The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved

Wei Zhou, Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu, *Member, IEEE*

***Abstract*—Internet of Things (IoT) is an increasingly popular technology that enables physical devices, vehicles, home appliances, etc., to communicate and even inter operate with one another. It has been widely used in industrial production and social applications including smart home, healthcare, and industrial automation. While bringing unprecedented convenience, accessibility, and efficiency, IoT has caused acute security and privacy threats in recent years. There are increasing research works to ease these threats, but many problems remain open. To better understand the essential reasons of new IoT threats and the challenges in current research, this survey first proposes the concept of "IoT features." Then, we discuss the security and privacy effects of eight IoT features including the threats they cause, existing solutions to threats and research challenges yet to be solved. To help researchers follow the up-to-date works in this field, this paper finally illustrates the developing trend of IoT security research and reveals how IoT features affect existing security research by investigating most existing research works related to IoT security from 2013 to 2017.**

***Index Terms*—Internet-of-Things (IoT), IoT features, privacy, security, survey.**

I. Introduction

With the development of critical technologies in the Internet of Things (IoT), the IoT applications (e.g., smart home, digital healthcare, smart grid, and smart city) become widely used in the world. According to statistics website Statista [1], the number of connected devices around the world will dramatically increase from 20.35 billion in 2017 to 75.44 billion in 2025. International Data Corporation [2] has predicted a 17.0% compound annual growth rate in IoT spending from $698.6 billion in 2015 to nearly $1.3 trillion in 2019, there seems to be a consensus that the impact of IoT technologies is substantial and growing.

Along with the rapid growth of IoT applications and devices, cyber-attacks will also be improved and pose a more serious threat to security and privacy than ever before. For instance, remote adversaries could compromise patients' implantable medical devices (IMDs) [3] or smart cars [4], which may not only cause huge economic losses to individuals but also endanger life safety. Furthermore, as the IoT devices become widely used in industry, military, and other key areas, attackers are able to jeopardize public and national security. For example, on 21 October 2016, a multiple distributed denial of service (DDoS) [5] attacks systems operated by domain name system provider Dyn, which caused the inaccessibility of several websites, such as GitHub, Twitter, and others. This attack is executed through a botnet consisting of a large number of IoT devices including IP cameras, gateways, and even baby monitors. For another instance, Stuxnet [6], a malicious computer worm targeting to industrial computer systems, was responsible for causing substantial damage to Iran's nuclear program.

However, most of the enterprises and users lack awareness of privacy and security. A recent study by Pew Research Center [7] found that many Americans feel over-optimistic about how their data have been used. Only 26% Americans do not accept their health information to be shared with their doctor. To obtain discounts on car insurance, nearly half of Americans agree to let auto insurance companies monitor the position and speed of their cars. Moreover, due to the lack of customer demand, manufacturers only focus on implementing products' core functions while the potential security problems are ignored. IoT device vendors typically do not update and patch their devices unless the user initiates firmware updates. At the same time, IoT devices are not able to run full-fledged security mechanisms due to constrained consumption and resource. As a result, IoT devices often remain easy-to-use vulnerabilities (e.g., default passwords and unpatched bugs) for extended periods [8].

Motivated by an increasing number of vulnerabilities, attacks, and information leaks, IoT device manufactures, cloud providers, and researchers are working to design

Manuscript received January 31, 2018; revised May 16, 2018; accepted June 5, 2018. Date of publication June 15, 2018; date of current version May 8, 2019. This work was supported in part by the National Key Research and Development Program of China under Grant 2016YFB0800700, in part by the National Natural Science Foundation (NSF) of China under Grant 61572460 and Grant 61272481, in part by the Open Project Program of the State Key Laboratory of Information Security under Grant 2017-ZD-01, in part by the National Information Security Special Projects of National Development and Reform Commission of China under Grant (2012)1424, in part by the NSF under Grant CNS-1505664 and Grant CNS-1422594, and in part by the ARO under Grant W911NF-13-1-0421 (MURI). *(Corresponding author: Yuqing Zhang.)*

W. Zhou and A. Peng are with the National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 100000, China (e-mail: zhouw@nipc.org.cn; pengan@nipc.org.cn).

Y. Jia is with the School of Cyber Engineering, Xidian University, Xi'an 710071, China (e-mail: jiay@nipc.org.cn).

Y. Zhang is with the National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 100000, China, and also with the State Key Laboratory of Information Security, Institute of Information Engineering, Beijing 100000, China (e-mail: zhangyq@nipc.org.cn).

P. Liu is with the College of Information Sciences and Technology, Pennsylvania State University, State College, PA 16802 USA (e-mail: pliu@ist.psu.edu).

Digital Object Identifier 10.1109/JIOT.2018.2847733

security systems [38] and protocols [42], to explore new vulnerabilities [20], [32], and to seek effective ways to protect data privacy [64], [73]. Although researchers continue to tackle IoT security and privacy, most studies are only in its incipient stages and lack applicability. Many problems still remain open. In order to point out valuable directions for further research and provide useful references for researchers, many published survey focus on IoT security. Li *et al.* [9] and Lin *et al.* [10] mainly discussed and analyzed current attacks and challenges following IoT architecture layers. Fu *et al.* [11] highlighted some opportunities and potential threats in two specific application scenarios—home and hospital. Roman *et al.* [12] and Sicari *et al.* [13] presented research challenges and promising solutions based on different security mechanisms including authentication, access control, confidentiality, and privacy. The latest survey published by Yang *et al.* [14] summarized the main point of previous surveys and present the classification of IoT attacks. Although these surveys presented most aspects of IoT security research, threats, and open issues, and suggested some hints for future research, few of them reveal the causes of research difficulties and security threats, and clearly identify what new challenges coming from IoT. Although Yang *et al.* and Trappe *et al.* [15] discussed that restricted battery capacity and computing power enhance the difficulty of securing IoT devices, there are still many other IoT constraints and features affecting the security and privacy have not been covered.

To fill the gap, this paper discusses and analyzes the IoT security issues from a new perspective—IoT features. "IoT features" refers to the unique features of IoT devices, network, and applications, which are quite different with smartphones and computers. For example, IoT devices have much less computing ability, storage resources, and power supply, thus "constrained" is an IoT feature. The contributions of this paper are summarized as follows.

1) To find out the root reasons of current threats and main challenges in IoT security research, we first time propose the concept of IoT features.
2) To better understand the effect of IoT features, we describe eight IoT features which have the most impact on security and privacy issues and discuss the threats, research challenges, and opportunities extracted from each feature.
3) We present the trends of current IoT security and its cause based on IoT features through the analysis of existing research in recent five years.

The rest of this paper is organized as follows. Section II is the main part of this paper, we focus on eight IoT features as shown in Fig. 1, and fully discuss and analyze them, respectively. Then we collect nearly 200 prominent research papers related to IoT security from 2013 to 2017 and provide many kinds of statistical analysis with them in Section III. Finally, the conclusions are presented in Section IV.

