Research Statement

Arsalan Mosenia (arsalan@princeton.edu)

I am interested in investigating and addressing emerging security and privacy challenges in Internet of Things (IoT). The emergence of the IoT paradigm is one of the most spectacular phenomena of the last decade. The development of new communication protocols, along with the miniaturization of transceivers, provides an opportunity to transform isolated devices into *communicating things*. Moreover, computing and storage capabilities of small embedded systems and sensing devices have significantly improved while their sizes have decreased drastically. These rapid advances in electronics and computer science have led to an exponential increase in the number of Internet-connected sensing/computing devices that can provide services only limited by human imagination.

Despite picturesque promises of IoT, the integration of smart things into the Internet introduces multiple new security challenges because the Internet infrastructure and several edge-side systems (for example, vehicles) were not initially designed to support IoT (see [1] for a survey on IoT security: this paper is among the most popular papers of IEEE Transactions on Emerging Topics in Computing). Furthermore, the introduction of new computing/networking paradigms around IoT (in particular, fog computing and edge computing), that promise the interconnection of numerous heterogeneous devices, have led to the emergence of new security concerns (see [2] for our position paper on fog security: it offers an overview of the security landscape of fog computing as discussed in Security Work Group at OpenFog Consortium [1]).

My research tackles emerging security/privacy challenges in IoT and cyber-physical systems. Towards this end, I combine the development of real-world systems with sound theoretical foundations, and leverage techniques from the disciplines of machine learning, information security, signal processing, embedded systems, network science, and biomedical engineering. *Specifically, I have explored the following themes: (1) addressing security and privacy challenges of implantable and wearable medical devices, (2) ensuring security of Internet-connected and autonomous vehicles, and (3) investigating emerging security concerns in embedded and cyber-physical systems.*

Summary of Impact: My research has uncovered fundamental security/privacy flaws in the design of multiple widely-used Internet-connected and cyber-physical systems, including medical implants and wearables, Internet-connected and autonomous vehicles, smartphones, and automation systems. It has resulted in several publications that are currently *among the most popular papers of top-tier IEEE Transactions.* Furthermore, it has received multiple prestigious awards, including *Princeton X, Princeton Innovation Fund, and French-American Doctoral Exchange Fellowship* and been featured in several news and media outlets [2]. One of my papers has been selected as the *"Spotlight Paper"* of the special issue on "Wearables, Implants, and Internet of Things" in IEEE Transactions on Multi-Scale Computing Systems and another one has received *"Selected Presenter Award"* from NJ Tech. Council. Four U.S. Patents have been filed based on the technologies that I have developed, and several potential industrial partners, such as Cisco and AT&T, are exploring commercialization of the technologies. At OpenFog Consortium, I am actively collaborating with Security Work Group, where I define domain-specific security standards for fog computing, and Testbed Work Group, where I design, build, and examine novel fog-inspired real-world systems.

1 Security of Implantable and Wearable Medical Devices

For my Ph.D., I focused on the security of implantable and wearable medical devices (see [3] for a comprehensive survey on wearable medical sensor-based system design: this paper is currently among the most popular papers of IEEE Transactions on Multi-Scale Computing Systems).

1.1 Continuous authentication based on BioAura: Most computer systems authenticate users only once at the time of initial login, which can lead to security concerns. Continuous authentication has been explored as an approach for alleviating such concerns. Previous methods for continuous authentication primarily use biometrics (e.g., fingerprint) or behaviometrics (e.g., key stroke patterns). We proposed CABA [4], a continuous authentication system that is inspired by and leverages the emergence of wearable medical sensors for pervasive and continuous health monitoring. CABA authenticates users based on their BioAura, an ensemble of biomedical signal streams that can be collected continuously and non-invasively using wearable medical devices. While each such signal may not be highly discriminative by itself, we demonstrated that a collection of such signals, along with robust *machine learning*, provides high accuracy levels. *The study has received **"Selected Presenter Award"** from NJ Tech. Council and **"Project X Award"** from Princeton University, and has been published in IEEE Transactions on Computers (the most popular paper in Jan. 2017). After a thorough evaluation of marketing opportunities, Office of Technology Licensing at Princeton University has filed a full U.S. Patent based on CABA in 2107.*

[1] To drive industry and academic leadership in fog computing, OpenFog Consortium was founded by Princeton University and Cisco in 2015. Since then, this consortium has brought together several researchers and designers from the industry (e.g., Intel, Microsoft, Dell, and ARM Holdings) and academia, and it now has over 55 members across North America, Asia, and Europe.

