PhD topic for Mohamad Mansouri: Securing the Internet of Things

The advent of 5G communications represents a potentially disruptive element, and its support for large amounts of devices enables the vision of a global Internet of Things (IoT). In addition, 5G may play the role of a unified interconnection framework, facilitating a seamless connectivity of "things" with the Internet. Recent forecasts expect more than 20 billion devices connected to the Internet by the end of this decade. Residential and corporate networks provide connectivity to billions of IP-enabled devices. IoT brings automation to industrial manufacturing, automotive industries, security etc. with a promise to improve life style of users. This huge potential of IoT devices comes at a cost of user security and privacy for different reasons. The first reason is that the IoT manufacturers have constrained resources and strict deadlines for developing products and launching them in the market. Hence, this will force the manufacturers to not follow security by design principles and use non-secure techniques such as unverified code snippets. The second reason is due to the pervasive device connectivity to the Internet that poses hidden security risks, including tampering with devices, eavesdropping on the wireless communication channel, unauthorized access to devices, and privacy risks. The inherent nature of constrained devices means that the state-of-the-art cryptographic algorithms are not easy to deploy on such devices and more difficult to keep the software up-to-date. The ability to manage and control a device requires appropriate authentication and authorization measures. The third reason is that as a population of billions of objects will interact with each other and with other entities such as human beings or virtual entities, all these interactions must be secured somehow, protecting the information and service provisioning of all relevant actors and limiting the number of incidents that will affect the IoT network.

The IoT security research is centered around three themes: Devices, Protocols and Platforms. In the **IoT device scope**, many IoT devices are reported to be vulnerable due to weak or default password or unprotected interfaces [1, 2]. For instance, in [3], the authors identified problems in the access control of the Philips Hue lighting system. On the **protocol level**, the authors in [4] report the misusing of some protocols in some IoT specific scenarios that cause security and safety problems. For example, refrigerators are vulnerable to denial of service attacks [5]. In the auto-unlock scenario, the Bluetooth Low Energy (BLE) range is insecure when it is used as a proof to verify physical proximity. On the **IoT platform level**, in [6] the authors discuss a series of security-critical design flaws such as the coarse-grained permission definition on the SmartThings platform. To limit the usage of sensitive data, the authors in [7] propose the FlowFence framework that supports flow policy rules for IoT apps. In [8], the authors propose ContexIoT that allows user control in cases where a particular data flow might be allowed in one scenario, and should be blocked in another.

An important aspect that is considered in the related work is the secure pairing of IoT devices [9]. In particular, the security goal of pairing personal devices is to ensure that the key agreement takes place between the devices owned by the user. When the number of IoT devices grows, it becomes burdensome to introduce new devices since it implies the manually pairing of the new device with each existing device. Therefore, there is a need to achieve pairing of devices with zero user interaction. Existing pairing solutions that do not require direct user interaction can be divided into two classes: key pre-distribution and context-based pairing approaches. Key predistribution-based approaches [10, 11] require key material to be distributed to all network nodes before their deployment in the field. In IoT scenarios, however, this kind of pre-distribution is not practical due to the large number of devices deployed in the field and different device vendors that do not necessarily share any security associations with each other. Context-based pairing approaches [12, 13] use co-presence of devices to identify the devices to be paired. The secure pairing is still an interesting research thread to be adaptive to different number of heterogeneous IoT devices.

Another research thread concerns the remote software attestation. An adversary can easily attack IoT devices, and compromise both their privacy and safety. For instance, an attacker can modify or replace a device's firmware, in order to execute a large attack [14]. In order to prevent such attacks and ensure the secure operation of a device, it is important to guarantee its software integrity via remote software attestation. Remote software attestation is a protocol that allows a prover to prove its software integrity to a remote verifier. The prover demonstrates to the verifier that its software has not been modified. This is usually achieved by signing integrity-protected memory regions. Different challenges are still required as there is a lack of scalability to a large number of devices, dynamicity, without degrading the performance of the scheme in terms of communication and computation overhead.

Research plan

IoT devices may become the "weakest link" for breaking into a secure IT infrastructure, or for leaking sensitive information about users and their behaviors. Hence, IoT devices are becoming attractive attack targets as they can be used as bots to launch DDoS or spam, or smart IoT meters can be hacked to lower utility bills. There is also a dire need for holistic security mechanism that considers the interaction between billions of objects with each other and with other entities such as human beings.

The objectives of this PhD study are as follows:

1. Detect and evaluate software attacks with considering the context, the deployment of IoT devices, and their constraints.
2. Propose new secure and privacy aware solutions to detect these attacks. The goal is to protect the information and the service provisioning of all relevant actors, and then limit the number of incidents that will affect the IoT network.
3. Propose new solutions to ensure trust between heterogeneous entities in IoT environments, and also guarantee that IoT services like IFTTT are not compromised.

Several research directions can be followed in order to achieve these goals. One research direction is to provide innovative IDS solutions for IoT. State of the art solutions deploy a custom IDS on each device or group of devices. The drawback of these approaches is that each IDS only has a local view of the security situation. Moreover, adapting existing IDS designed for traditional computing networks, is not viable.

Another research direction concerns the ability to provide secure solutions of device pairing in the IoT network with zero user interaction. Once a device joins a group of other devices, it can collaborate with devices and access the user's and the other devices' data. This includes the use of innovative machine learning algorithms in order to identify devices depending on their context and environment. Moreover, whenever a user needs to check the integrity of software in the IoT devices and update their firmwares, she needs to provide a scalable network attestation mechanism that can handle the network dynamicity and the scalability.

A third research direction is to study the impact of misbehaving devices on IFTTT (If-This-Then-That) services in IoT environments, and their different interactions between devices, and then propose a countermeasure in order to detect whether a device is compromised or not.

References

[1] 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, page 5. ACM, 2015.

[2] E. Ronen and A. Shamir. Extended functionality attacks on IoT devices: The case of smart lights. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P), pages 3–12. IEEE, 2016.

[3] B. Ur, J. Jung, and S. Schechter. The current state of access control for smart devices in homes. In Workshop on Home Usable Privacy and Security (HUPS), 2013.

[4] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner. Smart locks: Lessons for securing commodity internet of things devices. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, pages 461–472. ACM, 2016.

[5] Fridge sends spam emails as attack hits smart gadgets.
http://www.bbc.com/news/technology-25780908.

[6] 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, May 2016.

[7] 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.

[8] Yunhan Jack Jia, Qi Alfred Chen, Shiqi Wangy, Amir Rahmati, Earlence Fernandes, Z. Morley Mao, Atul Prakash, "ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms », NDSS 2017.

[9] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong. Talking to strangers: Authentication in ad-hoc
wireless networks. In Proc. Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, Feb. 2002.

[10] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In Proc. 9th
ACM Conference on Computer and Communications Security, CCS '02, pages 41{47, New York, NY, USA,
2002. ACM.

[11] D. Schurmann and S. Sigg. Secure communication based on ambient audio. IEEE Transactions on Mobile
Computing, 12(2):358{370, Feb 2013.

[12] A. Varshavsky, A. Scannell, A. LaMarca, and E. Lara. Amigo: Proximity-based authentication of mobile
devices. In J. Krumm, G. Abowd, A. Seneviratne, and

[13] T. Strang, editors, UbiComp 2007: Ubiquitous Computing, volume 4717 of Lecture Notes in Computer Science, pages 253{270. Springer Berlin Heidelberg, 2007.

[14] Jeep Hacking 101. http://spectrum.ieee.org/cars-that-think/transportation/systems/jeep-hacking-101, 2015.