II. Effect of IoT Features on Security and Privacy

In this section, we illustrate each IoT features from four aspects (i.e., description, threat, challenges, solutions, and opportunities) as shown in Fig. 1.

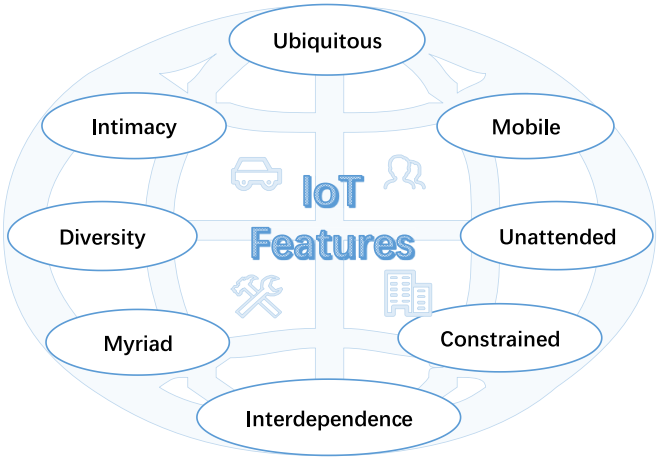


Fig. 1. IoT features.

1) *Description:* We describe what this feature is and explain what makes the feature different compared to the traditional computer or mobile phone.
2) *Threat:* We discuss what potential threats and vulnerabilities are brought by this feature, and what serious consequences are caused by these threats. We also provide diagrams and attack examples for some threats, which makes it easier for the reader to follow.
3) *Challenges:* We present what research challenges are to solve these threats.
4) *Solutions and Opportunities:* We present existing solutions tackling the challenges and threats, and discuss their drawbacks. In addition, we also demonstrate some new security techniques/ideas as opportunities that could help to wrestle with the challenges and threats.

A. Interdependence

1) Description: As the evolution of IoT devices, the interactions between devices become more complex and human involvement is needless. IoT devices are no longer just explicitly communicate with each other like traditional computers or smartphones. Many of them could also implicitly controlled by other devices' behaviors or environmental conditions using smart rules in the cloud issued by owners through the Internet like IFTTT [16], which has been widely used in IoT platforms (e.g., Samsung's SmartThings [17], Apple's HomeKit [18], and Amazon's AWS IoT [19]). For example, if the thermometer detects the indoor temperature exceeds the threshold and smart plug detects the air conditioner is in the "off" state, and then the windows will automatically open. The similar examples are more common in industrial and agricultural devices (e.g., automatic adding more water into smelters according to temperature and humidity). We describe this implicitly dependence relationship between devices as an IoT feature named "interdependence" here.

2) Threats: The target device or system itself might not be easily compromised, but the attackers could easily change other devices' behaviors or the surrounding environment, which have interdependence relationship with their target

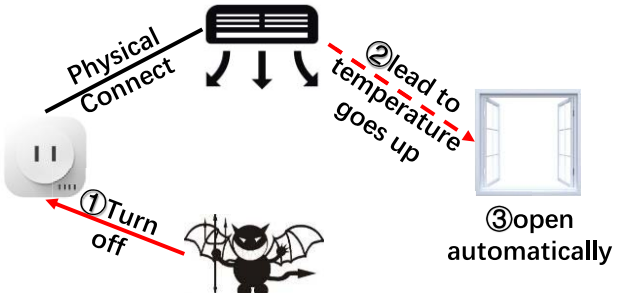


Fig. 2. Attack example of interdependence behaviors.

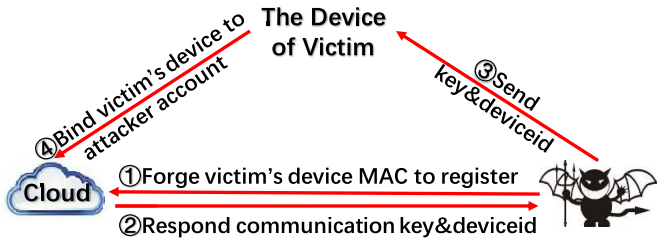


Fig. 3. Device hijacking attack example of Joylink protocols.

device. Thus, this feature could be maliciously used by attackers to reduce the difficulty of direct attack the target devices and bypass original defense mechanism. For example, back to the scenario described in the last paragraph, the attacker does not need to directly attack the automatic window control or thermometer. He could compromise the smart plug that connected to the public network to turn off the air-conditioner in a room and trigger a temperature increase, which will automatically open the windows and create a physical security breach, as shown in Fig. 2.

3) Challenges: The majority of the researchers do not realize the effect of interdependence behaviors on IoT security. Researchers generally protect the single device itself. However, it is difficult to make a clear defensive boundary of IoT devices or apply static access control methods and privilege management to them due to their interdependent behaviors. Furthermore, because the IoT device behaviors could be changed by other devices or environmental conditions, it is difficult to define a certain set of fine-grained permission rules for them. Thus, the *overprivilege* has become a common problem in the permission model of existing IoT platforms applications [20].

4) Solutions and Opportunities: The team at Carnegie Mellon University was aware of the cross-device dependencies early, and proposed a set of new security policies for detecting anomaly behavior of interdependence [21]. However, these policies will be more complicated and impractical with the increasing number of devices. Last year, Jia *et al.* [22] proposed ContexIoT, a new context-based permission system for IoT platforms to solve the overprivileged problem. It records and compares more context information, such as procedure control flow, data source, and runtime data of every device's behavior before it is executed, and then let the user allow or deny this behavior according to recorded information. That could detect the misuse of IoT devices interdependence behaviors. Because even if attackers make the misbehavior at the same physical conditions with the normal, it is hard to forge the same context information. However, this method relies too much on user decisions, once the user makes a wrong decision, the system will remember this wrong decision and will not prompt the user again. More effective and practical solutions are urgently needed to address the threats posed by the interdependence.

B. Diversity

1) Description: To better accommodate different application scenarios, heterogeneous IoT devices are designed for different specific tasks and interact strongly with the different physical environment. Thus, their hardware, system, and process requirements are unique. For example, a small temperature sensor might run on a single chip MCS-51 with small flash and RAM, while an automatic industrial machine has higher performance than our smartphone. On the other hand, different application scenarios also need different communication protocols. Even within the same application, such as smart home, different IT companies use different wireless access, authentication and communication protocols for their smart home platforms (e.g., Amazon's AWS IoT [19], JD's Joylink [23], and Alibaba's Alink [24]). The phenomenon that many different kinds of IoT devices and protocols appear in the current IoT market, we refer to as an IoT feature "diversity" here.

2) Threats: Due to many kinds of new IoT devices with insufficient safety checks beforehand, Ali mobile security team [25] found more than 90% of IoT device firmware has security vulnerabilities like hard-coded key and common Web security vulnerabilities, which could easily be used by attackers.

