christodorescu, Sep. 29, 2015.

[3] US Patent App. 14/090,261, "Methods and Systems of Using Boosted Decision Stumps and Joint Feature Selection and Culling Algorithms for the Efficient Classification of Mobile Device Behaviors", K. Fawaz, V. Sridhara, R. Gupta, Nov. 26, 2013.

[4] K. Fawaz, K.H. Kim and K.G. Shin, "Protecting Privacy of BLE Device Users," in 25^{th} *USENIX Security Symposium*, Austin, TX, August 2016.

[5] H. Feng*, K Fawaz* and K.G. Shin (* co-primary authors), "Continuous Authentication for Voice Assistants," in *IEEE S&P 2017*, Under Review.

[6] K. Fawaz and K.G. Shin, "Location Privacy for Smartphone Users," in 21^{st} *ACM Conference on Computer and Communications Security (CCS 2014)*, Arizona, USA, November 2014.

[7] K. Fawaz, H. Feng and K.G. Shin, "Anatomization and User-Level Prevention of Mobile Apps' Location Privacy Threats," in 24^{th} *USENIX Security Symposium*, Washington D.C., USA, August 2015.

[8] K. Fawaz, K.H. Kim and K.G. Shin, "Privacy vs. Reward in Indoor Location-Based Services," in 16^{th} *Privacy Enhancing Technologies Symposium (PETS 2016)*, Darmstadt, Germany, July 2016.

[9] H. Feng, K. Fawaz and K.G. Shin, "LinkDroid: Reducing Unregulated Aggregation of App Usage Behaviors," in 24^{th} *USENIX Security Symposium*, Washington D.C., USA, August 2015.

[10] H. Harkous, K. Fawaz, K.G. Shin, and K. Aberer "PriBots: Conversational Privacy with Chatbots," in *SOUPS 2016 Workshop on the Future of Privacy Indicators*, Denver, CO, USA, June 2016.