I am a computer systems security researcher who enjoys building secure systems. My research establishes practical and principled security techniques for emerging technologies while recognizing and overcoming domain-specific challenges. My current research thrust is systems security for the Internet of Things (IoT). Our homes, hospitals, cities, and industries are being enhanced with devices that have computational and networking capabilities. This emerging network of connected devices, or IoT, promises better safety, enhanced management of patients, improved energy efficiency, and optimized manufacturing processes. The fundamental building block that brings about these benefits is interoperability between the various types of devices. *IoT platforms*, which are an emerging technology, enable this interoperability. A platform is a software stack that unifies disparate devices and low-level connectivity protocols while supporting applications that work seamlessly across different types of devices. Examples of emerging IoT platforms include Samsung SmartThings, IoTivity, Google Brillo/Weave, If-This-Then-That, Microsoft Flow, Google Fit, and Android Auto. Studying these platforms avoids the issues of low-coverage and limited-applicability findings concomitant with studying individual devices—security design flaws in platforms can result in widespread risks to users. My goal is to systematically identify these risks and then design secure versions of these platforms using practically adoptable security techniques.

My work has contributed some of the first security studies and systems aimed at more secure and safe IoT platforms. I performed the first principled empirical security analyses for two popular and widely used kinds of platforms—Samsung SmartThings [9], a home automation system, and If-This-Then-That (IFTTT), a trigger-action end-user programming platform [11]. These studies used black-box fuzzing and dynamic OAuth API testing techniques to uncover security design shortcomings. To overcome the identified weaknesses, I and my co-authors designed FlowFence [10], a practical way to build IoT apps where information flow control is a first-class primitive. We also built Decoupled-IFTTT, a system that demonstrates the possibility of IFTTT functionality without users having to give IFTTT powerful and overprivileged access to their online services and devices [11].

My research also encompasses mobile systems. I have built contextual access control systems [3], defenses against UI deception attacks [7], and privacy-respecting information extraction algorithms [14] that are tuned to the specific challenges of this domain. For example, we are seeing the emergence of mobile systems that extract the semantics of text in apps (e.g., Now-on-Tap) by transmitting all of that privacy-sensitive information to cloud back-ends for processing. I built Appstract [14], a system that extracts app content semantics *without* transmitting in-app content to the cloud, thus reducing user risk.

Impact. The empirical security analysis of smart home applications received the *Distinguished Practical Paper Award* at IEEE Security and Privacy in 2016 along with widespread press coverage [2]. SmartThings has responded positively to our results and is currently implementing changes to its architecture based on recommendations from our study. Furthermore, the SmartThings analysis and FlowFence is now part of security and software testing curriculum at the University of Southern California (CSCI599 F16), the University of Illinois Urbana-Champaign (CS527 F16, CS598 F16), Lehigh University (CSE450 F16), Wayne State (CSC 6991 F16), and the University of North Carolina at Chapel Hill (590 F16). The IoT security curriculum at the Microsoft Research Summer School in Kazan, Russia in 2016 was based in part upon the SmartThings analysis. The Appstract system has resulted in two patent filings for Microsoft.

Approach. My approach to solving security problems is to build systems that serve as existence proof of a solution. However, breaking systems often yields the deepest lessons and it is an important step to take before we can build better versions of these systems. Therefore, I take on the roles of both attacker and defender in my work. A cross-cutting element of my approach is to independently seek out collaborators in related fields. Until now, I've collaborated with 18 other researchers across 6 institutions. Most recently, I helped bootstrap a collaboration between my group at Michigan (Prof. Atul Prakash and Amir Rahmati) and UIUC (Prof. Darko Marinov and Alex Gyori) that led to a recently funded NSF proposal (CPS-1646392, CPS-1646305, $800K) on IoT security testing.

Looking forward, I plan on exploring mechanisms that provide fail-safe security to IoT platforms, in-the-field recoverability of compromised devices, and tamper-proof audit of device activity. In the long-term, I am interested in exploring large-scale IoT platform security, and security for machine learning systems. I am excited to have the opportunity to tackle these problems.

IoT Systems Security

Identifying and Overcoming Security Risks in IoT Platforms (IEEE S&P'16). Based on the approach outlined above, I analyzed the security of two kinds of IoT platforms to determine how and why security fails in practice. Platforms unify heterogeneous devices and protocols into a common base where devices and software can talk to each other uniformly to realize the promised benefits of the IoT. This work focuses on IoT systems like wearables and smart homes because these systems currently have the most user adoption and traction.