Due to lack of practical security experience for new IoT functions, such as IoT device bootstrapping [26], new protocols usually have many potential security problems. For instance, Liu *et al.* [27] found the attacker could exploit several vulnerabilities of Joylink protocol [23], such as insufficient device authentication shown in Fig. 3. Moreover, different protocols have different semantic definitions, the attackers could also take advantage of this point to find security vulnerabilities like BadTunnel [28] when they incorrectly work together.

3) Challenges: On the system security point, due to the diversity of IoT devices, it is hard to design a common system defense for the heterogeneous devices, especially in industry area [29]. Thus, how to discover and deal with so many security vulnerabilities among the various IoT devices needs to be addressed urgently.

On the network security point, because every protocol has differences with others, so it is important for researchers to dig out general crucial security problems of them. Besides, researchers should not only consider the security problems of one protocol itself, but also the potential security risks associated with different protocols.

4) Solutions and Opportunities: To discover and address the potential vulnerabilities for more IoT devices, researchers performed static or dynamic analysis [30] on the device firmware and source. In 2014, Zaddach *et al.* [31] put forward a framework to support dynamic security analysis for a variety of embedded systems' firmware. However, it cannot simulate all action of the real devices and need to forward action from the emulator to the device by physical connection. Thus, it is unsuitable for large-scale automated firmware analysis. Chen *et al.* [32] presented a framework for large-scale automated firmware dynamic analysis, but it is only applicable to the Linux-based system. The firmware dynamic analysis simulation framework for real-time operating system and bare-metal systems is nearly blank.

Other researchers rely on the intrusion detection system (IDS) and intrusion prevention system (IPS) to protect different kinds of devices on the same network. However, attacks are different from each other according to different target devices. Thus, some researchers pointed out the IDS and IPS systems model based on anomaly traffic detection may not work well when the network has many different kinds of devices. They suggested that the IDS and IPS systems should take abnormal parameters which affect the devices' behaviors detection as the primary task. For example, Hadžiosmanovic *et al.* [33] detected potential attacks by determining whether the parameter beyond their legal ranges. Sullivan and Colbert [34] added that the legal parameter range of industrial IoT devices should not only extract from the legal traffic, but also need to be further revised by professional and experienced operators. More suitable and effective IDS and IPS system for heterogeneous IoT devices still need further study.

C. Constrained

1) Description: With the limitation of cost and physical conditions, many IoT devices, especially industrial sensor and IMDs, have been designed to be lightweight and small. Thus, they have much less computing ability and storage resources than traditional computers or mobile phone. In addition, many military, industrial, agricultural devices have to work for a long time in environments, where charging is not available, so they also have stringent requirements for power consumption. Moreover, many IoT devices used in vehicle systems, robot control systems, and real-time healthcare systems must meet the deadline constraints of the real-time processes. We describe the limitation of the computing/storage resource, power supply and latency of IoT devices as an IoT feature named constrained here.

2) Threats: Due to constrained feature, most IoT devices do not deploy necessary defenses for system and network. For example, lightweight IoT devices do not have the memory management unit (MMU), so memory isolation, address space layout randomization, and other memory safety measures cannot be applied to these devices. Most complicated encryption and authentication algorithms like public cryptography cannot also implement on such devices, because they occupy too much computing resource and causes a long delay, which seriously affects the normal operation and reduces performance for constrained IoT devices. Consequently, it is easy for attackers to use memory vulnerabilities to compromise these devices. Also, many IoT devices even communicate with the server without any encryption or use SSL encryption without checking the server's certificate. Attackers could easily intercept communication or launch man-in-the-middle attack.

3) Challenges: How to achieve fine-grain system protections with less system software and hardware resource on lightweight IoT devices is a great challenge for researchers. In addition, such system protections also need to be satisfied with the time and power constraints in practical application condition. In addition, it is also difficult for researchers to deploy much complex encryption and authentication algorithms with less latency and computing resource on tiny IoT devices.

4) Solutions and Opportunities: To enhance system security for constrained IoT devices, previous studies focus on designing system security mechanisms for lightweight devices, but most of them still cannot satisfy both the security and application requirements. ARMor [35] a lightweight software fault isolation can be used to protect critical application code running on small embedded processors, but it caused the high-performance overhead for some programs which need checking address many times (e.g., string searching). It is therefore not applicable for real-time IoT devices. Schulz *et al.* [36] presented a bunch of trusted computing functions for lightweight devices, such as attestation and trusted execution. However, its implementation has to change the existing hardware architecture of MCU, so it cannot be directly applied to existing IoT devices. Other system defenses like EPOXY [37] and MINION [38] have been proposed recently better address above challenges, but they need to be specifically configured based on static analysis of every firmware or source code before use, which increases the burden of developers.

To protect network security for constrained IoT devices, most cryptology researchers reduce resource consumption by designing new lightweight algorithms [39]–[41] or optimize the original cryptography algorithms [42]. Nevertheless, it is difficult for lightweight algorithms to achieve the same security level with classical algorithms. Some researchers attempt new methods to address this challenge. For example, Majzoobi *et al.* [43] and Hiller *et al.* [44] proposed the authentication and key generation algorithm both based on physical unclonable functions, which use the unique physical structure of the device to identify itself. This method not only saves key storage space and simplify the key generation algorithm, but can also effectively resist the side channel analysis. Other researchers tried to use users' unique biological characteristics like gait [45] and usage habits [46] collected by some IoT devices to improve authentication algorithms. It can save storage and authenticate user and device at same time. However, biometric or physical characteristics do not always follow the same pattern. Some unpredictable factors may change them slightly. The stability and the accuracy of these new methods need yet to be further improved.

D. Myriad

1) Description: Due to the rapidly proliferating IoT devices, the amount of data these devices generated, transited, and used, will be mounting to astronomical figures. We describe the enormous number of IoT devices and the huge amount of IoT data as an IoT feature named "Myriad" here.

2) Threats: In 2016, the attack traffic of Mirai botnet which was composed of more than 1 million IoT devices, exceeded 1Tb/s, which previous cyber-attacks have never been achieved. Furthermore, more and more new botnets like *IoTroop* [47], were made mostly based on unsecured IoT devices rather than computers or smartphone, and their speed of spread is much faster and could be used to launch large-scale DDoS attacks. Pa *et al.* [48] designed honeypot and sandbox system to collect attack samples from IoT devices, and found the most remote network attacks are large-scale DDoS attacks. As more industrial and public infrastructures are connected to the Internet, the target of IoT botnets would no longer just be the website, but also the important infrastructures, which would bring grave damages to the social security.

3) Challenges: Most of IoT devices lack system defense and do not have any intrusion detection tools like anti-virus software. Furthermore, as we discussed before, IoT devices are diverse and very limited in the power supply and computing resource. Thus, how to detect and resist IoT botnet virus in IoT devices is a great challenge for researchers. At the same time, how to stop the spread of IoT botnets is also a tough problem.

