Yuan B, Wan J, Wu YH *et al.* On the security of smart home systems: A survey. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 38(2): 228-247 Mar. 2023. DOI: 10.1007/s11390-023-2488-3

On the Security of Smart Home Systems: A Survey

Bin Yuan[1, 2, 3, 4, 5, 6] (袁　斌), *Member, CCF, ACM, IEEE*, Jun Wan[1, 2, 3, 4, 5] (万　俊)
Yu-Han Wu[4, 5, 7, 8] (吴宇晗), De-Qing Zou[1, 2, 3, 4, 5, *] (邹德清), *Senior Member, CCF, Member, ACM, IEEE*, and Hai Jin[4, 5, 7, 8] (金　海), *Fellow, CCF, IEEE, Lifetime Member, ACM*

[1] *School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China*

[2] *Hubei Key Laboratory of Distributed System Security, Huazhong University of Science and Technology Wuhan 430074, China*

[3] *Hubei Engineering Research Center on Big Data Security, Huazhong University of Science and Technology Wuhan 430074, China*

[4] *National Engineering Research Center for Big Data Technology and System, Huazhong University of Science and Technology, Wuhan 430074, China*

[5] *Services Computing Technology and System Lab, Huazhong University of Science and Technology, Wuhan 430074, China*

[6] *Shenzhen Huazhong University of Science and Technology Research Institute, Shenzhen 518057, China*

[7] *School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China*

[8] *Cluster and Grid Computing Lab, Huazhong University of Science and Technology, Wuhan 430074, China*

E-mail: yuanbin@hust.edu.cn; M202071401@hust.edu.cn; M201973097@hust.edu.cn; Deqingzou@hust.edu.cn
hjin@hust.edu.cn

Received May 10, 2022; accepted March 14, 2023.

Abstract　Among the plethora of IoT (Internet of Things) applications, the smart home is one of the fastest-growing. However, the rapid development of the smart home has also made smart home systems a target for attackers. Recently, researchers have made many efforts to investigate and enhance the security of smart home systems. Toward a more secure smart home ecosystem, we present a detailed literature review on the security of smart home systems. Specifically, we categorize smart home systems' security issues into the platform, device, and communication issues. After exploring the research and specific issues in each of these security areas, we summarize the root causes of the security flaws in today's smart home systems, which include the heterogeneity of internal components of the systems, vendors' customization, the lack of clear responsibility boundaries and the absence of standard security standards. Finally, to better understand the security of smart home systems and potentially provide better protection for smart home systems, we propose research directions, including automated vulnerability mining, vigorous security checking, and data-driven security analysis.

Keywords　IoT (Internet of Things), smart home, IoT security, smart home security

1　Introduction

With the rapid development of the Internet of Things (IoT), digitally connected devices and applications, including the smart home, office, and car, play an increasingly vital role in human life. Among the plethora of emerging IoT applications, the smart home is one of the most popular. IDC's report shows that the worldwide market of smart home applications is growing rapidly—in the next five years, China's smart home devices market shipments will continue to grow at a compound growth rate of 21.4%, with market shipments reaching 540 million units in 2025, while the number of smart home devices in Eu-

Survey

This work was supported by the Hubei Provincial Key Research and Development Technology Special Innovation Project under Grant No. 2021BAA032, the Wuhan Applied Foundational Frontier Project under Grant No. 2020010601012188, and the Guangdong Provincial Key Research and Development Plan Project of China under Grant No. 2019B010139001.

*Corresponding Author

rope will also reach 210 million in 2025[①].

Today, the smart home has influenced users' lives in various aspects, helping users manage their time effectively and save on various energy sources. One advantage of smart home devices is that they can be controlled remotely by users. For example, users can adjust the temperature of home air-conditioning before returning home, and Airbnb hosts can open doors for guests remotely. Another advantage is that they can provide intelligent automation control. For example, soft lights and music will wake users from their dreams to a breakfast that has already been heated in the microwave oven.

However, as a huge platform with all kinds of powerful functions, the smart home is facing a growing number of security issues. Researchers report that 70% of commonly-used IoT devices have serious vulnerabilities, with an average of 25 vulnerabilities per device[1]. These different types of threats and attacks not only compromise the security of the devices themselves but also pose a challenge to user privacy and authority and can directly endanger the user's safety or cause serious business losses. In fact, attacks on the smart home are increasingly emerging. For example, the Nest thermostat can turn on the camera without the owner's knowledge[②]; hackers can monitor babies through a flaw in the Philips baby cam[2]; and there are distributed denial of service (DDoS) attacks such as the "Mirai botnet"[3] that swept the US in 2016, whose imitators later made more use of the back door left by suppliers[③]. In general, detecting smart home security problems and finding effective solutions to these issues have become a top priority.

In the past few years, researchers have investigated the security problems of smart home systems. To provide a systematic review of the current smart home security research, we present a comprehensive literature survey on the security of smart home systems. It has a foundation for summarizing future research directions and providing practical guidance on designing secure smart home systems.

We will first introduce the current mainstream smart home architecture and describe various components in the architecture, as well as the relationship between the components, in Section 2. In Section 3, we categorize the security issues of smart home systems into three areas: platform security, device security, and communication security. We then review these security issues in the following three sections (Section 4, Section 5 and Section 6) respectively. Section 7 discusses the root causes of the security risks in current smart home systems and summarizes future research directions. Finally, we conclude this paper in Section 8.

2 Architecture of Smart Home Systems

Currently, many smart home platforms are designed by different service providers, such as HomeKit from Apple[④] and SmartThings from Samsung[⑤]. However, the systems of most of the mainstream platforms from different providers are similar. This section summarizes the architectures of the current mainstream smart home systems and some typical smart home usage scenarios.

2.1 Components of Smart Home Systems

We summarize the main components of smart home systems and their interactions in Fig.1, including smart devices, gateway devices, IoT cloud platforms, communication channels, and end users. These five components' main functions, manufacturers, and interactions are described below.

• Smart devices can collect physical environment information through sensors in real time and submit it to cloud platforms or end users. They can also receive instructions from cloud platforms or end users to perform corresponding device operations. Common smart devices include the light bulbs made by LIFX[⑥] and Philips Hue[⑦], the home appliances made by SmartThings, Xiaomi[⑧], and among many others.

• Gateway devices connect smart devices close to the gateways with the help of multiple wireless proto-

[①]IDC. https://www.yelunet.com/chanye/iot/2021-10-29/1726.html, Mar. 2023.
[②]Hacker breaks into smart home google nest devices terrorizes couple. https://www.businessinsider.com.au/hacker-breaks-into-smart-home-google-nest-devices-terrorizes-couple/-2019-9?r=US&IR=T, Nov. 2021.
[③]Hikvision backdoor confirmed. https://ipvm.com/reports/hik-backdoor, Nov. 2021.
[④]Apple. Home app—Apple. https://www.apple.com/ios/home/, Apr. 2023.
[⑤]Samsung SmartThings. Add a little smartness to your things. https://www.smartthings.com/, Mar. 2023.
[⑥]Lifx. https://www.lifx.com/, Mar. 2023.
[⑦]Philips hue. https://www.philips-hue.com/, Mar. 2023.
[⑧]Xiaomi. https://www.mi.com/, Mar. 2023.