1) Smart Home Platform and App Analysis: I analyzed the security of Samsung SmartThings, a mature platform with wide support for devices and third party apps. It shares core design principles (privilege separation through capabilities, trigger-action programming through events) with other such platforms that are currently in nascent design stages. Therefore, the lessons we extracted from analyzing SmartThings will help inform the design of other systems of this kind. This work used black-box fuzzing techniques and custom-built static program analysis tools to determine that SmartThings and its apps do not adhere to the tried-and-tested security principles of least-privilege, sensitive data protection, and proper access control. The analysis revealed that SmartThings apps are *automatically* overprivileged. Based on the discovered design flaws, I built long-range attacks that reprogrammed door locks and the first smart home malware that snooped on pincodes [9], [12].

This work received the Distinguished Practical Paper Award at IEEE Security and Privacy 2016, along with widespread press coverage. SmartThings is creating design changes to mitigate the automatic overprivilege in the capability system, inspired by recommendations in the paper. The SmartThings team has regular conference calls with me to discuss the fixes.

2) Cloud API Integrator Analysis: While SmartThings is intended at professional developers, there is another kind of IoT platform that is aimed at end-user programming—Cloud API Integrators. They support end-user programming using a trigger-action model. For example, users can create programs of the form "If smoke is detected, then turn off my oven." I conducted an empirical analysis of the authorization model of IFTTT, a popular and representative trigger-action programming platform. The analysis reveals that channels, an IFTTT abstraction of online services and devices, have access to perform more operations with a user's services and devices than what they need to support their functionality. I built semi-automated dynamic API testing tools that overcame the challenges of ill-defined OAuth scope-to-API mapping, incomplete API documentation, and inconsistent API formats to quantify this overprivilege at scale and found that 75% of channels studied in-depth were overprivileged [11]. This overprivilege increases the risk users face. For example, this work demonstrates how an attacker can reprogram a Particle[1] chip's firmware using a single HTTP API call.

Based on the findings above, I and my co-authors designed and built Decoupled-IFTTT, a trigger-action platform where users do *not* have to trust the platform with highly-privileged access to their data and devices. We designed cryptographic extensions to the OAuth protocol that limit the risk users face if the platform is compromised. Although Decoupled-IFTTT uses very fine-grained OAuth tokens, it does not increase the number of OAuth permission prompts (compared to IFTTT), thus overcoming a key challenge of fine-grained permission systems.

Practical Information Flow Control for IoT Apps (USENIX Security'16, SecDev'16, SPSM@CCS'14). Based on the above analyses of IoT platforms, the common denominator is that all of them use a permission model that potentially leads to overprivilege. Couple this with the fact that the IoT fundamentally produces a lot of sensitive data (e.g., related to people's activities, their family members, etc.), the overprivilege can quickly lead to data-stealing apps. Even without overprivilege, a permission system fundamentally cannot control *how* apps use data once they have access. Therefore, I and my co-authors designed and built FlowFence [4], [10], [15], a system where information flow control is a first class primitive. It does not suffer from implicit flows and computational overheads that plague other flow control systems. FlowFence draws on principles from language-based flow control and from label-based mandatory flow control. It forces developers to design their apps around flows of information from sources to sinks. Developers declare intended data flows, and FlowFence automatically prevents all other flows. This gives us a clean-slate opportunity to build security from the ground up for IoT apps.

FlowFence is tailored to overcome IoT-specific challenges. In particular, it requires minimal primitives from the underlying operating system, it is efficient, it allows for rapid app development and programmers can quickly port existing IoT apps.

[1]https://www.particle.io/

MOBILE SYSTEMS SECURITY

I've made several contributions to mobile systems security. Mobile systems are a precursor to IoT systems, and the experience from the projects here have helped me identify important problems in IoT security. Furthermore, some of the techniques discussed below include insights to deal with environments similar to the IoT. For example, resource- and energy-aware techniques are relevant to IoT platforms.