[2] For example, an article, that describes one of my recent studies (known as "PinMe"), can be found on "Schneier on Security": https://www.schneier.com/blog/archives/2017/12/tracking_people_5.html

1.2 Energy-efficient long-term continuous personal health monitoring: Health monitoring using wireless body area networks of wearable medical devices is envisioned as a transformative approach to healthcare. The constrained sizes of wearables imply that they are designed with very limited resources. To bring cryptographic mechanisms to such devices and ensure the security of health monitoring systems, there is a strong need for efficiency in data processing/storage and communication. In [5], we quantified the energy/storage requirements of a continuous health monitoring system that uses eight biomedical sensors. Our analysis suggested that there exists a significant gap between the energy/storage requirements for long-term continuous monitoring and the capabilities of current devices. To enable secure energy-efficient health monitoring, we proposed schemes for sample aggregation, anomaly-driven transmission, and compressive sensing. We demonstrated that they result in two to three orders-of-magnitude improvements in energy and storage requirements, and can help realize the potential of long-term continuous health monitoring. *This publication has been selected as the **"Spotlight Paper"** of the special issue on "Wearables, Implants, and Internet of Things" in IEEE Transactions on Multi-Scale Computing Systems, and is currently among the most popular papers of the journal.*

1.3 A Secure Communication Channel for Implantable Medical Devices: Integration of radio frequency (RF) modules in implantable medical devices (IMDs), e.g., pacemakers, has made them susceptible to various security attacks. Several lightweight encryption mechanisms have been developed to prevent well-known attacks. However, lack of a secure key exchange protocol (that enables the exchange of the encryption key while maintaining its confidentiality) and the immaturity of wakeup protocols (that are used to turn on the RF module before an authorized data transmission) are two fundamental challenges that must be addressed to ensure the security of wireless-enabled IMDs. We introduced OpSecure [6], an optical secure communication channel between an IMD and an external device, which enables: (1) a wakeup protocol that is resilient against battery draining attacks, and (2) a secure key exchange protocol to share the encryption key between the IMD and the external device. *This study has been published in IEEE Transactions on Multi-Scale Computing Systems and has been patented.*

1.4 Physiological information leakage: Previous work in the area of health information security has largely focused on attacks on the wireless communication channel of medical devices, or on health data stored in databases. We pursued an entirely different angle to health information security, motivated by the insight that the human body itself is a rich source of data. We proposed a new class of information security attacks [7] that exploit physiological information leakage, i.e., various forms of information that naturally leak from the human body (body organs, such as lungs and the heart or the devices attached to the body), to compromise privacy. As an example, we showed how an adversary can estimate blood pressure by capturing and processing the acoustic signal or electromagnetic radiation of an ambulatory blood pressure monitoring device.

2 Security of Internet-connected and Autonomous Vehicles

As a postdoctoral researcher, I am exploring the security of Internet-connected and autonomous vehicles.