4) Solutions and Opportunities: Many researchers tried to detect IoT botnets by analyzing the characteristics of the Mirai. For instance, Kolias *et al.* [49] designed a tool that extracts several attack vectors from the Mirai botnet and use them to detect potential vulnerabilities in IoT devices. While few effective methods for preventing botnet virus were proposed. Zhang and Green [50] first considered constraints of devices and environment when detecting malicious requests in a sensor network. However, their attack assumption is too simplistic. Attackers are unlikely to send requests with the same content, but usually forge normal users' requests with different reasonable content. In addition, the current DDoS intrusion detection methods are only applied in certain scenarios like smart grid [51] or the network based on a specific protocol like 6LoWPAN [52].

E. Unattended

1) Description: Smart meters, IMDs and sensors in the special industrial, agricultural and military environment have to operate for a long period of time without physical access. As increasing adoption of wireless networking prompts, these devices are evolving into IoT devices. We describe the long-time unattended status of IoT devices as an IoT feature named "unattended" here.

2) Threats: In such settings, it is hard to physically connect an external interface to verify the state of these devices. Thus, the remote attacks targeted them are difficult to detect. In addition, because such devices like IMDs and industrial control devices usually carry out crucial operations, attackers are more likely to regard them as prime targets. For instance, Stuxnet worm could infect the programmable logic controllers used in industrial control systems, which results in considerable physical damage.

3) Challenges: As mentioned above, these unattended devices are also mostly made of constrained devices. Moreover, they are usually designed to perform highly specific tasks and interact strongly with the physical environment. It is hard to deploy traditional mobile trusted computing defenses for them [29]. For instance, process memory isolation based on virtual memory is no longer feasible, because many tiny IoT devices are built on microcontrollers that do not provide MMU. Thus, building trusted execution environment (TEE) to ensure security-critical operations be correctly executed under remote exploits and verifying internal state of a remote unattended IoT device become important tasks in many scenarios.

4) Solutions and Opportunities: TrustShadow [74] use ARM TrustZone to build a TEE for security-critical applications for mobile devices. However, such technology is based on the ARM Cortex-A processor and does not support tiny IoT devices based on lightweight processors, such as ARM Cortex-M. Defrawy *et al.* [53] utilized a software/hardware co-design approach to achieve an attestation mechanism SMART with minimal hardware requirements. However, some access control logic of SMART like updating the attestation code and interacting with multiple protected processes involve too much delay. Noorman *et al.* [54] built a lightweight TEE for small embedded devices, but they did not consider how to safely handle the hardware interrupt and memory exception. Designing effective and widely applicable remote attestation, lightweight trusted execution, and safety patch methods are still open problems.

F. Intimacy

1) Description: In recent years, smart meters, wearable devices, and even some smart sex toys [55] have been widely used in our lives. These devices not only collect our biology information including heart rate and blood pressure but also monitor and record our surrounding information and daily activities like the change of indoor temperature and the locations you have been. We describe the intimate relationship between users and IoT devices as an IoT feature named "Intimacy" here.

2) Threats: The intimate relationships between users and IoT devices will certainly raise more serious and unnoticed privacy concerns. Some researchers [56] showed that attackers can infer whether the home is occupied with more than 90% accuracy just by analyzing the data of smoke and carbon dioxide sensors. The power consumption recorded by the smart plug can be used to analyze your operations on the computers [57]. In addition, more and more IoT applications use the cloud-based service, according to the Gartner statistics [58]. The sensitive data collected by IoT devices are shared with cloud-based service providers. Driven by profit, these providers usually keep this data forever and even share these data with other advertising agency

without the user's consent, which increases the risk of privacy leak.

3) Challenges: IoT applications rely on users' personal information to provide service (e.g., auto insurance companies collect driving data of each user to offer customized discounts [59]). On the other hand, collecting, transferring and using these sensitive information increases the possibility of privacy leak. Thus, how to offers an attractive tradeoff between sensitive information utility and protection is a great challenge for the academic community.

4) Solutions and Opportunities: Recently, there are increasing studies focusing on the privacy protection of IoT data. Many solutions use the data masking and encryption like homomorphic algorithm to protect sensitive information, but these solutions reduce the availability of original data and increase the time delay of data processing. Effective privacy protection method should also remain high availability of original data and minimize delay at the same time. Another major problem among current privacy protection methods is narrow application scope. The most methods are only applied to the specific application scenarios, (e.g., smart grid [60], smart medical [61], or car networking [62]), or to one process of data life-cycle (e.g., data collection [63], privacy data sharing with the cloud service [64]). More complete protection measures for private IoT data needs further in-depth research.

Conversely, due biological characteristics are different from person to person, the intimate relationships between users and IoT devices can also be contributed to cryptography. For instance, biological signals collected by IoT devices can be used to generate encryption key or user authentication [65].

G. Mobile

1) Description: Many IoT devices, such as wearable devices and smart cars are used in the mobile environment. These mobile IoT devices usually hop from one network environment to another and communicate with many unknown new devices. For example, when user drives a smart car from one district to another, the car can automatically collect road information for highway foundational facilities in the new district. It will become more common in the future. We describe the frequent movement of IoT devices as an IoT feature named "mobile" here.

2) Threats: Because mobile IoT devices usually join more networks, attackers tend to inject the malicious code into mobile IoT devices to accelerate its spread. At the same time, mobile devices need to communicate with many new devices in new network, thus attack surface of themselves will be border. These problems will become worse in social IoT devices. The social IoT devices will carry more sensitive information and automatically follow the users joining many different social networks.

3) Challenges: To confront the potential threats, the main security challenge should be addressed is cross-domain identification and trust. For example, when a mobile device hops from one domain to another, how does the new domain verify this device and what kind of permissions should be given to it? When data carried with mobile IoT devices pass from one network to another, the key negotiation, data confidentiality, integrity protection and other important security issues need to be carefully concerned.

Fig. 4. Attack example of insecure configuration.

4) Solutions and Opportunities: Chen *et al.* [66] tried to decrease the probability of mobile IoT devices being attacked in different networks through dynamically changing the security configuration of devices according to different trust condition. However, this method cannot address the root of the problem. There are few suitable access control policies for the mobile IoT devices have been proposed. More thorough studies should be done to solve these problems early.

H. Ubiquitous

1) Description: The IoT devices have pervaded every aspect of our lives. We do not just use them, but also rely more on them. IoT devices will become an indispensable part of people's daily lives like air and water. The phenomenon, IoT devices will be everywhere in our future lives, we refer to as an IoT feature "ubiquitous." In this section, we do not focus on the effect of this feature on security from a technical perspective as above. We discuss the threats caused by lack of security and privacy awareness of the ubiquitous feature. We also give some suggestions to deal with these threats, thus fundamentally avoiding "human" becoming the weakest link in the IoT security. In the remainder of this section, we discuss above issues from four distinct social roles: 1) manufacturers; 2) ordinary consumers; 3) professional operators; and 4) security researchers.