Privacy-Respecting Information Extraction in Mobile Apps (MobiCom'16, HotOS'15). Understanding the semantics of contents that people consume inside apps can enable new experiences. For example, if a user is listening to some music in one app, an intelligent system will understand this fact, and then dynamically present options to purchase that particular song. We are seeing an emergence of systems that offer such functionality (e.g., Google Now-on-Tap and Bing Snapp). However, these systems transmit all app contents to third-party cloud back-ends. Often, in-app content could be privacy sensitive information, such as medications or bank data. Therefore, current systems do not help improve or maintain user privacy. We designed and built Appstract [13], [14], a system and a set of algorithms that efficiently and accurately extracts the semantics of text without transmitting that text to a cloud server. This is challenging because: (1) mobile UIs provide very little context and (2) understanding the semantics of text poses prohibitive computational and storage overheads. A key insight is to split the analysis into a user-agnostic cloud-phase and a user-specific device-phase. Lessons learned from designing Appstract are useful for IoT security research—developing efficient privacy-respecting information extraction algorithms for constrained environments will be helpful to extract semantics from the streams of data the IoT generates.

Android Security (FC'16, DSN'15, IEEE TIFS'12, '14, IEEE TDSC'14, SACMAT'12). My research has explored UI phishing defenses [7], systems that help apps reduce their trusted computing base [6], FM radio based attacks on phones [8], early techniques for contextual access control on smartphones [3], and mechanisms for bring-your-own-device (BYOD) solutions [16], [17], [19]. Versions of these techniques have since appeared as standard elements of mobile operating systems. For example, BYOD is now a common feature on Android.

FUTURE SYSTEMS SECURITY RESEARCH

My future research agenda in the near-term will explore techniques to provide desirable properties like fail-safe security, recoverability of compromised devices, and tamper-proof audit. In the long-term, I plan on examining systems security for large-scale IoT systems, and security for machine learning systems.

Fail-Safe Security and Intrusion Detection. Vendors are driven by go-to-market deadlines and functionality-based priorities [18]. This creates a dangerous situation where devices and platforms with security design flaws are pushed into the market. Therefore, continuing the line of work I started with FlowFence, which was motivated by the fact that a security framework should be tuned to the rapid development of the IoT, I intend to explore techniques for fail-safe security. Even if some security components fail, they should fail in a manner that limits the physical danger to users. I envision a system where safety rules of the form "My fire alarm should always be powered whenever the oven is being used" can be specified, learned automatically, and enforced with a minimal trusted computing base. This is challenging for a variety of reasons: 1) The expressiveness of the specification language can either make automated learning harder or reduce security making its design difficult; 2) Learning techniques require positive and negative examples that can be hard to obtain given that such IoT platforms are still gaining adoption.

In-The-Field Recoverability with Trusted Hardware. Network connected sensors and actuators can be deployed on bridges and other infrastructure where attackers might have physical access. A challenge is that in the event of a compromise, we need techniques to securely re-establish a connection to these devices and restore them to a known good state. I am interested in exploring techniques that use minimal trusted hardware (SGX, TrustZone, RIoT) to provide such abilities.

Tamper-Proof Audit. In the event that damage occurs to a physical space or its inhabitants due to IoT devices, finding the root cause is important. For instance, if a house catches fire, insurance agencies would need proof of the cause. Was the fire due to an on-premise arsonist, was it due to a malfunctioning networked oven, or was it due to a remote-arsonist who compromised the oven? More generally, we are seeing that IoT devices are being used as evidence in legal proceedings [1]. I am interested in exploring techniques that enable tamper-proof auditing of device activity. A challenge is dealing with the amount of data IoT devices produce, and finding a balance where we can sacrifice data amount and quality yet maintain legal admissibility. I plan to explore the use of minimal

trusted hardware on the devices coupled with advances in encrypted processing in the cloud or cloud-based secure enclave technologies to enable such kind of auditing.

Security of Large-Scale IoT Systems. Smart cities (buildings, traffic control), critical infrastructure (electricity grid, water and waste treatment), and transportation (cars, buses) are examples of large-scale IoT systems that can cause widespread physical damage if attackers compromise them. I intend to apply my research methodology to this area as well: characterize security failures in practice, and then build solutions tuned to the specific challenges such IoT platforms face. A key challenge is to determine whether and how existing security mechanisms scale-up to these systems. For instance, I plan on extending FlowFence, which is designed for a single-hub architecture, to span multiple hubs that might exist in a building or in a city block. Another challenge is accessibility—critical infrastructures are not as easily available for research as systems like connected homes. I plan on exploring ways to overcome this challenge by leveraging recent results in generating realistic SCADA datasets [5], and by leveraging the wealth of simulation research in industrial control systems.

