Security and Privacy Challenges in the Internet of Things

By Jong-Hyouk Lee and Hyoungshick Kim

This is the first installment of the new "Security and Privacy Matters" column in *IEEE Consumer Electronics Magazine*. Security and privacy are always at the heart of everything that happens in the Consumer Electronics (CE) industry. This column aims to provide insight on various aspects of security and privacy in the CE industry.

We begin by focusing on security and privacy challenges in the Internet of Things (IoT). The following items are significant topics in the current IoT landscape:

- security in mobile-edge computing (MEC)
- security in connected cars
- blockchains
- artificial intelligence and security
- usable security
- security as a service.

We will briefly examine these topics and then explore each in detail in future columns.

SECURITY IN MOBILE-EDGE COMPUTING

Fifth generation (5G) is a collective name for wireless and mobile technologies and methods. Its commercial deployments are expected in 2020. Compared with Third Generation Partnership Project Long-Term Evolution Release 8, 5G will provide much better performance, e.g., up to 20 Gb/s per km^2 traffic volume density, 1-Gb/s throughput, less than 1-ms latency contribution of the radio part, support for connecting IoT devices, and more.

A recent trend in wireless and mobile communication is virtualization in a cloud environment. For instance, various Evolved Packet Core functionalities can be implemented to the cloud for reducing costs and enhancing agility. However, the real cost of cloud computing is an increased latency, lowered control on the quality of experience, and less traffic management flexibility. To address this, MEC is being considered.

MEC, an enabling technology for 5G, allocates computing, storage, and networking resources at a network edge, e.g., base station, for compute intensive and latency sensitive applications [1]. It minimizes the interaction with the cloud, but it tends to process on the edges. Several use cases have been developed, e.g., active device location tracking, augmented reality content delivery, video analytics, radio access network aware content optimization, distributed content and domain name server (DNS) caching, and application-aware optimization.

However, MEC will pose new security and privacy issues due to its characteristics. An MEC server platform, consisting of the MEC-specific applications, an application platform, and a hosting infrastructure, is located at a network edge for localized services. As the MEC server platform is distributed at network edges (e.g., at base stations or wireless access routers, over a city), sensitive data being handled by the MEC server platform will be an easy target for attackers. The MEC server platform is much easier to hack compared with the cloud system. Attackers will be also able to physically access the MEC server platform.

Most of the current research on MEC is focused on optimization and its use cases. However, as mentioned, it will bring new security and privacy problems that should be considered before deploying MEC for 5G.

SECURITY IN CONNECTED CARS

Today's car is already a computing device that is moving. It has computing power, various software features with 100 million lines of program code, and can process up to 25 GB of data an hour [2]. Cars equipped with wireless communication systems (i.e., vehicle-to-vehicle communication and vehicle-to-infrastructure communication) are poised to deliver vehicular communication messages for traffic efficiency, safety, and infotainment. Onboard communication systems, such as controller area network, local interconnect network, and media-oriented systems transport, also exist to interconnect components inside a vehicle.

Obviously, the connected car has paved a new road for exciting opportunities. The connected car market will reach US$155 billion by 2022, while 75% of the 92 million cars will be equipped with wireless communication systems in 2020 [3]. However, news of car hacking continues to increase. Current automotive security is not enough to

Digital Object Identifier 10.1109/MCE.2017.2685019
Date of publication: 14 June 2017

protect against car hacking, and this problem is not easily solved for connected cars. What can we do to eliminate current vulnerabilities and build automobiles that are secure by design? That is a serious question to ponder.

BLOCKCHAINS

A *blockchain* is a new buzzword that was once only known to geeks and specialists on cryptocurrencies (e.g., Bitcoin), as it is the basis of the cryptocurrencies. But in the last year, it has attracted wide attention from security experts because it provides a transparent and secure means for tracking data ownership and the transfer of data without a trust entity.

Blockchains are being studied to build new security systems, e.g., decentralized versions of DNS and public key infrastructure that will have no trust entities [4]. A smart contract that is a transaction protocol to execute the terms of a contract over blockchains also allows us to build totally automated security systems, e.g., automated obligation enforcement systems. We are still at a very early stage and have an opportunity to take steps to develop various blockchain-based security systems that will provide the missing link to settle scalability, privacy, and reliability concerns in the IoT era.

ARTIFICIAL INTELLIGENCE AND SECURITY

Recent advances in artificial intelligence could boost the performance of security solutions to mitigate the risks from the cyberattacks that we are currently facing [5]. Using machine-learning techniques such as classification and clustering is not new, but the importance of these techniques has recently been greatly highlighted as machine-learning algorithms (e.g., deep learning) evolve. Previously, most research in security applications using artificial intelligence was devoted to modeling attack patterns with their unique characteristics. However, it can be inherently weak against new types of sophisticated attacks with different characteristics.

To overcome this limitation of existing machine-learning approaches, a recent trend has been to use the concept of anomaly detection to develop more generic and robust security solutions against unknown attacks that were not detected with existing attack signatures [6]. Machine learning could be applied to most applications, such as antivirus scanners, network intrusion systems, spam detectors, and fraud-detection systems. In general, such solutions work by analyzing huge amounts of data generated by network traffic, host processes, and human users to identify suspicious activities using unsupervised learning algorithms (e.g., recurrent neural networks). We expect that using artificial intelligence for security applications will soon be part of commonly used security techniques.

> We expect that using artificial intelligence for security applications will soon no longer be special but be part of a commonly used technique.

However, machine-learning-based security solutions might also be vulnerable to a new type of sophisticated attack called *adversarial machine learning* [7]. In many security domains (e.g., e-mail spam detection), the adversary can successfully control the contents of the input to the machine-learning algorithms to evade classifiers designed to detect them. Moreover, the training data set used to construct classifiers could be contaminated by adding normal samples to the abnormal sample class and/or vice versa.