2) Threats and Suggestions:

a) Manufacturers: The manufacturers do not attach enough attention to the security of their IoT products. A large proportion of manufacturers consider security measures will add additional cost without any profits. Thus, they usually produce and deploy new IoT devices with insecure-by-default configuration. These devices not only have many known implementation vulnerabilities, but also have the potential design flaws. For example, the in-vehicle infotainment systems or vehicle navigation systems in many smart cars directly are connected to CAN-Bus. Once attackers compromise these systems, they are able to use the CAN-Bus to control the car [69], as shown in Fig. 4.

In addition, enterprises usually do not supply any security service for customers. For example, they only write simple instructions in their manual without any security suggestions and notices. Customers usually do not know what sensitive information are collected by the devices, and how to more safely use them. Manufacturers also do not help customers install patches or update firmware against new malware threats and even do not send any security warnings. Therefore,

IoT devices vulnerabilities have longer exploited period and broader impact. It is the urgent needs of setting the detailed security standards for IoT products. IoT manufactures should work tightly with the supervisory agencies, such as DHS and FSA.

b) Consumers: As the IoT device is taking off in emerging markets, the number of devices will surpass the number of humans. According to the statistics from Govtech [67], everyone will own an average of six to eight IoT devices by 2020. That is, just the number of the devices owned by each person, and the number of the devices actually used will be larger. However, most people lack the management and privacy protection awareness. As IoT devices become more intelligent and closer to our lives, they are able to automatically complete many assignments without any manual intervention and even reminders. It is therefore hard for normal users to detect their devices have been compromised until the attack causes obvious and serious consequences. People usually ignore the safety and reliability of IoT products when they use them. As a result, that increases the risk of the IoT devices being hacked by malware. For instance, Mirai virus just took advantage of default username and password to exploit many IoT devices. In 2014, we live security highlighted the discovery of 73 000 security cameras with default passwords [68]. Consumers should change their concepts and transition from a user to an IoT devices administrator. They should pay the same attention to IoT security issues as to food safety.

c) Operators: As the IoT devices are widely used in industry, agriculture and even military, the security awareness of profession operators also needs to be raised. Most operators remain optimistic that attackers may do not know how to use these specialist devices, let alone attack them [70]. Thus, when these devices have abnormal behaviors, most operators' first regard the reason is the malfunction of the equipment or their own incorrect operations. However, attacking a well-targeted device is much easier than using all devices correctly, thus operators should increase the sensitivity of abnormal behaviors and must be skilled in using security tools like IDS and IPS.

d) Researchers: In order to better meet the needs of more scenarios, IoT devices have been designed with different resources and architectures, as we mentioned above. To discover and solve the potential problems in specific scenarios early, researchers should not only focus on theory study, but also need more cooperation with consumers, manufacturers, and professional operators to make actual test and analysis. Researchers should have more comprehensive insight into the actual usage of IoT devices in the real conditions and design more practical defenses with little system resources and low extra cost.

I. Summary

The features we demonstrated above are not independent but interact with each other. For instance, the resource of most *unattended* devices is also *constrained*. When designing security solutions for these devices, researchers need to take the effect of both features into consideration. In addition, other IoT features that have less impact on security and privacy are out of the scope. Also, some IoT features, such as extensibility and integration may bring certain security and privacy issues, but most of these issues have much overlap with the discussed features. We finally summarized the main threats, challenges, and opportunities of each feature in Table I.

TABLE I
THREATS, CHALLENGES, AND OPPORTUNITIES OF EACH IOT FEATURES

Feature	Threat	Challenge	Opportunity
Inter-dependence	Bypassing static defenses, Overprivilege	Access control and privilege management	Context-based permission
Diversity	Insecure protocols	Fragmented	Dynamic analysis simulation platform, IDS
Constrained	Insecure systems	Lightweight defenses and protocols	Combining biological and physical characteristics
Myriad	IoT botnet, DDoS	Intrusion detection and prevention	IDS
Unattended	Remote attack	Remote verification	Remote attestation, Lightweight trusted execution
Intimacy	Privacy leak	Privacy protection	Homomorphic encryption, Anonymous protocols
Mobile	Malware propagation	Cross-domain identification and trust	Dynamic configuration
Ubiquitous	Insecure configuration	\	Safety consciousness

III. IoT Security Research Analysis

To help researchers catch up the latest trend of IoT security research and better understand how mentioned features affect previous IoT security research, we studied nearly 200 research papers related to IoT security from top journals and conferences according to CCF rating[1] in recent five years. Then, we demonstrate the development of IoT security research and its cause through statistical analysis of these papers. We also point out the latest IoT security research directions and priorities for further study.

A. Research Collection and Label

To facilitate understanding of the statistical analysis and classification of IoT research papers in this section. We first demonstrate how we search and filter existing research papers either in or out of this paper scope, and then introduce how we labeled each paper in this section.

After collecting the research paper from leading journals and conferences in computer security (concrete catalog see the GitHub link in the Appendix), we determined whether the research is related IoT security by the following procedure. First, we chose the words directly related to IoT as

[1][Online]. Available: http://history.ccf.org.cn/sites/ccf/biaodan.jsp?contentId=2903940690850

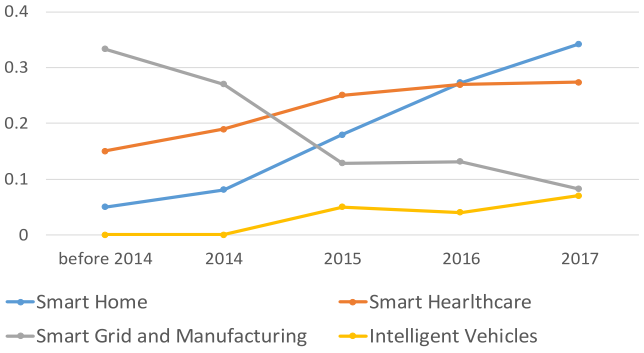


Fig. 5. Proportion of the number of papers in different application scenarios per year.

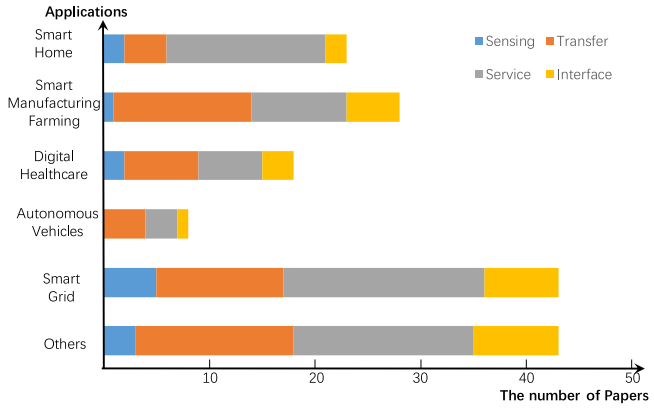


Fig. 6. Number of papers of each layer in different IoT application scenarios.