Systems Security for Machine Learning. Recent advances in machine learning have resulted in widespread applicability of ML algorithms to a solve a variety of inference problems with good success. I envision that ML techniques will be equally applicable to understanding the massive amounts of sensor and actuator data from our IoT-enabled world. A key challenge here will be extracting meaningful insights from this data while maintaining data security and privacy. In the long-term, I am interested in exploring systems techniques to securely and privately extract such inferences using advances in data-oblivious machine learning algorithms and encrypted cloud processing.

Overall, I am broadly interested in systems security with an emphasis on IoT security, and in the areas that intersect these fields.

REFERENCES

[1] "Fitbit tracking data comes up in another court case," https://www.engadget.com/2015/06/28/fitbit-data-used-by-police/.

[2] "Media coverage of my work," https://iotsecurity.eecs.umich.edu.

[3] M. Conti, B. Crispo, **E. Fernandes**, and Y. Zhauniarovich, "CRePE: A System for Enforcing Fine-Grained Context-Related Policies on Android," *IEEE Transactions on Information Forensics and Security (TIFS)*, 2012.

[4] M. Conti, **E. Fernandes**, J. Paupore, A. Prakash, and D. Simionato, "OASIS: Operational Access Sandboxes for Information Security," in *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM@CCS)*, 2014.

[5] A. Lemay and J. M. Fernandez, "Providing SCADA Network Data Sets for Intrusion Detection Research," in *9th Workshop on Cyber Security Experimentation and Test (CSET 16)*, 2016.

[6] **E. Fernandes**, A. Aluri, A. Crowell, and A. Prakash, "Decomposable Trust for Android Applications," in *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2015.

[7] **E. Fernandes**, Q. A. Chen, J. Paupore, G. Essl, J. A. Halderman, Z. M. Mao, and A. Prakash, "Android UI Deception Revisited: Attacks and Defenses," in *Proceedings of the 20th International Conference on Financial Cryptography and Data Security (FC)*, 2016.

[8] **E. Fernandes**, B. Crispo, and M. Conti, "FM 99.9, Radio Virus: Exploiting FM Radio Broadcasts for Malware Deployment," *IEEE Transactions on Information Forensics and Security (TIFS)*, 2013.

[9] **E. Fernandes**, J. Jung, and A. Prakash, "Security Analysis of Emerging Smart Home Applications," in *Proceedings of the 37th IEEE Symposium on Security and Privacy (S&P)*, 2016.

[10] **E. Fernandes**, J. Paupore, A. Rahmati, D. Simionato, M. Conti, and A. Prakash, "FlowFence: Practical Data Protection for Emerging IoT Application Frameworks," in *Proceedings of the 25th USENIX Security Symposium*, 2016.

[11] **E. Fernandes**, A. Rahmati, J. Jung, and A. Prakash, "Decoupled-IFTTT: Constraining Privilege in Trigger-Action Platforms for the Internet of Things," in *Under Review*, 2017.

[12] **E. Fernandes**, A. Rahmati, J. Jung, and A. Prakash, "The Security Implications of Permission Models in Smart Home Application Frameworks," *IEEE Security and Privacy Magazine*, 2017.

[13] **E. Fernandes**, O. Riva, and S. Nath, "My OS Ought to Know Me Better: In-app Behavioural Analytics as an OS Service," in *15th Workshop on Hot Topics in Operating Systems (HotOS XV)*, 2015.

[14] **E. Fernandes**, O. Riva, and S. Nath, "Appstract: On-The-Fly App Content Semantics with Better Privacy," in *Proceedings of the 22nd ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2016.

[15] A. Rahmati, **E. Fernandes**, and A. Prakash, "Applying the Opacified Computation Model to Enforce Information Flow Policies in IoT Applications," in *Proceedings of the 1st IEEE CyberSecurity Development Conference (SecDev)*, 2016.

[16] G. Russello, M. Conti, B. Crispo, and **E. Fernandes**, "MOSES: Supporting Operation Modes on Smartphones," in *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies (SACMAT)*, 2012.

[17] G. Russello, B. Crispo, **E. Fernandes**, and Y. Zhauniarovich, "YAASE: Yet Another Android Security Extension," in *3rd IEEE Conference on Privacy, Security, Risk and Trust (PASSAT)*, 2011.

[18] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*, 2015.

[19] Y. Zhauniarovich, G. Russello, M. Conti, B. Crispo, and **E. Fernandes**, "MOSES: Supporting and Enforcing Security Profiles on Smartphones," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2014.