2.1 Bringing programability and connectivity into isolated vehicles: Despite the existence of several novel vehicular applications in the literature, there still exists a significant gap between resources needed for a variety of vehicular (in particular, data-dominant, latency-sensitive, and computationally-heavy) applications and the capabilities of in-market vehicles. To address this gap, different smartphone-/Cloud-based approaches have been proposed that utilize the external computational/storage resources to enable new applications. However, their acceptance and application domain are still very limited due to programability, wireless connectivity, and performance limitations, along with several security/privacy concerns. In [8], we presented a novel fog-oriented architecture that can potentially enable rapid development of various vehicular applications while addressing shortcomings of previous approaches. The architecture is formed around a privacy/security-friendly programmable dongle that brings general-purpose computational and storage resources to the vehicle and hosts in-vehicle applications. Based on the proposed architecture, we developed an application development framework for vehicles, that we called ProCMotive. ProCMotive enables developers to build customized applications along the Cloud-to-edge continuum, i.e., different functions of an application can be distributed across SmartCore, the user's personal devices, and the Cloud. *This study has received **"Princeton Innovation Award"**. A Provisional Patent has been filed based on ProCMotive. In collaboration with our industrial partner, Cisco, we are currently exploring the next steps toward the commercialization of the proposed systems.*

2.2 A secure infrastructure-independent navigation system: With the widespread use of Global Positioning System (GPS) in modern vehicle, the security of GPS has garnered ever-increasing attention in recent years. GPS receivers compare timestamped signals from a constellation of satellites, inferring their position through computations on the lightspeed lag from each signal. Several studies demonstrated the feasibility of faking the satellite signals and discussed that security attacks against the GPS used in autonomous vehicles may lead to disastrous consequences. Unfortunately, protecting GPS signals is difficult since the implementation of new mechanisms, which need modifications to the GPS infrastructure, is difficult and costly. We developed a satellite-independent navigation system [9] that accurately tracks a vehicle without utilizing external signals. It exploits sensory data collected by smart devices and vehicles, along with publicly-available auxiliary information, to track the vehicle. Our examinations showed that the technology can potentially offer a promising secure alternative to GPS. *It has been patented by the Office of Technology Licensing at Princeton University and several companies have shown interest in its further development. We are currently optimizing the algorithms for cars and smartphones. We plan to conduct a large-scale user study later this year.*

2.3 Prevention and detection of attacks against Internet-connected vehicles: Any security attack against vehicles may lead to life-threatening consequences. Attackers can launch a multitude of well-known attacks against the vehicles, ranging from Denial of Service (DoS) attacks to packet sniffing. The majority of after-market dongles are vulnerable to well-known security attacks, offering a valuable opportunity for attackers to remotely take control of several components embedded in the vehicle. To address these attacks, we proposed [8]: (1) a novel context-aware access control scheme that enables the user to decide what information she wants to share with each in-vehicle application or dongle, and (2) and an intrusion detection scheme that detects the maliciousness of a dongle based on its abnormal behavior (for example, high rates of requests). *In collaboration with Cisco Systems, we plan to strengthen and broaden the patent protection around this concept, thus providing a strong technology platform on which it is expected a new venture will be spun out to bring the above technologies to market.*

2.4 Privacy-preserving usage-based auto insurance: Usage-based insurance policies are envisioned as the future of auto insurance. Many insurance companies worldwide have already introduced new low-rate insurance plans for which they take traveling mileage, along with the driver's behaviors, into account. Despite the potential benefits that insurance dongles have offered, their usage is currently limited due to privacy concerns: the dongles can collect several types of sensitive information (or raw data that leak private information), such as the vehicle's location. To address such privacy concerns, we applied various data manipulation and differential privacy techniques and proposed a privacy-friendly insurance scheme [8]. Implemented based on ProCMotive framework (discussed earlier in Section 1.2), the proposed approach filters and/or adds noise to the raw data to conceal or remove inessential parts of the data, before sharing the data with insurance dongles. Unlike prior privacy-preserving proposals that require fundamental design changes in the hardware (insurance dongle) or back-end infrastructures, our approach imposes no design change (and consequently, no additional cost) on insurance companies.

