Security and Privacy Challenges in IoT-Based Machine-to-Machine Collaborative Scenarios

Hsin Chung Chen, Mohammad Abdullah Al Faruque, Pai H. Chou
Center for Embedded and Cyber-Physical Systems
University of California, Irvine, CA, 92697-2625 USA
{hsinchuc, alfaruqu, phchou}@uci.edu

ABSTRACT

Security is important in IoT as any other computing systems. However, standard solutions are necessary but not sufficient due to the added dimensions of their presence in physical space and the possibility for them to interact. This talk presents a new set of challenges on security in IoT systems that compose synergistically. We illustrate the problems and approaches using collaborative indoor localization on resource-constrained nodes as a representative example.

1. INTRODUCTION

The recent growth in the Internet of Things (IoT) also brings a set of new challenges on security and privacy. IoT devices not only perform input/output with the physical world but they are often personal in the form of object tags, biomedical monitors, and home automation systems. Their intimate connection with the owners has taken their security and privacy issues to a new level, as their attacks can affect the owners much more directly and closely than ever before. While traditional solutions to security problems are applicable and necessary, they are often not sufficient in addressing the problems in this new class of systems [9].

This talk takes a closer look at a class called collaborative IoT. These tend to be resource-constrained nodes that are embedded inside everyday objects such as keychains and wearable wristbands. For illustration purposes, let us consider location sensing as a fundamental feature. Although many such "edge devices" are unlikely to contain full-fledged location sensing capabilities due to size, power, and cost constraints, they may still get location information from a more powerful device such as a smartphone. When location information may not always be available, through collaboration, they may turn their limited location sensing capability into fairly accurate location determination by use of existing RF interface for proximity sensing, RF ranging, or inertial sensing, all of which can be done with minimal additional hardware and power overhead. Because IoT devices are likely to be deployed in larger numbers and are likely to have machine-to-machine (M2M) communication capabilities, the nodes collectively have broader coverage if their partial, local views can be pieced together to construct a more global of complete view that can then be shared with all participants in a distributed fashion. The different nodes can gather their partial location data by scanning location beacons and record their own trajectories, and upon encountering each other, they can exchange their partial location information to help each other find their locations on a map.

CODES/ISSS '16, October 01-07, 2016, Pittsburgh, PA, USA

DOI: http://dx.doi.org/10.1145/2968456.2974008

2. PRIVACY

Privacy concerns arise from the leakage of identity information that could be inferred by matching the personal profile and the available source data [2]. As an example, the MAC address is an identifier that can be used to ascertain the identity of the user. The traditional approaches include randomizing or hashing MAC address for de-identification [4]. However, they are not sufficient to thoroughly secure user privacy especially in the M2M communication scenarios, as the attack models extends beyond the cyber world into the physical space. A possible attack could be launched by utilizing RSSI or proximity sensing to infer the physical distance of nearby device. While attackers are eavesdropping on the packets combined with available distance information, the identity of user can be easily inferred without the MAC address.

One general approach to the privacy problem is to introduce entropy into the system [5]. The concept of entropy is to quantify the randomness of the system so that we can realize the difficulty for the attacker to steal the personal information. Similar to MAC address randomization, the transmit power can also be "randomized" to prevent the attacker from estimating the distance of the nearby device by leveraging the RSSI function. Today's RFICs are commonly capable of setting 3-4 different power levels (e.g., 0 dBm, -6 dBm, and -23 dBm on the CC2541 BLE MCU) but that may not add sufficient entropy. Future hardware can be built to offer more power levels. We have implemented a proof-of-concept by adding a programmable attenuator onto the RF front-end to expand the dynamic range of the RF power down by another -30 dBm to near-field level.

Another possible solution is to randomize the shared content involved in the collaboration. Take collaborative indoor localization system as an example, which entails exchanging partial trajectories that are composed with the node's own to better determine its own location on the map. To prevent the hacker from collecting the trajectory over time for identity comparison, the shared trajectory can be modified as long as it leads to the same spot on the same map. In summary, the entropy idea can be leveraged to evaluate the randomness of the system for optimization.

3. SECURITY

The general wireless network relies on the central hub or router devices to communicate with other devices. In contrast, M2M

refers to the direct communication between two devices without infrastructure support or manual intervention. This enables data exchange with a much diverse set of devices and opens up new application opportunities. However, M2M communication also poses new security challenges on the communication link and the shared content [8].

