Invited Keynote

Data Security and Privacy in the IoT

Elisa Bertino
Department of Computer Science
Purdue University
West Lafayette, IN 47907
bertino@purdue.edu

ABSTRACT

Deploying existing data security solutions to the Internet of Things (IoT) is not straightforward because of device heterogeneity, highly dynamic and possibly unprotected environments, and large scale. In this paper, after outlining key challenges in data security and privacy, we summarize research directions for securing IoT data, including efficient and scalable encryption protocols, software protection techniques for small devices, and fine-grained data packet loss analysis for sensor networks.

1. INTRODUCTION

The Internet of Things (IoT) paradigm refers to the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with servers, centralized systems, and/or other connected devices based on a variety of communication infrastructures. IoT makes it possible to sense and control objects creating opportunities for more direct integration between the physical world and computer-based systems. When IoT is augmented with sensors and actuators, IoT is able to support cyber-physical applications by which networked objects can impact the physical environment by taking "physical" actions. IoT will usher automation in a large number of domains, ranging from manufacturing and energy management (e.g. SmartGrid), to healthcare management and urban life (e.g. SmartCity). Applications range from monitoring the moisture in a field of crops, to tracking the flow of products through a factory, to remotely monitoring patients with chronic illnesses and remotely managing medical devices, such as implanted devices and infusion pumps. Forecasts by McKinsey&Company estimate that the economic impact of IoT technology by year 2025 will range from 2.7 to 6.2 trillion dollars [7]. Gartner forecasts predict that by the year 2020 20.8 billions of IoT devices will be installed. Such staggering numbers show that IoT will have a major impact.

However, while on one side, IoT will make many novel applications possible, on the other side IoT increases the risk of cyber security attacks. In addition, because of its fine-grained, continuous and pervasive data acquisition and control/actuation capabilities, IoT raises concerns about privacy and safety. A recent study by HP about the most popular devices in some of the most common IoT niches reveals an alarmingly high average number of vulnerabilities per device [10]. On average, 25 vulnerabilities were found per device. For example, 80% of devices failed to require passwords of sufficient complexity and length, 70% did not encrypt local and remote traffic communications, and 60% contained vulnerable user interfaces and/or vulnerable firmware [10]. Multiple attacks have already been reported in the past against different embedded devices [2], [16] and we can expect many more in the IoT domain.

2. SECURITY AND PRIVACY RISKS FOR IOT

IoT systems are at high security risks for several reasons. They do not have well defined perimeters, are highly dynamic, and continuously change because of mobility. In addition IoT systems are highly heterogeneous with respect to communication medium and protocols, platforms, and devices. IoT systems may also include "objects" not designed to be connected to the Internet. Finally, IoT systems, or portions of them, may be physically unprotected and/or controlled by different parties. Attacks, against which there are established defense techniques in the context of conventional information systems and mobile environments, are thus much more difficult to protect against in the IoT. The OWASP Internet of Things Project [1] has identified the most common IoT vulnerabilities and has shown that many such vulnerabilities arise because of the lack of adoption of well-known security techniques, such as encryption, authentication, access control and role-based access control. A reason for the lack of adoption may certainly be security unawareness by IT companies involved in the IoT space and by end-users. However another reason is that existing security techniques, tools, and products may not be easily deployed to IoT devices and systems, for reasons such as the variety of hardware platforms and limited computing resources on many types of IoT devices. Even well known encryption protocols, such as RSA, prove to be very expensive when running on devices with limited computing capabilities especially when multiple encryption operations have to executed concurrently such as in the case of networked vehicles [12], and small drones [14].

Privacy is particularly critical in the context of IoT. As

medical and well-being devices are increasingly been adopted by users and personalized medicine and health care applications are being designed and deployed that rely on continuous fine-grained data acquisition from these devices, the human body is becoming a rich source of information. Such information is typically collected from devices and then uploaded to some cloud and/or transmitted to other devices, such as mobile phones, which in turn may forward the information to other parties. The collected information is typically very rich and often includes meta-data such as location, time, and context, thus making possible to easily infer personal habits, behaviors, and preferences of individuals. It is thus clear that on one side such information has to be carefully protected by all parties involved in its acquisition, management, and use, but also users should be provided with suitable, easy to use tools to protect their privacy and support anonymity depending on specific contexts [11].

3. RESEARCH DIRECTIONS

Developing comprehensive security and privacy solutions for IoT requires revisiting almost all security techniques we may think of. Encryption protocols need to be engineered so to be efficient and scalable for deployment on large-scale IoT systems and devices with limited computational resources. Benchmarks are needed to perform detailed assessments of such protocols [14]. In addition, as devices may be physically unprotected, attackers may have access to the state of the memory while encryption operations are being performed. Addressing such problems may require new techniques based, for example, on white-box cryptography [3]. White-box encryption techniques hide encryption keys by transforming them into large look-up tables in order to make harder for attackers to extract the keys. Such techniques are however very expensive and many of the proposed white-box encryption protocols have been cryptanalyzed. Introducing dynamics in the look-up tables by a shuffling approach [15] may help addressing such problem. In addition, scalability of such protocols is critical, in that in many safety-sensitive applications encryption operations must be very efficient. For example, in a vehicle network, a message from a vehicle informing other vehicles of a sudden break should be processed very quickly in order to give the other vehicles enough time to break. Carefully engineered approaches taking advantage of specialized hardware, such as GPUs, available on systems on chip must be designed and benchmarked [12].