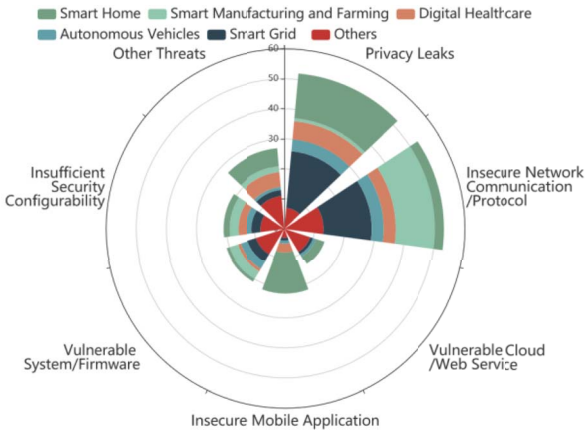


Fig. 7. Number of papers of different threat tags in different application scenarios.

IoT keywords including the types of IoT devices, protocols, and application scenarios [e.g., smartwatch, wireless sensor network (WSN), and smart home]. Then if the title of paper contains these IoT keywords or its abbreviation, we added it to this paper list. Otherwise, we checked whether the abstract of this paper includes the word "privacy" or "security," and IoT keywords at the same time. Finally, there nearly 200 research papers were singled out (all tags of these papers see the GitHub link in the Appendix).

After that, to reveal and analyze the change of hot area of IoT security research, we labeled three tags—SOA IoT layers (i.e., sensing, transfer, service, and interface) [71], application scenarios and threat for every chosen paper. It is easy to determine which layer and application this paper belong to base on its topic. Although the challenges every paper try to solve are different from each other, they usually are based on several common IoT security or privacy threats. We find out and generalize six major IoT security threats as shown in Fig. 7 based on OWASP IoT top ten [72]. Then, we label the "threat" tag of each paper according to its common threats.

B. Statistical Analysis

In this section, we draw and analyze three statistical diagram of IoT security research papers and then we also give some suggestions to researchers based on our analysis.

Fig. 5 illustrates the change of the proportion of the number of papers in different application scenarios in recent years. We can find the IoT security research hotspot always follows the development of IoT applications. For example, in the early 2010s, the use of smart grid and smart manufacturing became wider and deeper, thus the security research papers in these fields are more than others. With the rapid development of smart home and healthcare technology over the last three years, security researchers turned more attention to these fields, at the same time, the research interest in the smart grid and smart manufacturing was on the decline.

Suggestion: Security researchers should pay attention to the new IoT applications to prevent the potential threats before they emerge.

Fig. 6 shows the number of research papers in each layer of every IoT application scenario. As can be seen from the figure, security studies distribution of different layers varied from one application scenario to another. For instance, there is more research of transfer layers in smart manufacturing than in application layer, but it is opposite in smart home. Because in industrial and agriculture environment, all sensors depend on WSN to communicate with each other and remote control system. Thus, the security problems in WSN will be more dangerous to others. By contrast, smart home devices are controlled by mobile applications or Web applications. Therefore, more researchers drew more attention to application security in the smart home.

Suggestion: IoT devices in different application scenarios have different working models. Researchers should understand the differences between different scenarios, so as to grasp their main security problems.

We counted the number of research papers of each threat tag in every application scenario, as shown in Fig. 7. Most of the research focused on migrating privacy disclosure and insecure network or protocol problems, due to the intimacy, myriad, and diversity features which we have discussed above. More sensitive information has been collected, transferred and used by IoT devices especially smart home and healthcare devices, which inevitably involves more privacy problems. New IoT devices and protocols are more likely to contain potential vulnerabilities, which catching more efforts to solve these problems. The leading cause of insufficient security configures

and vulnerable cloud and Web service is the lack of security awareness as we mentioned above. In addition, although security research on IoT operating system and mobile application are less in the past years, more attackers will find and use the potential system and application vulnerabilities in future due to the constrained and interdependence IoT features. More research and attention need to be paid to these potential problems early.

Suggestion: Researchers need to investigate further to discover the root causes of new IoT security threats, and design more generic and practical protective measures.

IV. Conclusion

In this paper, we first analyze and discuss the IoT security and privacy issues from a new perspective—IoT feature. We showcase the security threats, the existing solutions, and research challenges yet to be solved associated with these IoT features. We also point out what new security technologies are required further study. Finally, based on analyzing lots of precious research, we illustrate the development trend of recent IoT security research and how IoT features reflect on the existing research. Through deeply analyzing the effect of IoT new features on security and privacy, we can better understand the future research hotspots and development of the IoT security.

Appendix

All research and survey papers that the authors collected and studied are available on the GitHub repo as shown below. The authors will continue to update the list https://github.com/chaojixx/IoT-security-papers.

References

[1] The Statistics Portal. (2017). *Internet of Things (IoT) Connected Devices Installed Base Worldwide From 2015 to 2025 (in Billions)*. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] *Internet of Things Market Statistics*, Int. Data Corporat., Framingham, MA, USA, 2016. [Online]. Available: http://www.ironpaper.com/webintel/articles/internet-of-things-market-statistics/

[3] Bigthink Edge. (2016). *Hacking the Human Heart*. [Online]. Available: http://bigthink.com/future-crimes/hacking-the-human-heart

[4] Envista Forensics. (2015). *The Most Hackable Cars on the Road*. [Online]. Available: http://www.envistaforensics.com/news/the-most-hackable-cars-on-the-road-1

[5] Wikipedia. *2016 Dyn Cyberattack*. [Online]. Available: https://en.wikipedia.org/w/index.php?title=2016_Dyn_cyberattack&oldid=763071700

[6] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May/Jun. 2011.

[7] R. Patterson. (2017). *How Safe Is Your Data With the IoT and Smart Devices*. [Online]. Available: https://www.comparitech.com/blog/information-security/iot-data-safety-privacy-attackers/

[8] GeekPwn. (2017). *IoT Devices Have a Large Number of Low-Level Loopholes*. [Online]. Available: http://www.sohu.com/a/129188339_198147

[9] S. Li, T. Tryfonas, and H. Li, "The Internet of Things: A security point of view," *Internet Res.*, vol. 26, no. 2, pp. 337–359, 2016.

[10] J. Lin *et al.*, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[11] K. Fu *et al.*, "Afety, security, and privacy threats posed by accelerating trends in the Internet of Things," Comput. Community Consortium, Washington, DC, USA, Rep., 2017. [Online]. Available: http://cra.org/ccc/wp-content/uploads/sites/2/2017/02/Safety-Security-and-Privacy-Threats-in-IoT.pdf

[12] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013.

[13] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw. Int. J. Comput. Telecommun. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[14] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[15] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the Internet of Things," *IEEE Security Privacy*, vol. 13, no. 1, pp. 14–21, Jan./Feb. 2015.