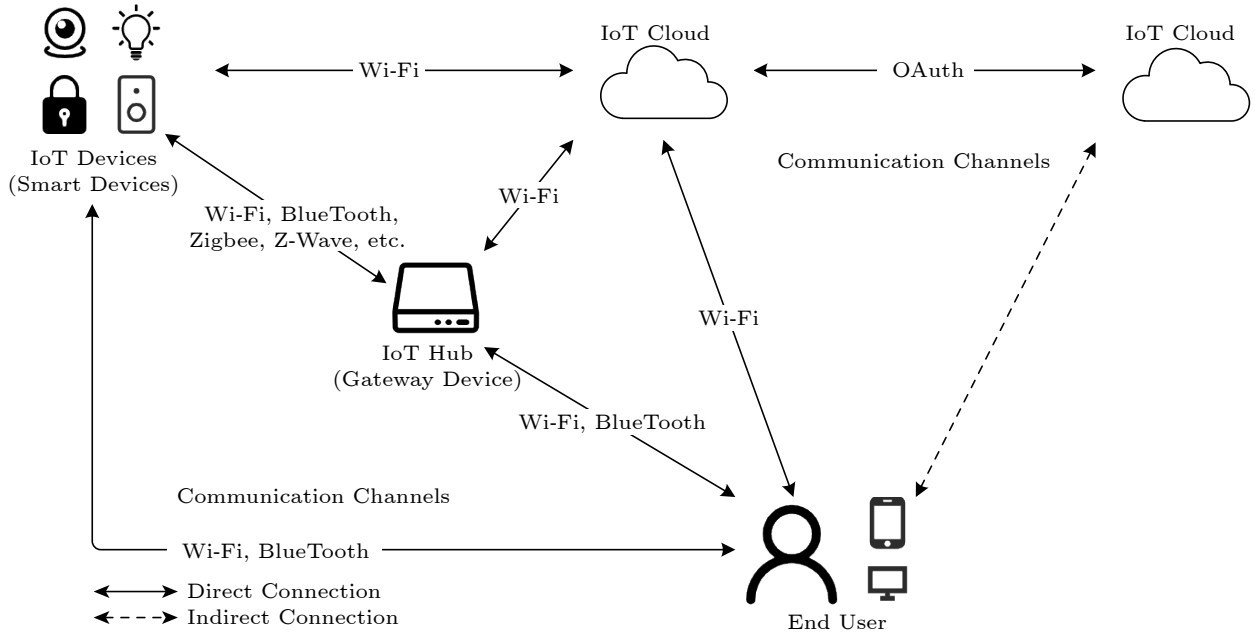


Fig.1. Architecture of smart home systems.

cols, gather sensor data from the smart devices, and submit it to the cloud platform or end user. Common gateway devices include the SmartThings hub, the Xiaomi gateway, and the Aqara gateway.

• Cloud platforms consist of various application services deployed by various smart home platform vendors in the cloud. For instance, SmartThings, Philips, and LIFX provide certification management services that allow users to manage devices. SmartThings and IFTTT provide programming services that help users create trigger-action rules (e.g., SmartApp, applet) to implement automated device operations (such as opening the door when a movement is detected at the door).

• Communication channels connect to the Internet through a wired network (such as Ethernet) or wireless protocol (such as Wi-Fi, Zigbee, Z-wave, or BlueTooth) to achieve communication among smart devices, gateway devices, cloud platforms, and users. However, because of the differences in the protocols supported by various components in the smart home, the protocols used for communication between different components are also different. We mark the different protocols that may be used when every two components communicate in Fig.1.

• With the help of the above components, the end users can simply control smart devices by operating applications and web pages. For example, SmartThings, LIFX, and Philip Hues provide users with applications to remotely control smart devices.

2.2 Typical Control Scenarios

Once all the components can communicate normally, the smart home systems will start to serve users. Typical smart home scenarios include automation control scenarios and cross-cloud platform control scenarios.

• *Device Automation Control Scenario.* Taking SmartThings as an example, after a user purchases a SmartThings device, the user first needs to connect the device with the SmartApp in the SmartThings companion application through the Wi-Fi protocol or hub. Afterward, SmartApp can subscribe to SmartDevice (encapsulate physical devices and communicate with SmartApps to control the devices) events or events related to a specific time, location, and mode. When an event occurs in a device or an environment, the event management subsystem triggers the execution of SmartApp and sends instructions to the device to perform corresponding device automation operations[9].

• *Cross-Cloud Devices Automation Control Scenarios.* To relieve the burden on users of using multiple apps to control different manufacturers' devices, third-party service providers offer a solution—cross-

[9]SmartThings Developer. https://smartthings.developer.samsung.com/, Mar. 2023.

cloud device control—in which users can use one and only one app to control all their smart home devices from different manufacturers. For example, to enable cross-cloud device control with Google Home, the user first binds/connects the device (e.g., a Philips Hue bulb) to the manufacturer's cloud platform (Philips Hue cloud). Then, the user authorizes Google Home to control the Philips Hue bulb, after which the Philips Hue cloud issues an OAuth token to Google Home. In this way, the user can use the Google Home app to control the Philips Hue bulb by the OAuth protocol.

3 Security Issues of Smart Home Systems

As introduced in Section 2, in the application scenarios of smart home systems, the components interact with each other. Therefore, if any one of them is exploited by an attacker, the security of the whole smart home system may be affected.

Considering that the gateway device is a special smart device, we combine gateway devices and smart devices as a category to simplify the analysis of the security issues of smart home systems. Ultimately, we simplify the components of the smart home systems into three parts: cloud platforms, smart devices, and communication channels, and we analyze the security issues of the three parts, respectively.

Firstly, cloud platforms provide users with application-level services (such as authentication management, voice assistant, automation program and so on). Therefore, the defects of the platform itself may allow attackers to affect the normal use of these services or even threaten the security of other components of the smart home systems[4–9]. In addition, when the degree of automation control in a smart home becomes higher, the interaction between platform automation applications becomes more complicated and easier to be exploited by attackers[10–13].

Secondly, smart devices provide services and perform operations at the level of the physical environment. The malicious operations of smart home devices by attackers will directly affect the privacy security, personal safety, and property safety of end users[3, 14–18]. Therefore, the security of intelligent devices and the environmental changes arising from their implementation must be focused on. In addition, smart devices are different from traditional devices in that they add many sensors, and their execution may be affected by sensors[16].

Finally, since the communication channels transmit data between components, they significantly impact on users' private information security[19, 20]. In addition, the communication channels are diverse and have different characteristics that may be exploited by attackers[21–25].

In addition, since all three components need to process data in use, we are concerned about these three components' privacy security issues.

Table 1 lists the related questions of our investigation, which are expanded in detail in Sections 4–6. Besides, Fig.2 shows the scope of influence of smart home systems security issues.