USABLE SECURITY

Within a few years, it is expected that most household appliances such as televisions, washing machines, clothes dryers, dishwashers, air conditioners, light bulbs, refrigerators, and home routers will be equipped with at least one network connection (e.g., Wi-Fi, Bluetooth, or ZigBee) for the Internet. So, protecting those devices from remote attackers becomes inherently challenging. Attackers might not only try to steal a user's sensitive data from his or her household appliances but also to control them in an unauthorized manner. Recently, many home routers were infected with the notorious malware called *Mirai* (which means *the future* in Japanese) and used to launch distributed denial of service attacks [8].

To fix this problem, incoming and outgoing traffic should be properly monitored, controlled, and filtered by creating rules that specify which type of network packets are allowed and which are not. For this purpose, the firewall application is already available by default on most home routers. However, there remains a most difficult dilemma that we must overcome: how can casual users create such firewall rules?

Even though web interfaces are provided to effectively manage firewall rules, most users don't use such interfaces because they are not motivated to create the rules and do not know how those rules can be used in practice. Therefore, it will be critical to develop usable security solutions that are designed to help users easily configure, install, and maintain access control rules to control potentially harmful network traffic. Surely, it will be very challenging to develop a security configuration management tool for casual users.

SECURITY AS A SERVICE

We have traditionally implemented security features (e.g., encryption, antivirus scanning, and intrusion detection) on devices. In the era of the IoT, however, the conventional approach often has limited applicability. Because many IoT devices have limited computing resources and strict power requirements, implementation of security features can be problematic for such devices. Moreover, it's obvious that patch management is a critical issue to mitigate cybersecurity attacks. If one device in an environment is not properly patched, it may threaten the security of the entire environment. Even though device manufacturers release patches to fix software security problems, it is not easy to apply them for casual users. Manually patching IoT devices seems to be a big problem. Who is going to apply a security patch to a refrigerator?

Security as a service is a new paradigm for security management [9]. Security features are provided and managed by an external party on the cloud rather than user devices. This strategy offers several benefits. Outsourcing of administrative tasks, such as security policy management and patch management, seems helpful to significantly reduce a user's administrative burden of managing security applications. For example, a cloud-based antivirus service analyzes suspicious files submitted by thin client applications running on user devices and provides feedback about the analysis results to the client applications. Such cloud-based services can make efficient use of the collected samples from a lot of Internet users to improve the performance of the services. In this scenario, users don't need to worry about keeping the antivirus engine up to date.

CONCLUDING REMARKS

It is obvious that we are facing a new set of security and privacy challenges in IoT environments. It is probable that the IoT world would be a playground for hackers without careful consideration of its security and privacy issues. As a small step toward the construction of secure IoT systems, we will continue to focus on security and privacy changes in the IoT in depth in future columns.

ABOUT THE AUTHORS

Jong-Hyouk Lee (jonghyouk@smu.ac.kr) is a security engineer who earned his Ph.D. degree in computer engineering from Sungkyunkwan University in 2010. He is an associate editor of the security and privacy areas of *IEEE Transactions on Consumer Electronics* and *IEEE Consumer Electronics Magazine*. He is a Senior Member of the IEEE.

Hyoungshick Kim (hyoung@skku.edu) is an assistant professor in the Department of Computer Science and Engineering in the College of Information and Communication Engineering, Sungkyunkwan University. He earned his B.S. degree from the Department of Information Engineering at Sungkyunkwan University, his M.S. degree from the Department of Computer Science at KAIST, and his Ph.D. degree from the Computer Laboratory at the University of Cambridge in 1999, 2001, and 2012, respectively. He is an associate editor of *IEEE Consumer Electronics Magazine*.

REFERENCES

[1] D. Sabella, A. Vaillant, P. Kuure, U. Rauschenbach, and F. Giust, "Mobile-edge computing architecture: The role of MEC in the Internet of things," *IEEE Consum. Electron. Mag.*, vol. 5, no. 4, pp. 84–91, Oct. 2016.

[2] McKinsey & Company. (2014, Sept.). What's driving the connected car. [Online]. Available: http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car

[3] S. Kirby. (2017, Jan. 13). Securing the connected car. [Online]. Available: https://www.infosecurity-magazine.com/opinions/securing-the-connected-car/

[4] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Bootstrapping trust in distributed systems with blockchains, *;login: USENIX Mag.*, vol. 41, no. 3, 2016.

[5] G. Ollmann. (2016, Dec. 28). How artificial intelligence will solve the security skills shortage. [Online]. Available: http://www.darkreading.com/operations/how-artificial-intelligence-will-solve-the-security-skills-shortage/a/d-id/1327756

[6] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems, and tools," *IEEE Commun. Surveys Tutorials*, vol. 16, no. 1, pp. 303–336, 2014.

[7] L Huang, A. D. Joseph, B. Nelson, B. I. P. Rubinstein, and J. D. Tygar, "Adversarial machine learning," in *Proc. 4th ACM Workshop Security Artificial Intelligence*, 2011, pp. 43–58.

[8] Z. Whittaker. (2016, Nov. 29). Mirai botnet attack hits thousands of home routers, throwing users offline. [Online]. Available: http://www.zdnet.com/article/mirai-botnet-attack-hits-thousands-of-home-routers-throwing-users-offline/

[9] S. Oh, E. Kim, J. P. Jeong, H. Ko, and H. Kim, "A flexible architecture for orchestrating network security functions to support high-level security policies," in *Proc. 11th ACM Int. Conf. Ubiquitous Inform. Manage. Commun.*, 2017.

IMAGE LICENSED BY GRAPHIC STOCK