[16] L. Tibbets and J. Tane. (2012). *IFTTT*. [Online]. Available: https://platform.ifttt.com/

[17] Samsung. (2014). *SmartThings*. [Online]. Available: https://www.smartthings.com/

[18] Apple. (2014). *HomeKit*. [Online]. Available: https://developer.apple.com/homekit/

[19] Amazon. (2012). *Alexa*. [Online]. Available: https://developer.amazon.com/alexa

[20] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *Proc. IEEE Security Privacy*, San Jose, CA, USA, 2016, pp. 636–654.

[21] T. Yu *et al.*, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things," in *Proc. ACM Workshop Hot Topics Netw.*, 2015, p. 5.

[22] Y. J. Jia *et al.*, "ContexIoT: Towards providing contextual integrity to appified IoT platforms," in *Proc. Netw. Distrib. Syst. Security Symp.*, 2017, pp. 1–15.

[23] JD Alpha. (2015). *Joylink*. [Online]. Available: http://smartdev.jd.com/

[24] Alibaba. (2015). *Alink*. [Online]. Available: https://open.aliplus.com/docs/open/

[25] Alibaba. (2015). *Internet of Things Security Report*. [Online]. Available: https://jaq.alibaba.com/community/art/show?articleid=195

[26] Network Working Group Internet-Draft. (2017). *Secure IoT Bootstrapping: A Survey*. [Online]. Available: https://tools.ietf.org/html/draft-sarikaya-t2trg-sbootstrapping-03

[27] H. Liu *et al.*, "Smart solution, poor protection: An empirical study of security and privacy issues in developing and deploying smart home devices," in *Proc. IoT Security Privacy Workshop*, Dallas, TX, USA, 2017, pp. 13–18.

[28] Y. Yang. *BadTunnel: NetBIOS Name Service Spoofing Over the Internet*. [Online]. Available: https://www.blackhat.com/docs/us-16/materials/us-16-Yu-BadTunnel-How-Do-I-Get-Big-Brother-Power-wp.pdf

[29] J. Rubio-Hernan, J. Rodolfo-Mejias, and J. Garcia-Alfaro, "Security of cyber-physical systems," in *Proc. Conf. Security Ind. Control Cyber Phys. Syst.*, 2016, pp. 3–18.

[30] D. Davidson, B. Moench, S. Jha, and T. Ristenpart, "FIE on firmware: Finding vulnerabilities in embedded systems using symbolic execution," in *Proc. USENIX Security Symp.*, 2013, pp. 463–478.

[31] J. Zaddach, L. Bruno, A. Francillon, and D. Balzarotti, *AVATAR: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares*, Nat. Down Synd. Soc., New York, NY, USA, 2014.

[32] D. D. Chen, M. Egele, M. Woo, and D. Brumley, "Towards automated dynamic analysis for Linux-based embedded firmware," in *Proc. Netw. Distrib. Syst. Security Symp.*, 2016, pp. 1–16.

[33] D. Hadžiosmanovic, R. Sommer, E. Zambon, and P. H. Hartel, "Through the eye of the PLC," in *Proc. Comput. Security Appl. Conf.*, New Orleans, LA, USA, 2014, pp. 126–135.

[34] D. T. Sullivan and E. J. Colbert, "Network analysis of reconnaissance and intrusion of an industrial control system," Comput. Inf. Sci. Directorate, U.S. Army Res. Lab., Adelphi, MD, USA, Rep. ARL-TR-7775, 2016.

[35] L. Zhao, G. Li, B. D. Sutter, and J. Regehr, "ARMor: Fully verified software fault isolation," in *Proc. IEEE Int. Conf. Embedded Softw.*, Taipei, Taiwan, 2011, pp. 289–298.

[36] P. Schulz, S. Koeberl, A.-R. Sadeghi, and V. Varadharajan, "TrustLite: A security architecture for tiny embedded devices," in *Proc. ACM EuroSys*, Amsterdam, The Netherlands, 2014, pp. 1–14.

[37] A. A. Clements *et al.*, "Protecting bare-metal embedded systems with privilege overlays," in *Proc. IEEE Security Privacy*, San Jose, CA, USA, 2017, pp. 289–303.

[38] C. H. Kim *et al.*, "Securing real-time microcontroller systems through customized memory view switching," in *Proc. Netw. Distrib. Syst. Security Symp.*, 2018.

[39] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 763–771, May 2014.

[40] Y. Shi, W. Wei, Z. He, and H. Fan, "An ultra-lightweight white-box encryption scheme for securing resource-constrained IoT devices," in *Proc. ACM Conf. Comput. Security Appl.*, 2016, pp. 16–29.

[41] J. Buchmann, F. Göpfert, T. Güneysu, T. Oder, and T. Pöppelmann, "High-performance and lightweight lattice-based public-key encryption," in *Proc. 2nd ACM Int. Workshop IoT Privacy Trust Security*, 2016, pp. 2–9.

[42] T. Rauter, A. Höller, N. Kajtazovic, and C. Kreiner, "Privilege-based remote attestation: Towards integrity assurance for lightweight clients," in *Proc. ACM Workshop IoT Privacy Trust Security*, 2015, pp. 3–9.

[43] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas, "Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching," in *Proc. IEEE Security Privacy Workshops*, San Francisco, CA, USA, 2012. pp. 33–44.

[44] M. Hiller, A. G. Önalan, G. Sigl, and M. Bossert, "Online reliability testing for PUF key derivation," in *Proc. Int. Workshop Trustworthy Embedded Devices*, 2016, pp. 15–22.

[45] W. Xu *et al.*, "KEH-Gait: Towards a mobile healthcare user authentication system by kinetic energy harvesting," in *Proc. Netw. Distrib. Syst. Security Symp.*, 2017.

[46] R. A. Scheel and A. Tyagi, "Characterizing composite user-device touchscreen physical unclonable functions (PUFs) for mobile device authentication," in *Proc. Int. Workshop Trustworthy Embedded Devices*, 2015, pp. 3–13.

[47] Checkpoint Research. (2017). *IoTroop Botnet: The Full Investigation*. [Online]. Available: https://research.checkpoint.com/iotroop-botnet-full-investigation/

[48] Y. M. P. Pa *et al.*, "IoTPOT: Analysing the rise of IoT compromises," in *Proc. USENIX Conf. Offensive Technol.*, 2015, p. 9.

[49] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, Jul. 2017.

[50] C. Zhang and R. Green, "Communication security in Internet of Thing: Preventive measure and avoid DDoS attack over IoT network," in *Proc. Symp. Commun. Netw. Soc. Comput. Simulat. Int.*, 2015, pp. 8–15.

[51] Z. Lu, W. Wang, and C. Wang, "Camouflage traffic: Minimizing message delay for smart grid applications under jamming," *IEEE Trans. Dependable Secure Comput.*, vol. 12 no. 1, pp. 31–44, Jan./Feb. 2015.