4 Platform Security of Smart Home Systems

The security of the cloud platforms is related to the entire smart home systems. If an attacker takes advantage of the security risks of a platform, it will affect all the devices and end users under the platform. After conducting a systematic investigation of existing research, we divide the security issues of the cloud platforms into six categories: programming security, linkage security, authentication, authorization, voice assistants security and privacy protection.

4.1 Programming Security

4.1.1 Threats

As stated in Section 2, some smart home plat-

Table 1. Research Type of Smart Home Systems Security

Analysis Field	Security Issue Category	Specific Issue
Platform security	Platform programming, platform linkage, authentication, authorization, voice assistant, platform privacy protection	API interface interaction vulnerabilities, application dependency conflicts, violations, cheats, defective authentication between users and platforms, vulnerable access control between users and platforms, defective speech recognition algorithm, information maliciously leaked
Device security	Device vulnerability, sensor linkage, side-channel information, authentication, authorization, device privacy protection	Devices abused or disabled, device sensor dependency conflicts, violations, cheats, device cheating and privacy disclosure, defective authentication between users and devices, vulnerable access control between users and devices, information maliciously leaked
Communication security	Protocol vulnerability, communication flow	Protocol connectivity abused, information maliciously leaked

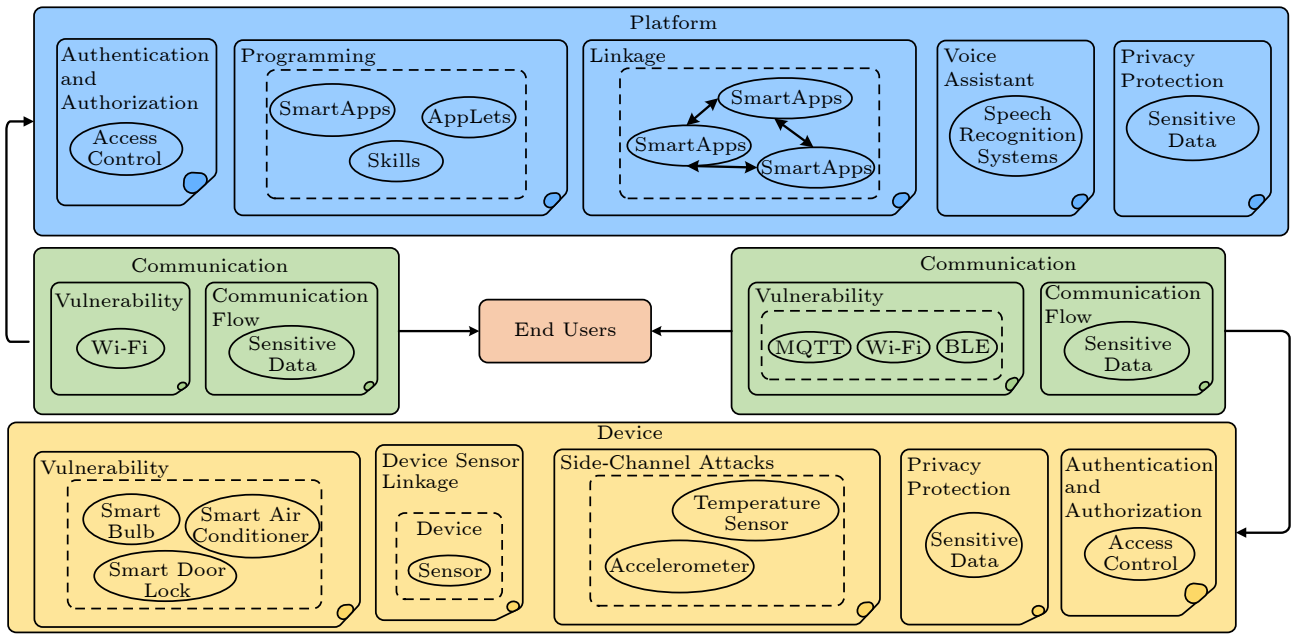


Fig.2. Scope of influence of smart home systems security issues.

forms provide developers with programming frameworks, for example, SmartThings allows users to develop SmartApps, and virtual personal assistant (VPA) allows users to develop skills, which greatly facilitates the customization needs of users. Unfortunately, attackers can exploit vulnerabilities in programming frameworks to write malicious applications to carry out attacks.

By way of illustration, because of the coarse granularity of permissions, Fernandes *et al.*[4] proposed that SmartApp can use the `sendLocationEvent` API forgery event to change the mode and then trigger malicious actions. Similarly, VPA can also be attacked by malicious skills. Cheng *et al.*[26] proved that it is still difficult to fully carry out the certification of skills by the platform. They released some of their design of Amazon Alexa skills and Google Assistant actions, a large portion violating the platform provider's strategy but passing the certification.

In addition to malicious automated programs developed by attackers, security protection is insufficient in some APIs, for example, Google's Nearby Connections API[27], which can be used by attackers to access all Wi-Fi traffic of the victim, tamper with the victim's configuration, and even force the victim to establish a TCP connection with other arbitrary devices.

4.1.2 *Mitigations*

For security issues of platform automation applications, since many involve the underlying and undisclosed design of the platforms, the solution to the vulnerability requires consultation with the platform provider. To be more specific, there will be different solutions to specific attacks. For example, in response to fake events, HoMonit[28] converts the behaviors into DFAs, and detects abnormal operations of SmartApps from encrypted wireless traffic by comparing them with the expected behaviors. In addition, for the programming problems existing in VAP, Zhang *et al.*[5] conducted a review of skills with the help of a skill-name scanner to help prevent attacks.

Summary. The programming problems of the platform mainly include malicious automated applications and the abuse of unsafe API interfaces. At present, some researchers have designed the audit scheme of automated applications for platform suppliers[5, 28]. However, a more in-depth research is still needed to improve the accuracy and compatibility of detection. In addition, platform providers can also redesign insecure public interfaces to prevent them from being abused by attackers.

4.2 Linkage Security

4.2.1 *Threats*

As we have discussed, cloud platforms connect various household devices and make it easy for end users to create new features through programmatic abstractions such as automated rules. However, unex-

pected interactions (such as conflicts, violations, and cheats) between rules can lead to new security issues[11]. For example, an attacker could use a heater to trigger the "open windows when room temperature reaches a certain value" rule and then enter the room, which will seriously threaten the safety of users[13].

4.2.2 Mitigations

In order to solve linkage security threats, some researchers use static program analysis methods to ensure the security of IoT applications through application description and source code analysis. For example, Wang *et al.*[11] first enumerated the inter-rule loopholes in the trigger-action platform, then developed a new evaluation method based on natural language processing(NLP), checked the trigger and action descriptions on the IoT platform website, and determined that 66% of the deployments in the IFTTT ecosystem may have interaction vulnerabilities between their rules. Similarly, A3ID[12] uses the NLP technology and a vocabulary database to extract device information from the knowledge graph, and then detect the antisense relationship between two functional descriptions to identify conflicts. In addition to using NLP techniques, IoTMon[13] analyzes applications through static programs to obtain essential information (such as triggers, devices, and actions) to build applications.