2.5 Smart traffic signs: Autonomous vehicles rely on image processing and machine learning techniques to detect human-perceptible traffic signs. Recent studies in adversarial machine learning have discussed the possibility of creating adversarial perturbation of signs that can potentially deceive the sign detection algorithms used in autonomous vehicles, leading to life-threatening situations. We tackle this challenge from a completely different angle, inspired by the observation that traffic signs were initially designed to attract human drivers' attention, and may not be suitable for the world of autonomous vehicles. Borrowing concepts from applied cryptography and communication, we rethink the design of traffic signs and introduce a new generation of signs [10], referred to as smart signs. Smart signs are self-advertising signs, which periodically create and cryptographically sign a packet, including their GPS coordinates and type, and send it to nearby vehicles. This new design offers two fundamental benefits. First, it eliminates the feasibility of adversarial attacks against machine learning algorithms. Second, it significantly reduces the computation burden of sign detection.

3 Emerging Security Challenges in Embedded and Cyber-physical Systems

3.1 Achilles' heel of industrial/home systems–Emergency responses: We introduced a new class of attacks against cyber-physical systems (CPSs), called dedicated intelligent security attacks against sensor-triggered emergency responses (DISASTER) [11]. DISASTER targets safety mechanisms deployed in CPSs and exploits design flaws and security weaknesses of such mechanisms to trigger emergency responses in the absence of a real emergency. Launching DISASTER leads to serious consequences for two main reasons. First, almost all CPSs offer specific emergency responses, and as a result, are potentially susceptible to such attacks. Second, the widespread deployment of insecure sensors in safety mechanisms along with the endless variety of CPS-based applications magnifies the impact of launching DISASTER. We demonstrated the feasibility of launching DISASTER against the two most widely-used CPSs: residential and industrial automation/monitoring systems.

3.2 Acoustic injection attack against embedded hard drives: Among storage components, hard disk drives (HDDs) have become the most commonly-used type of non-volatile storage due to their significant advances: their energy efficacy, fault tolerance, and storage capacity have significantly improved while their sizes have decreased drastically. Such advances in HDDs have made them an inevitable part of numerous computing systems, including, personal computers, bedside monitors, closed-circuit television surveillance systems, and automated teller machines (ATMs). We proposed the first instance of remote DoS attack against HDDs [12]. It relies on a physical phenomenon, known as acoustic resonance, in which an acoustic signal forces an object to oscillate with greater amplitude at specific frequencies. We conducted a thorough examination of physical characteristics of fundamental components of HDDs (read/write head and platters) and created acoustic signals that cause significant oscillations in HDD's internal components. These oscillations halt write/read operation of embedded HDDs, leading to serious security concerns in mission-critical systems. We demonstrated the feasibility of the attack in three real-world case studies, namely, Internet-connected surveillance systems, personal computers, and colocation facilities (data center facilities in which a business rents space for its own servers).

4 Future research

I am interested in coupling theoretical principles with practical design of systems to solve emerging security challenges in IoT. In particular, I would like to further explore three challenging research directions:

Privacy-preserving and attack-resilient machine learning: Machine learning forms the foundation of numerous emerging IoT-enabled systems. For my future research, I plan to explore novel approaches to incorporate the notion of privacy/security into learning frameworks. In particular, I am interested in finding answers to following problems: (1) How can we design privacy-preserving learning frameworks and algorithms that allow different entities to train models on their joint data without revealing any information beyond the outcome? (2) How can we make machine learning techniques more resilient against emerging security attacks? (3) How can we leverage data transformation techniques to remove sensitive portions of raw data without degrading utility?

Usable security: Usability is one of the most critical requirements of security solutions: multiple studies have suggested that users tend to disregard security for better usability. In my future work, I plan to improve the usability of security solutions and rigorously investigate answers to following questions: (1) How can we build usable security functions, services, and tools to help users make more rationale security-related decisions? (2) How can we offer user-friendly and transparent tools to users and help them understand what may be inferred from their data? (3) How can we make it easier for designers to integrate security into their design. Towards this goal, I aim to collaborate with researchers in the fields of usable security, human-computer interaction, and social engineering.