Software running on the devices must also be secured. Major challenges here arise from the fact that many IoT devices are based on processors such the ARM processor, which have differences in the instruction sets with respect to other conventionally used processors. Such diversity has an implication for example on the techniques for protecting software from attacks, such as return-oriented programming attacks, as such techniques must be tailored to the specific instruction set of the platform of interest [6]. Other research issues concern how to protect at run-time software from memory vulnerabilities. Solutions to this problem may have to take into account the specific programming languages used on IoT devices, such the case of nesC used in TinyOS, and the resource limitations [8]. Also well-known software management practices, like remote software patching and firmware updates, may become difficult if at all possible in an IoT environment and may actually open the door to additional attacks [5], [4]. Communication protection and defense techniques against novel botnet attacks that exploit IoT devices [8] are also critical.

Data security, availability, and quality are other critical areas for IoT. Data security requires, in addition to the use of encryption to secure the data while being transmitted and at rest, access control policies to govern access to data, by taking into account information on data provenance and meta-data concerning the data acquisition context, such as location and time [9]. Availability requires among other things to make sure that relevant data is not lost. Addressing such requirement entails designing protocols for data acquisition and transmission that have data loss minimization as a key security goal. Kinesis [13] is an example of a sensor network system designed to make it possible for sensors to automatically take response actions in the event of data transmission disruptions. Ensuring data quality is a major critical requirement in IoT as data acquired and transmitted by IoT devices may be of poor quality, because of several reasons such as bad device calibration, device faults, and deliberate attacks aiming at data deception attacks. Solutions like data fusion need to be revised and extended to deal with dynamic environments and large-scale heterogeneous data sources.

Finally privacy introduces new challenges, including how to prevent personal devices from acquiring and/or transmitting information depending on the user location and other context information, and how to allow users to understand risks and advantages in sharing their personal data.

4. CONCLUDING REMARKS

IoT technology introduces several exciting opportunities and new applications. However, it is critical that solutions be adopted to ensure security, privacy, and safety of IoT systems with minimal impact on performance, scalability, and usability. Even though the computer and network security area has offered over the years many important techniques and methods, revisiting and extending these techniques and methods in order to address the specificities of IoT systems entails many scientific and engineering challenges.

5. ACKNOWLEDGMENTS

The work reported in this paper has been partially supported by the Purdue Cyber Center and the National Science Foundation under grant CNS-1111512.

6. REFERENCES

[1] `https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project`.

[2] S. K. Bansal. Linux worm targets internet-enabled home appliances to mine cryptocurrencies. `http://thehackernews.com/2014/03/linux-worm-targets-internet-enabled.html`, March 2014.

[3] A. Bogdanov and T. Isobe. White-box cryptography revisited: Space-hard ciphers. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015*, pages 1058–1069, 2015.

[4] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti. A large-scale analysis of the security of embedded firmwares. In *Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014.*, pages 95–110, 2014.

[5] A. Cui, M. Costello, and S. J. Stolfo. When firmware modifications attack: A case study of embedded exploitation. In *20th Annual Network and Distributed System Security Symposium, NDSS 2013, San Diego, California, USA, February 24-27, 2013*, 2013.

[6] J. Habibi, A. Panicker, A. Gupta, and E. Bertino. Disarm: Mitigating buffer overflow attacks on embedded devices. In *Network and System Security - 9th International Conference, NSS 2015, New York, NY, USA, November 3-5, 2015, Proceedings*, pages 112–129, 2015.

[7] J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, and A. Marrs. Disruptive technologies: Advances that will transform life, business, and the global economy. `http://www.mckinsey.com/insights/business_technology/disruptive_technologies`, May 2013.

[8] D. Midi, M. Payer, and E. Bertino. nesCheck: Static analysis and dynamic instrumentation for nesC memory safety. 2016. Submitted for publication.

[9] R. V. Nehme, H. Lim, and E. Bertino. FENCE: continuous access control enforcement in dynamic data stream environments. In *Third ACM Conference on Data and Application Security and Privacy, CODASPY'13, San Antonio, TX, USA, February 18-20, 2013*, pages 243–254, 2013.

[10] K. Rawlinson. Hp study reveals 70 percent of internet of things devices vulnerable to attack. `http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.VpfsZ8ArJcw`, July 2014.

[11] B. Shebaro, O. Oluwatimi, D. Midi, and E. Bertino. Identidroid: Android can finally wear its anonymous suit. *Transactions on Data Privacy*, 7(1):27–50, 2014.

[12] A. Singla, A. Mudgerikar, I. Papapanagiotou, and A. A. Yavuz. Haa: Hardware-accelerated authentication for internet of things in mission critical vehicular networks. In *IEEE Military Communications Conference*, 2015.

[13] S. Sultana, D. Midi, and E. Bertino. Kinesis: a security incident response and prevention system for wireless sensor networks. In *Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems, SenSys '14, Memphis, Tennessee, USA, November 3-6, 2014*, pages 148–162, 2014.

[14] J. Won, S. Seo, and E. Bertino. A secure communication protocol for drones and smart objects. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '15, Singapore, April 14-17, 2015*, pages 249–260, 2015.

[15] J. Won, S. Seo, and E. Bertino. White-box attack-resistant dynamic block cipher for vehicular networks. 2016. Submitted for publication.

[16] A. Wright. Hacking cars. *Commun. ACM*, 54(11):18–19, 2011.