However, these static methods are insufficient to identify violations in a multi-application environment, and the problem of dataset annotation exists in NLP. Therefore, another type of solutions dynamically detects by generating a directed graph and comparing it with the actual execution graph. For instance, Celik *et al.*[29] proposed a dynamic system, IOTGUARD, which collects the information of the application at run time, describes its behavior with a directed graph, and compares it with the previously generated policy to analyze whether there are exceptions, and then perform operations according to the response. Analogously, IOTSAFE[30] generates static interaction graphs through static analysis and generates directed interaction graphs by capturing real physical interactions between IoT devices through dynamic testing techniques to implement safety/security policies. RemedIoT[31] uses actuation graphs and policies to detect conflicts in an IoT-based smart environment.

In particular, by modeling the IoT ecosystem as a finite state machine, SAFECHAIN[32] transforms the problem of discovering the attack chain into an accessibility problem in the finite state machine (FSM). Compared with other methods of discovering attack chains[30, 31], the method is more efficient and detects more comprehensive attacks.

Summary. At present, there are two kinds of solutions to the linkage problem of automation applications. One combines NLP and static program analysis methods, and the other combines graph and dynamic program analysis methods. In the future, dynamic program analysis can be combined with NLP, and further machine learning models can be added to achieve more automated solutions. In addition, more novel methods can be designed to discover abnormal linkage.

4.3 Authentication

4.3.1 Threats

There are usually multiple users or other visitors in smart home scenarios. An incomplete authentication mechanism in the platforms may allow attackers to gain access to smart home components, causing great harm to users' security and privacy. Some adversaries may impersonate a real user. For example, malicious attackers can imitate real users to send smart home voice commands[6].

4.3.2 Mitigations

To solve the authentication problem, Dong and Yao[6] used biometric features such as vocal cord vibration and lip movement to authenticate users. In another approach, HomeShield[7] is a credential-less authentication framework used to protect smart home systems.

Summary. There is little research on the protection measures of user identity authentication, and more novel solutions are needed in the future.

4.4 Authorization

4.4.1 Threats

Authorization is another key concern for platforms, and flaws in platform authorization mechanisms may allow attackers to gain excessive device control, further threatening user security. Recently, Fernandes *et al.*[4] discovered that the inherent design

flaws of SmartThings make SmartApps overprivileged, exposing users to risks. They exampled four proof-of-concept attack cases that demonstrated the seriousness of the overprivileged problem.

In addition, there is no standard delegation agreement for cross-cloud delegation supported by mainstream IoT clouds. Therefore, delegation will bring security risks, such as allowing an attacker to access the victim's device without authorization[33]. Similarly, Schuster *et al.*[34] found that many commercial frameworks couple the implementation of the situation tracking with access control, resulting in excessive privileges.

4.4.2 *Mitigations*

In response to the above problems, some researchers have proposed corresponding solutions. On the one hand, authorization operations rely heavily on the user's understanding of permissions. Therefore, SmartAuth[35] uses information gleaned from application descriptions, code, and comments to generate interfaces that explain the connection between authorization and actual operations, ultimately enhancing the platform's security policies. On the other hand, we need to strengthen the platform's control over permissions. To achieve the goal of access control, ContexIoT[36] automatically patches SmartApps and provides rich context information to help users run time to achieve the goal of access control. SoftAuthZ[37] uses a linear regression model to generate scores related to specific attributes (such as environment context and requested functions) to make context-sensitive authorization decisions. HoMonit[28] infers SmartApps activities from encrypted traffic, and then compares them with the expected behavior specified in source code or UI interfaces.

In addition to access control on a cloud, the privilege problem caused by the cross-cloud platform OAuth also needs to be noticed. Fernandes *et al.*[38] introduced decentralized action integrity to prevent attackers from abusing OAuth tokens in ways inconsistent with the given user rules. They installed the client on the device, obtained the rule-specific tokens bound to related information, and then interacted with the cloud service to achieve access control. Furthermore, Schuster *et al.*[34] proposed a new access control method, introducing environmental situation oracles (ESOs) to enable multiple access control frameworks in the entire ecosystem to execute common policies consistently and reduce excessive privileges.

Summary. At present, researchers have paid attention to the issues of single-platform authorization and cross-cloud platform authorization and have designed many context-sensitive mechanisms for platform authorization. In the future, we still need to innovate the authorization scheme of the platform. He *et al.*[39] conducted a user study of 425 participants. They have determined the keywords of the access control that participants want, providing new ideas for the future redesign of access control and authentication of the IoT.

4.5 Voice Assistant Security

4.5.1 *Threats*

As a special component of the smart home platforms, voice assistants suffer more stealthy security threats due to their unique voice processing technology. First, as a typical threat to voice assistants, DolphinAttack[8], a completely inaudible attack, can be correctly parsed by the device's hardware without being noticed by the user's voice recognition systems. Similarly, Yuan *et al.*[9] proposed an attack to embed voice commands into songs, which sounds completely normal to ordinary users but will be well understood by the automatic speech recognition (ASR) software. Particularly, Yan *et al.*[40] studied the characteristics of different communication media and designed SurfingAttack, which extends the attack distance by utilizing the unique characteristics of acoustic transmission through solid materials.

Second, the natural language understanding (NLU) algorithms' recognition accuracy also affects speech recognition's security. For example, intent classifier[41] may have semantic misunderstandings when encountering some common grammatical errors. Voice Squatting Attack[5] takes advantage of the platform's longest match principle by naming a skill close to the user's needs, enabling the attacker to trigger the VPA to work without the user's knowledge.

4.5.2 *Mitigations*

First, existing solutions to resist inaudible attacks are mainly divided into two types, depending on whether they are based on hardware or software. From the hardware point of view, defense is mainly carried out through hardware designed to strengthen

the hardware to supplement the signals[8, 40]. However, Mao *et al.*[42] stated that changing the hardware design of all voice-activated devices developed by different manufacturers is impractical. Therefore, to prevent attackers from modulating voice commands on the ultrasonic carrier, they proposed a detection method based on signal processing and used an independent device. Software-based solutions generally work through algorithms to extract signal features for further analysis to determine the attack[8, 9, 40]. Meng *et al.*[43] proposed a wireless signal-based voice authentication system, which verifies the activity of voice commands by sensing the movement of lips, face, and tongue and reflecting it on the channel state information of the Wi-Fi signals.

Second, to avoid semantic misunderstanding, Zhang *et al.*[41] designed the LAPSUS language model to model incorrect voice commands to help the platform find malicious skills.

Summary. The current problems of speech assistants mainly lie in the accuracy of the speech recognition algorithm and NLU algorithms. However, in the current solutions, there are few improvements in the NLU algorithms, and further research is needed to ensure that the corresponding operations of the voice instructions can be correctly matched.

4.6 Privacy Protection

4.6.1 Threats

Smart home platforms have important privacy issues. To be specific, Bastys *et al.*[44] proved that common IoT application platforms, including IFTTT, Zapier, and Microsoft Flow, are vulnerable to malicious applications, which can leak user privacy, such as users' photos and locations.

Besides the common smart home cloud platforms, special systems such as voice assistants, which can provide users with specific services, will also pose privacy issues. For example, the user's voice may be recorded and uploaded to the cloud server. The user's voice information will also be disclosed if the cloud is attacked.