[52] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito, "DEMO: An IDS framework for Internet of Things empowered by 6LoWPAN," in *Proc. ACM Sigsac Conf. Comput. Commun. Security*, 2013, pp. 1337–1340.

[53] K. E. Defrawy, A. Francillon, D. Perito, and G. Tsudik, "SMART: Secure and minimal architecture for (establishing a dynamic) root of trust," in *Proc. Netw. Distrib. Syst. Security Symp.*, 2012.

[54] J. Noorman *et al.*, "Sancus: Low-cost trustworthy extensible networked devices with a zero-software trusted computing base," in *Proc. 22nd USENIX Conf. Security*, 2013, pp. 479–494.

[55] E. A. Moore and USA Today. (2016). *Woman Sues Sex-Toy Maker for Invading Privacy*. [Online]. Available: http://www.usatoday.com/story/news/2016/09/15/womansues-sex-toy-maker-invading-privacy/90400592/

[56] B. Copos, K. Levitt, M. Bishop, and J. Rowe, "Is anybody home? Inferring activity from smart home network traffic," in *Proc. IEEE Security Privacy Workshops*, San Jose, CA, USA, 2016, pp. 245–251.

[57] M. Conti, M. Nati, E. Rotundo, and R. Spolaor, "Mind the plug! Laptop-user recognition through power consumption," in *Proc. ACM Int. Workshop IoT Privacy Trust Security*, 2016, pp. 37–44.

[58] Volansys. (2016). *Connecting Devices to Cloud IoT Platform-As-a-Service: Challenges and Solution*. [Online]. Available: https://volansys.com/connecting-devices-cloud-iot-platform-service-challenges-solution/

[59] MarketsandMarkets. (Dec. 2015). *Insurance Telematics Market Worth 2.21 Billion USD by 2020*. [Online]. Available: http://www.prnewswire.com/news-releases/insurance-telematics-market-worth-221-billion-usd-by-2020-561817961.html

[60] W. Yang *et al.*, "Minimizing private data disclosures in the smart grid," in *Proc. ACM Conf. Comput. Commun. Security*, 2012, pp. 415–427.

[61] E. M. Chan, P. E. Lam, and J. C. Mitchell, "Understanding the challenges with medical data segmentation for privacy," in *Proc. USENIX Conf. Safety Security Privacy Interoperability Health Inf. Technol.*, 2013, p. 2.

[62] L. Guo *et al.*, "A secure mechanism for big data collection in large scale Internet of Vehicle," *IEEE Internet Things J.*, vol. 4, no. 4, pp. 601–610, Apr. 2017.

[63] G. Barthe, G. Danezis, B. Grégoire, C. Kunz, and S. Zanella-Béguelin, "Verified computational differential privacy with applications to smart metering," in *Proc. IEEE Comput. Security Found. Symp.*, New Orleans, LA, USA, 2013, pp. 287–301.

[64] L. Yang, A. Humayed, and F. Li, "A multi-cloud based privacy-preserving data publishing scheme for the Internet of Things," in *Proc. ACM Conf. Comput. Security Appl.*, 2016, pp. 30–39.

[65] S.-Y. Chang, Y.-C. Hu, H. Anderson, T. Fu, and E. Y. Huang, "Body area network security: Robust key establishment using human body channel," in *Proc. USENIX Conf. Health Security Privacy*, 2012, p. 5.

[66] I.-R. Chen, F. Bao, and J. Guo, "Trust-based service management for social Internet of Things systems," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 6, pp. 684–696, Nov./Dec. 2016.

[67] Govtech. (2015). *FutureStructure: The New Framework for Communities (Infographic)*. [Online]. Available: http://www.govtech.com/dc/articles/FutureStructure-The-NewFramework-for-Communities.html

[68] WeLiveSecurity. (Oct. 2016). *10 Things to Know About the October 21 IoT DDoS Attacks*. [Online]. Available: https://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/

[69] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," in *Proc. Black Hat USA*, Las Vegas, NV, USA, 2015.

[70] A. Wright, "Mapping the Internet of Things," *Commun. ACM*, vol. 60, no. 1, pp. 16–18, 2016.

[71] Z. Bi, L. D. Xu, and C. Wang, "Internet of Things for enterprise systems of modern manufacturing," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1537–1546, May 2014.

[72] OWASP. (2014). *OWASP Internet of Things Top Ten*. [Online]. Available: https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

[73] L. Guan *et al.*, "From physical to cyber: Escalating protection for personalized auto insurance," in *Proc. 14th ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, 2016, pp. 42–55.

[74] L. Guan *et al.*, "TrustShadow: Secure execution of unmodified applications with ARM TrustZone," in *Proc. 15th Annu. Int. Conf. Mobile Syst. Appl. Services*, 2017, pp. 488–501.

Wei Zhou received the B.S. degree in information security from Xidian University, Xi'an, China, in 2016. He is currently pursuing the Ph.D. degree at the National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing, China, under the supervision of Dr. Y. Zhang.

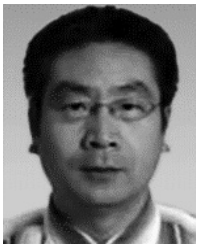
His current research interests include embedded system security, trust computing, and network security.

Yan Jia received the B.S. degree in information countermeasure technology from Xidian University, Xi'an, China, in 2015, where he is currently pursuing the Ph.D. degree in information security at the School of Cyber Engineering.

His current research interests include IoT security, Web security, network, and system security.

Anni Peng received the B.S. degree from the School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China, in 2017. She is currently pursuing the Ph.D. degree at the National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing, China, under the supervision of Dr. Y. Zhang.

Her current research interests include IoT security, networks, and system security.



Yuqing Zhang received the Ph.D. degree in cryptography from Xidian University, Xi'an, China.

He is a Professor and the Director of National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing, China. He has authored or co-authored over 100 research papers in international journals and conferences, such as the ACM *CCS*, the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING. His research has been sponsored by NSFC, Huawei, Qihu360, and Google. His current research interests include network and system security and applied cryptography.

Peng Liu (M'99) received the B.S. and M.S. degrees from the University of Science and Technology of China, Hefei, China, and the Ph.D. degree from George Mason University, Fairfax, VA, USA, in 1999.

He is a Professor of information sciences and technology, the Founding Director of the Center for Cyber-Security, Information Privacy, and Trust, and the Founding Director of the Cyber Security Laboratory, Pennsylvania State University, State College, PA, USA. He has authored or co-authored a monograph and over 260 refereed technical papers. His research has been sponsored by the U.S. National Science Foundation, ARO, AFOSR, DARPA, DHS, DOE, AFRL, NSA, TTC, CISCO, and HP. His current research interests include computer and network security.

Dr. Liu has served on over 100 Program Committees and reviewed papers for numerous journals.