Emerging computing/networking paradigms for security-enhancing technologies: In recent years, several promising computing and networking paradigms (for example, fog computing and software-defined networking) have emerged to address rapidly-growing challenges of IoT. These fast-growing paradigms introduce many interesting research directions, including new security, networking, load balancing, and usability problems. In my future research studies, I would like to further explore potential benefits of these new paradigms to security-/privacy-friendly systems and investigate answers to the following questions: (1) How can we rethink our architectural and networking foundations to build trustworthy systems? (2) How can we rely on emerging computing/networking paradigms, such as fog computing, to enhance the security of IoT-based services? (3) How can we use close-to-edge resources to develop new privacy-enhancing IoT-enabled technologies?

I strongly believe that many security and privacy challenges require an interdisciplinary perspective, and this offers tremendous opportunity for collaboration across disciplines. For example, the core of my Ph.D. research work was focused on enhancing the security of medical technologies. Technical discussions and collaboration with researchers in the areas of healthcare and biomedical engineering significantly helped me design real-world security-enhancing technologies for medical devices. *In my research, I have collaborated with over 35 co-authors across 12 industrial research labs and academic departments and intend to continue this tradition going forward.*

References

[1] **A. Mosenia** and N. K. Jha, "A Comprehensive Study of Security of Internet of Thing," IEEE Trans. Emerging Topics in Computing, 2017 [**Among most popular papers**].

[2] B. A. Martin, F. Michaud, D. Banks, **A. Mosenia**, R. Zolfonoon, S. Irwan, S. Schrecker, and J. K. Zao, "OpenFog Security Requirements and Approaches," in Proc. Fog World Congress, 2017 [**Invited paper**].

[3] **A. Mosenia**, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Wearable Medical Sensor-based System Design: A Survey," IEEE Trans. Multi-Scale Computing Systems, 2017 [**Among most popular papers**].

[4] **A. Mosenia**, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "CABA: Continuous Authentication Based on BioAura", IEEE Trans. Computers [**Awarded "Selected Presenter Award" and "Project X Award"**] [**Among most popular papers**].

[5] **A. Mohsen Nia**, M. Mozaffari-Kermani, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "An Energy-efficient System for Long-term Continuous Personal Health Monitoring," IEEE Trans. Multi-scale Computing Systems, Special Issue on Wearables, Implants, and Internet of Things, vol. 1, no. 2, pp. 85–98, 2015 [**Spotlight paper**]

[6] **A. Mosenia** and N. K. Jha, "OpSecure: A Secure Optical Communication Channel for Implantable Medical Devices," IEEE Trans. Multi-scale Computing Systems, 2017.

[7] **A. Mohsen Nia**, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Physiological Information Leakage: A New Frontier in Health Information Security", IEEE Trans. Emerging Topics in Computing, vol. 4, no. 3, pp. 321–334, 2016.

[8] **A. Mosenia**, P. Mittal, and M. Chiang, "ProCMotive: Bringing Programability and Connectivity into Isolated Vehicles," Submitted to ACM Int. Conf. Pervasive and Ubiquitous Computing (Ubicomp), 2017. [**Awarded "Princeton Innovation Award"**]

[9] **A. Mosenia**, X. Dai, P. Mittal, and N. K. Jha, "PinMe: Tracking a Smartphone User around the World," IEEE Trans. Multi-scale Computing Systems, 2017

[10] C. Sitawarin, A. Bhagoji, **A. Mosenia**, P. Mittal, and M. Chiang "Experimental Security Analysis of Sign Detection in Autonomous Vehicles," to be submitted ACM Int. Conf. Pervasive and Ubiquitous Computing (Ubicomp), 2017.

[11] **A. Mosenia**, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "DISASTER: Dedicated Intelligent Security Attacks on Sensor-triggered Emergency Responses," IEEE Trans. Multi-scale Computing Systems, 2017.

[12] M. Shahrad, **A. Mosenia**, Lewei Song, D. Wentzlaff, M. Chiang, and P. Mittal "Acoustic Denial of Service Attacks on HDDs," To be submitted to IEEE Symposium on Security and Privacy, Jan. 2017 [Preprint version is available on ArXiv].