4.6.2 Mitigations

To alleviate the privacy problem of smart home platforms, Bastys *et al.*[44] provided FlowIT, a tool to track information flow and automatically check applications' security before they are published. Moreover, FlowFence[45] requires consumers to declare the expected data flow patterns and limits the flow when an undeclared pattern occurs. However, this scheme needs to reconstruct the automation application program, which is difficult to be applied in practice.

For special voice assistant privacy issues, MicShield[46] obfuscates the private voice to ensure that the voice is not leaked while the voice assistant can still work normally.

Summary. At present, the platform privacy protection solutions mainly use data flow tracking and encryption methods, but the application cost is high. Further improvement measures need to be designed in the future.

5 Device Security of Smart Home Systems

Various smart devices are used in smart home application scenarios built by end users. Attackers may exploit the smart devices' vulnerabilities to disclose the user's private information and living habits. Even directly affecting the physical environment of the user's home and threatening the user's safety or the safety of the property. After systematic research, we classify device security issues into six categories: device vulnerabilities, device sensor linkage issues, device side-channel issues, device authentication issues, device authorization issues, and device privacy issues.

5.1 Device Vulnerability Analysis

5.1.1 Threats

Device firmware is susceptible to various software errors (such as memory corruption vulnerabilities) and application logic defects (such as authentication bypass)[47]. Specifically, memory corruption vulnerabilities may directly cause the program to crash and execute the corresponding exception handler, and authentication bypass allows an attacker to control the victim's devices without the victim's knowledge, thus forming a botnet.

To illustrate, [3, 14, 15, 48] conduct comprehensive investigations on the Mirai botnet and its derivatives and find that the Mirai botnet behavior has worm characteristics. The authors[3, 14, 15, 48] pointed out that some large-scale smart device manufacturers have been found to use insecure default passwords and to lack adequate security design, which makes the smart devices vulnerable to attacks[3].

5.1.2 Mitigations

Currently, many researchers are focusing on mining security vulnerabilities in the firmware of smart home devices. Hence, we summarize and compare some firmware vulnerability mining methods in Table 2.

First, fuzzy testing is the most widely-used vulnerability mining technology. Chen *et al.*[49] first introduced FIRMADYNE's dynamic analysis technology, which uses software-based full-system simulation to perform analysis and identified 14 new device vulnerabilities. However, the full-system simulation consumes high computing resources. Therefore, Zheng *et al.*[50] proposed an enhanced process simulation Firm AFL grey box fuzzy platform combining full system simulation and user mode simulation to optimize FIRMDYNE's full system simulation performance bottleneck. The above traditional fuzzing typically generates inputs for fuzzing through binary analysis, while Redini *et al.*[52] proposed a new approach to generating fuzzing inputs for devices by analyzing companion applications.

Second, as the fuzzing test usually depends on the device hardware, applying it systematically to devices with different operating systems is not easy. Therefore, Shoshitaishvili *et al.*[47] proposed the binary analysis framework Firmalice, using the concepts of static program slicing, symbolic execution and input determinism to detect authentication bypass vulnerabilities in firmware. Firmalice can improve the scalability of vulnerability analysis, but it needs to provide manually obtained security policies for each device. Therefore, it is impossible to use it on research of large-scale devices.

Finally, to perform a wide range of device vulnerability analyses, Wang *et al.*[51] inferred the vulnerabilities of device reuse components by analyzing the mobile companion applications of smart home devices. Notably, their method does not require actual devices or firmware mirroring, and thus it can be used to perform large-scale device vulnerability analysis.

Summary. Most of the existing vulnerability mining research adopts a fuzzy testing method, which is difficult to be compatible with various devices. Few methods are widely applicable to all kinds of equipments, and innovative methods still need to be designed.

5.2 Device Sensor Linkage Analysis

5.2.1 Threats

The smart home systems realize interaction through the devices' event sensor information, and thus a device's one or more event sensors' failures or attacks can also trigger abnormal behaviors of the user's other devices[53].

5.2.2 Mitigations

First, researchers can analyze the different activation sequences of sensors when the device performs user tasks to implement the anomaly detection system. By illustration, Sikder *et al.*[54] targeted smart devices such as smartphones and smart-watches based on the Android system. They designed the 6thSense context-aware intrusion detection system, which utilizes the data changes of different sensor groups activated when the device performs different user tasks to determine whether the device's behavior contains malicious elements. Analogously, Cameranesi *et al.*[55] analyzed sensor data based on the sensor activation sequence and combined it with the process discovery technology to identify macro activities to describe user behavior patterns. Bianchi *et al.*[56] used deep learning technology to classify Wi-Fi wearable sensor data to infer user behaviors.

Furthermore, in order to deal with malicious device behaviors caused by sensor data errors, Birnbach *et al.*[53] developed Peeves, which uses common sensor collection data in the physical environment of smart homes to measure the impact of device operations on the physical environment and verify the authenticity of device events.

Summary. Currently, for the interaction security

Table 2. Comparison of Firmware Vulnerability Mining Methods

Literature	Vulnerability Type	Discovery Method	Dynamic/Static	Large-Scale	Analyzed Type
Firmalice[47]	Authentication bypass	Symbolic execution	Static	No	Binary
FIRMADYNE[49]	Software vulnerabilities	Fuzzing	Dynamic	Yes	Binary
FIRM-AFL[50]	Software vulnerabilities	Fuzzing	Dynamic	Yes	Binary
Wang *et al.*[51]	Software vulnerabilities	Program analysis	Static	Yes	App source code
Diane[52]	Software vulnerabilities	Fuzzing	Dynamic	Yes	App source code

between device sensors, researchers usually find exceptions based on the activation sequence of sensors. However, such schemes are only applicable to single-user device scenarios[54, 55]. In the future, it is necessary to expand anomaly detection in multi-user scenarios. In addition, there needs to be more research on the reliability of device sensor information in the future.

5.3 Device Side-Channel Attack

5.3.1 Threats

Smart devices are composed of various sensors, which gather information and generate electromagnetic radiation, physical information, communication traffic, and other side-channel characteristics during an operation. However, this side-channel information may be exploited by attackers to cause harm to users.

Firstly, attackers can use electromagnetic radiation to cheat smart device sensors. Tu *et al.*[16] used the rectification effect in the operational amplifier and the instrumentation amplifier to remotely control the temperature sensor readings, and then controlled the system or prevented the operations of the temperature alarm.

Secondly, attackers can also use smart device sensors to sense the physical information generated by user activities to gain access to user privacy information. For example, Liu *et al.*[17] used an accelerometer built into the smartwatch to capture hand movements and combined them with the sound signal collected by the smartphone microphone to infer the content entered by the user on the keyboard. Sami *et al.*[57] designed the LidarPhone eavesdropping system. The system senses the vibration signal of the user's household objects through the lidar sensor and recovers the sound traces that cause the object's vibration, eavesdropping on the private dialogue.

Summary. Because the side channel information is usually generated by the user or used to prompt the user, it is not easy to eliminate it. At present, there are few systematic defense schemes for side-channel attacks. In the future, we can further study the solutions or focus on improving users' security awareness when using devices.