As with traditional wireless communication, encryption is the first line of defense to protect the confidentiality of the transmitted data [1]. Encryption can handle attacks such as data injection, spoofing, and eavesdropping, but the low power constraints and low cost requirement of IoT devices result in the difficulty of finding a reliable high-entropy source for key generation. One possible solution is to utilize the hardware entropy, physical unclonable function (PUF), which depends on the unique hardware structure as source of randomness to generate the key [3]. Physical layer security would be another solution since it provides a low-cost, reliable source to generate the secret key [6]. This is because the channel information from the estiblished connection between a sender and receiver pair is unique and can be leveraged as a source of high entropy.

The shared content can be another target of attack. The attacker may provide false data to severely disrupt the system operation. Cryptography or security key authorization techniques cannot resolve this attack, because false data can be spread through malicious users who are authorized to communicate with nearby devices. The scenario may be similar to the reliability issue in the wireless sensor networks, where some nodes send inaccurate data unintentionally. However, in the shared content attack model, the malicious user sends out the false data purposely. A potentially solution is to create a voting or reputation system to track the reliability of the device nodes [7].

Unfortunately, the voting and reputation solution may be insufficient for thwarting a more sophisticated attack. For example, just as a node can randomize its MAC address, the malicious user can use the same mechanism to spoof as multiple nodes to skew the vote and ruin the reputations of good nodes. The extra defense mechanism will be required to distinguish valid from forged identity in the randomized address space.

4. CONCLUSIONS

The benefits and convenience brought by IoT come with new challenges on their security and privacy. Existing solutions on networked systems form a foundation for IoT security but must be adapted to take into consideration resource constraints, the added dimension of the physical presence, and new forms of interaction such as collaborative computation. In our illustrative example of collaborative indoor localization, adding entropy can be generalized from MAC address randomization to RF power and shared content to better protect privacy without disabling collaboration. However, a clever attacker can still exploit entropy to skew votes and tarnish the reputation of genuine nodes that traditional wireless sensor networks use for outlier detection. To this extent, future solutions will require even stronger physical layer security without increasing computational or resource complexity while enabling validation of mangled identity. More generally, security and privacy in IoT will require a cross-layer solution that takes the added considerations into account.

5. ACKNOWLEDGMENTS

H.-C. Chen was supported by "Broadcom Fellowship UCI Electrical Engineering Fellowship Program" sponsored by the Broadcom Foundation.

6. REFERENCES

[1] J. Buchmann, F. Göpfert, T. Güneysu, and T. Odera. High-performance and lightweight lattice-based public-key encryption. In *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security, (IoTPTS'16)*, pages 2–9, 2016.

[2] A. K. Das, P. H. Pathak, C.-N. Chuah, and P. Mohapatra. Uncovering privacy leakage in ble network traffic of wearable fitness trackers. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, (HotMobile'16)*, pages 99–104, 2016.

[3] R. Maes, A. V. Herrewege, and I. Verbauwhede. Pufky: A fully functional puf-based cryptographic key generator. *Cryptographic Hardware and Embedded Systems, (CHES'12)*, 7428:302–319, 2012.

[4] R. Snader, R. Kravets, and A. F. H. III. Cryptocop: Lightweight, energy-efficient encryption and privacy for wearable devices. In *Proceedings of the 2016 Workshop on Wearable Systems and Applications, (WearSys'16)*, pages 7–12, 2016.

[5] D. R. Stinson. *Cryptography: Theory and Practice*. Chapman and Hall/CRC, 2005.

[6] J. Wan, A. B. Lopez, and M. A. A. Faruque. Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security. In *International Conference on Cyber-Physical Systemss, (ICCPS'16)*, pages 1–10, 2016.

[7] D. Wang, L. Kaplant, H. Le, and T. Abdelzaher. On truth discovery in social sensing: a maximum likelihood estimation approach. In *Proceedings of the 11th international conference on Information Processing in Sensor Networks, (IPSN'12)*, pages 233–244, 2012.

[8] Z. Yan, P. Zhang, and A. V. Vasilakos. A survey on trust management for internet of things. *Journal of Network and Computer Applications*, 42:120–134, 2014.

[9] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh. Iot security: Ongoing challenges and research opportunities. In *IEEE International Conference on Service-Oriented Computing and Applications, (SOCA'14)*, pages 230–234, 2014.