5.4 Device Authentication

5.4.1 Threats

The smart home environment typically includes multiple family members and may also have visitors (e.g., babysitters, neighbors, relatives) who legitimately and temporarily use the devices. However, not all members should be allowed to configure devices arbitrarily. In addition, smart devices and users that communicate over unsecured Internet channels may suffer from various attacks, such as capturing attacks, imitating attacks, and so on.

5.4.2 Mitigations

Since smart home devices often lack the user interface of traditional devices (e.g., keyboards and monitors), they cannot use traditional authentication methods based on username and password. In addition, due to the limited cost and high diversity of smart devices, most smart devices do not integrate inertial sensors (such as hardware components, e.g., fingerprint scanners or NFC readers) that can be used for authentication, and thus they cannot implement a unified authentication scheme. To this end, researchers have proposed novel authentication schemes to identify device users, such as biometrics, key, and protocol authentication. Table 3 summarizes and compares the device authentication methods proposed in some research work.

- *Biometrics Authentication.* Some studies employ timestamp-based biometric authentication to address the physical resource constraints of device authentication. In 2019, Li *et al.* proposed an authentication scheme based on the device clock P2Auth[58]. Li *et al.*[58] authenticated by comparing the device with the sequence of descriptions of the user's physical actions perceived by the user's wristband. Their authentication method does not require retrofitting the device hardware and can be applied directly to a commercial off-the-shelf (COTS) device. In 2020, Li *et al.* again proposed the T2Pair[18] authentication scheme. They used the motion data captured by user wristband inertial measurement unit (IMU) to identify the device timestamp description of the significant points, encoding the interval between significant points for authentication. Another biometric authentication method is based on challenge-response, which can use gyroscope and accelerometer sensors to measure the user's response signals to the random vibrations when the smartwatch emits a vibration, and then generate a verification model to verify the user's identity[59].
- *Key Authentication.* In order to enable secure

Table 3. Comparison of Device Authentication (AuthN) Methods

Literature	Type	Method	Encryption	Resistant to Attacks
P2Auth[58]	Biometrics	Physical operation	-	Replay attack, imitation attack
T2Pair[18]	Biometrics	Physical operation	Diffie-Hellman encryption	Imitation attack, man-in-the-middle attack
Lee *et al.*[59]	Biometrics	Random vibrations	-	Not-in-wear attacks, impersonation attacks
Alam[60]	Key	Trusted registration agency	Bitwise XOR, symmetric key, one-way hash	Replay attack, desynchronization attack
Wazid *et al.*[61]	Key	Trusted registration agency	One-way hash, bitwise XOR, symmetric key	Imitation attacks, internal privilege attacks
Zhang *et al.*[62]	Key	Key agreement	Merkle puzzle	Brute force password cracking
HomeChain[63]	Key	Integrated blockchain	Public key encryption, symmetric encryption, group signature	Hijacking attacks, denial of service attacks
Huang *et al.*[64]	Key	Keyless authentication	Hash collision puzzle	Replay attacks, message forgery attacks, man-in-the-middle attacks

communication between users and smart devices under an unsecured channel, some researchers use key negotiation mechanisms when implementing authentication schemes. Based on the smart home software-defined network (SDN) centralized controller, Iqbal *et al.*[60] proposed a new privacy protection security architecture using heterogeneous, symmetrical keys, one-way hash, and other lightweight encryption original design authentication mechanisms. Their method protects against replay and de-synchronization attacks and features low computational costs for quick verification. A typical smart home scenario allows users to use gateway devices to communicate with smart home devices. Therefore, some research work achieves key agreement through a gateway. For example, Zhang *et al.*[62] proposed a hybrid key negotiation mechanism. They generated Merkle puzzle keys on the home gateway, extending the short random key generated by the device to a high-entropy encryption key. As a result, their work significantly reduced the time and computational overhead of key negotiation. Lin *et al.*[63] integrated blockchain into their design of a new security inter-certification system, which uses group signatures to authenticate anonymous users and message verification codes to authenticate home gateways. Moreover, Wazid *et al.*[61] proposed a remote user authentication mechanism that establishes a protected session between the user and the device over the gateway node.

- *Protocol Authentication.* Traditional key authentication schemes discussed above incur a large overhead of processing, memory, and communication. For example, lightweight encryption authentication protocols rely on trusted permissions to generate and manage keys when storing certificates. However, not all smart home devices have enough computing power to implement these scenarios. With this in mind, Neto *et al.*[65] used identity-based cryptography to distribute keys, used attribute-based cryptography to perform access control, and realized the whole life cycle of authentication and access control of a device. These keys are encrypted without certificates and do not incur additional overhead on a device. Last, Huang *et al.*[64] proposed a keyless authentication protocol. In their work, smart devices use command messages sent by gateways to generate puzzles and validate evidence to authenticate between gateways and smart home devices. However, command messages sent by the gateway in clear text can be easily read by an attacker.

Summary. Researchers have designed corresponding biometric authentication, key authentication, and protocol authentication schemes according to different characteristics of intelligent devices, and combined SDN, blockchain, and other emerging technologies in traditional authentication methods to optimize the performance of authentication. In the future, more specific types of smart devices must be provided with appropriate authentication.

5.5 Device Authorization

5.5.1 Threats

Different platforms have independently designed device management channels (DMCs). For the convenience of users, today's devices usually support multiple DMCs. However, DMCs with inconsistent security policies and controls may allow attackers to exploit one DMC to bypass the security policies of other DMCs, causing confusion in device management and allowing attackers to gain additional control[66].

5.5.2 Mitigations

To this end, Jia *et al.*[66] also built the first systematic and practical cross-DMC access control framework CGuard, which utilizes the device manufacturer's application logic layer (ALL) in the device to control the accessibility of each DMC.

Summary. Device authorization problems mainly occur in the cross-cloud platform scenario, and there needs to be more research on such problems. In the future, it is necessary to study the device management mode of the platform that supports the cross-cloud platform scenario and propose suitable solutions.

5.6 Device Privacy Protection

5.6.1 Threats

Firstly, the smart devices themselves may have some privacy risks. For example, surveillance cameras directly monitor all aspects of a user's life. If a data leak occurs, the user may be blackmailed or burglarized.

Secondly, if there is information leakage or unauthorized access to a gateway device, the information of all devices connected to the gateway will be threatened, causing greater security and privacy issues.

5.6.2 Mitigations

First, the research work of both Yu *et al.*[67] and Fang *et al.*[68] concerned the data security of specific surveillance camera devices. Pinto[67] uses hash pixilation for real-time signatures, which can protect visual privacy and video authenticity without affecting video clarity. For a wider range of smart devices, Javaid *et al.*[69] established a BlockPro network model based on the blockchain, using physical unclonable functions (PUFs) and Ethereum to provide data sources and ensure data integrity.

Second, to enhance the privacy protection of gateway devices, Lee *et al.*[70] designed an operating system called S2Net, which can distinguish and manage multiple sessions belonging to different users. Consequently, S2Net improves throughput performance while reducing the overhead of implementing encryption tasks. However, it has limited program functions and only supports coarse-grained access control.

Summary. Because various devices have different features and functions, the solutions to privacy problems of various devices are different. We also need to investigate special devices' characteristics and corresponding design solutions. For example, gateway devices also need more fine-grained privacy protection solutions.

6 Communication Security of Smart Home Systems

Communication is an important part of a smart home architecture, completing data exchange and information transfer among devices, platforms, and users. Each protocol has its specific functions. For example, protocols such as Zigbee, Bluetooth Low Energy (BLE), and BlueTooth (BT) mainly solve the problem of device interconnection and network access, and the MQTT protocol mainly solves the problem of data exchange between applications. However, some design flaws in these protocols will pose a threat to users[21–23, 25, 71]. Therefore, much research focuses on the protocol's vulnerability to help further optimize the protocol, strengthen communication security, and protect users from attacks.

6.1 Protocol Vulnerability

6.1.1 Threats

First, we focus on the security issues caused by design flaws in smart home communication protocols (including Zigbee, BLE, BT, Wi-Fi, and MQTT).

- *Vulnerabilities of Zigbee.* Based on Philips Hue smart lamps, Ronen *et al.*[21] discovered that developers protect firmware updates by sharing an easy-to-crack symmetric encryption key across multiple devices. Therefore, they simply used its built-in Zigbee wireless connection to launch worm attacks.
- *Vulnerabilities of BLE.* Zuo *et al.*[22] discovered that UUID could be obtained from broadcast packets sent by smart devices to applications. With UUID, applications could identify and bind BLE devices to allow further data communication. They further revealed that attackers could exploit many vulnerable applications and devices connected to BLE. In addition, Zhang *et al.*[71] discovered that BLE does not require the boot device to use secure connections only (SCO) mode, which makes all BLE applications vulnerable to degrade attacks. At the same time, if the BLE programming framework of the initiator does not implement the SCO mode correctly, an attacker could create a fake BLE device to carry out an at-

tack.

• *Vulnerabilities of BT.* Since BT addresses are fixed, attackers can infer device addresses and track users[23] by collecting traffic from BT channels through signal processing and iterative reasoning.

• *Vulnerabilities of Wi-Fi.* The radio frequency signals emitted by Wi-Fi devices are everywhere and easy to obtain, which may constitute a severe privacy security problem. For instance, Zhu *et al.*[24] found that attackers could track users' movements and activity information in buildings through existing Wi-Fi signals, which may reveal users' behavior patterns and physiological characteristics, and if used for malicious purposes, may present huge risks.

• *Vulnerabilities of MQTT.* Since there are few built-in authentication and authorization mechanisms in MQTT, and the smart home scenarios are complex, it is difficult for cloud platform providers to provide customized protection measures. For example, Jia *et al.*[25] focused on the security issues of smart home clouds that use the MQTT protocol. More specifically, the paper points out that malicious former users can retain control over devices whose access rights have expired, secretly issue commands when the smart devices serve other users, and take advantage of MQTT protocol vulnerabilities to control the victim's devices, infer user behavior patterns, and connect to the cloud platform via any ClientId to launch a DoS attack.

6.1.2 *Mitigations*

It can be seen from the research on protocols referenced above that there is currently no unified standard for smart home device communication. Therefore, if the implementation process of the protocols themselves has design flaws or problems, users will be exposed to great danger. The security problems of the protocols need to be solved urgently using two approaches. On the one hand, optimizing the protocols' designs and standardizing the protocols' use to reduce security vulnerabilities are necessary. On the other hand, the security and the availability of protocols need to be balanced to reduce security threats to users when security vulnerabilities cannot be completely eliminated.

• *Mitigation of Vulnerabilities.* As mentioned earlier, communication protocols have security vulnerabilities, and researchers have put forward solutions to these issues[72]. First, it is possible to reduce the generation of security threats by standardizing protocol standards and application processes. For Zigbee, the encryption method of firmware updates in the device should be examined and improved[21]. In view of the authentication flaw of BLE, programmers should implement a secure encryption function to reinforce the credentials in the app. In addition, Zhang *et al.*[71] argued that, in the process of applying BLE, both the initiator and peer devices should have the option of SCO mode so that mutual authentication between them can be realized. Furthermore, the privacy leakage caused by BT requires new revisions to the BlueTooth standard to maintain the anonymity of BT devices[23]. Additionally, there is a method based on the Wi-Fi access point (AP) to inject traffic to obfuscate and prevent attackers from tracking human movements from the Wi-Fi signals[24]. Finally, to address the problem of MQTT, Jia *et al.*[25] introduced new design principles and an access model for MQTT that allows for more fine-grained checking of access rights.

• *New Design Related to Communication.* Beyond the mitigation of vulnerabilities mentioned above, some new ideas based on existing protocols have been proposed recently[73–75]. First, there are some designs related to encryption. Zhang *et al.*[76] specifically designed a method for smart home systems to establish secret keys without preloading the secrets of the third party. Sciancalepore *et al.*[77] optimized several schemes and proposed a new key management protocol (KMP) that can guarantee a greater degree of communication security. Finally, SecureIoT[78] implements a security solution suitable for IoT networks based on service-oriented architecture (SOA) to pair and transmit data.

Second, some of the work relates to communication patterns. Borgia *et al.*[79] proposed MobCCN, a content-centric rather than device-centric protocol, with the main focus on supporting data access near the physical location of data generation.

Summary. Smart home systems use a variety of protocols to achieve interactions. According to the different characteristics of each protocol, researchers have designed their own security solutions for each protocol. However, it is a new direction to design new and more applicable protocols according to smart home system communication requirements.

6.2 Communication Flow Analysis

6.2.1 *Threats*

During the operation of smart home devices, net-

work traffic that contains information related to the devices, users, applications, or the traffic itself will be generated. The question of how to analyze this communication traffic is another key area in the study of smart home security. By analyzing the traffic between devices, platforms, and user interactions, attackers can understand the relationship between traffic characteristics and device behaviors, resulting in privacy leakage.

For example, for the communication traffic generated by smart devices, Beyer *et al.*[80] found that attackers can use communication traffic to classify devices from smart home systems in order to identify devices in the user's home, infer user behaviors, and even gain physical access to the home. Similarly, Trimananda *et al.*[19] proposed a tool that can automatically extract the packet-level signature of device events from network traffic, which is more effective and convenient than previous statistically-based methods. Moreover, more detailed information, such as the type of events, can be inferred from the extracted traffic. In addition, Yu *et al.*[20] extracted network traffic characteristics from broadcast and multicast packets and proposed a deep learning model to identify devices.

Summary. The research on communication traffic protection in smart home systems is still in its infancy, and there are relatively few related studies. We look forward to more security research related to communication traffic that may bring more unexpected insights.

7 Discussion

7.1 Root Causes

The reasons for the risks in current smart home systems are numerous and varied. We summarize the root causes of the risks as follows.

Heterogeneity. The heterogeneous nature of smart home systems makes it challenging to secure the whole system with a single solution. The heterogeneity comes from many different levels and layers—various communication protocols (e.g., Wi-Fi, BlueTooth, Zigbee, and Z-wave), device control methods (e.g., commands originated from clouds, mobile apps, third-party cloud, and automation rules), application layer protocols (e.g., MQTT, OAuth, and HTTP(S)), authentication mechanisms (e.g., signature, certificate, and password), access control mechanisms (e.g., ACL, white-list, role-based, and token-based) and different delegations (e.g., user-to-user, user-to-cloud, and cloud-to-cloud). To make it worse, different platforms often choose different schemes to implement their unique systems. As a result, real-world users' smart home systems are highly heterogeneous and complex, for they involve multiple devices, protocols, and platforms from different vendors or organizations. Hence, any susceptibility in a single point of the system will threaten the security of the whole system.

Customization. Current smart home systems apply many protocols or schemes customized from existing or legacy protocols or schemes that were not designed for smart home systems. For example, the Actions on Google protocol is a customized OAuth protocol by Google[10] that requires the delegator cloud to send device information (e.g., device ID or device type) to Google Home along with an OAuth token. Such customization usually has not undergone rigorous security analysis and sufficient user/market inspections. Therefore, customized protocols or schemes have become a source of hazards in smart home systems.

Unclear Boundaries of Responsibility. Many different parties are involved in a user's smart home system, including the end user, the manufacturer(s), the cloud service provider(s), and the design/management organizations of the protocols. These parties interact with each other, each providing certain functionalities to make the whole system work. However, the responsibility each party should bear is unclear. For instance, in Apple's HomeKit system, end users are responsible for preventing the setup codes of the HomeKit accessories from being disclosed. In the meantime, Apple asks the Homekit accessory manufacturers to safely manage the `AAD` (additional authorization data). Such unclear boundaries of responsibility make it quite challenging to design a secure system in practice.

Absence of Standardization. In the rapidly growing area of smart home technology, new designs and practices are emerging daily. However, the standardization of the implementation and enforcement of security for smart home systems is absent. Consequently, there is no guarantee that a new mechanism will not inadvertently introduce new security flaws, espe-

[10] Actions on Google. https://developers.google.com/assistant/smarthome/develop/process-intents, Mar. 2023.

cially when the newly released platform interacts with existing platforms. To be more specific, if a new service provider (e.g., the owner of a new platform) does not fully understand the security assumption and policy of an existing platform A, the interactions between the new platform and platform A will introduce new security risks. We believe the absence of standardization is one of the major root causes of the vulnerability of today's smart home systems.

7.2 Future Research Directions

Toward more secure smart home systems, we summarize the following research directions based on our understanding of the work reviewed in Sections 3–6, including automated vulnerability discovery, vigorous security checking and data-driven analysis.

Automated Vulnerability Discovery. Recent research has identified many new vulnerabilities in smart home systems[11, 44, 45, 47]. In Subsection 5.1.1, we discuss vulnerability discovery methods in smart home devices, and in Subsection 4.2.2, we discuss solutions to linkage problems related to smart home platforms. We find that because the problems of devices and platforms involve their underlying undisclosed designs, and devices and platforms are mostly heterogeneous, most solutions adopt manual or semi-automatic designs in order to discover specific vulnerabilities of different devices or platforms. For example, some methods require humans to input specific security rules into the tool[11, 47], and some methods require building a model to describe the investigated smart home system[32, 44]. Given the time cost and human effort, a more efficient and promising approach would be to discover the vulnerabilities in a fully automated way. This may require abstracting solutions independent of a specific device or platform architecture for wider applications.

Vigorous Security Checking. Due to the parties that make up a smart home system do not have uniform standards and clear boundaries of responsibility, smart home systems require stricter security reviews. Hence, developing a way to perform a vigorous check and comprehensive analysis of a system is very important. Potential techniques that can be used here include formal verification, fuzzing, and differential testing. In our discussion in Subsection 5.1.1, we find that many vulnerability mining methods use fuzzing, which can be further optimized. In addition, in Subsection 4.2.2 we mention that there is work to model the IoT ecosystem as an FSM for model checking, and it has achieved better results. However, this formal verification method is rarely used in the current research work, and it needs to be further studied and used in the future.

Data-Driven Analysis. Smart home systems generate a great account of data, including the system log, device status, environment data collected by sensors, and traffic among the components. There is a huge amount of valuable information in the data. Like our discussion in Subsection 5.2.2, the anomaly detection based on device sensor behavior is mainly driven by sensor data. Similarly, we discuss the communication traffic data-driven vulnerability discovery in Subsection 6.2, but this kind of research is little and needs further supplementation and improvement. Hence, data-driven analyses, such as root cause analysis of malicious events in the systems, are also important to enhance the security of smart home systems.

8 Conclusions

We conducted a comprehensive review of security research on smart home systems, dividing security issues into three areas: platform security, device security, and communication security. Then we summarized that the root causes for the security flaws of the current smart home systems are the combination of heterogeneous components within the systems, the specially customized protocols and solutions for different platforms, the lack of clear responsibility boundaries for each part of the systems, and the lack of uniform standards. Toward more secure smart home systems, we also discussed future research directions, such as the development of automated vulnerability mining tools, more stringent security checks on smart home systems, and security analysis through the generated data of smart home systems, which will help to better study the security of smart home systems and provide a more powerful security guarantee for smart home systems.

References

[1] Kumar P, Braeken A, Gurtov A, Iinatti J, Ha P H. Anonymous secure framework in connected smart home environments. *IEEE Transactions on Information Forensics and Security*, 2017, 12(4): 968–979. DOI: 10.1109/TIFS.2016.2647225.

[2] Stanislav M, Beardsley T. HACKING IoT: A case study on baby monitor exposures and vulnerabilities. Rapid7,

2015. https://www.rapid7.com/globalassets/external/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf, Mar. 2023.

[3] Antonakakis M, April T, Bailey M, Bernhard M, Bursztein E, Cochran J, Durumeric Z, Halderman J A, Invernizzi L, Kallitsis M, Kumar D, Lever C, Ma Z E, Mason J, Menscher D, Seaman C, Sullivan N, Thomas K, Zhou Y. Understanding the Mirai botnet. In *Proc. the 26th USENIX Conference on Security Symposium*, Aug. 2017, pp.1093–1110.

[4] Fernandes E, Jung J, Prakash A. Security analysis of emerging smart home applications. In *Proc. the 2016 IEEE Symposium on Security and Privacy*, May 2016, pp.636–654. DOI: 10.1109/SP.2016.44.

[5] Zhang N, Mi X H, Feng X, Wang X F, Tian Y, Qian F. Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems. In *Proc. the 2019 IEEE Symposium on Security and Privacy*, May 2019, pp.1381–1396. DOI: 10.1109/SP.2019.00016.

[6] Dong Y D, Yao Y D. Secure mmWave-radar-based speaker verification for IoT smart home. *IEEE Internet of Things Journal*, 2021, 8(5): 3500–3511. DOI: 10.1109/JIOT.2020.3023101.

[7] Xiao Y H, Jia Y Z, Liu C C, Alrawais A, Rekik M, Shan Z G. HomeShield: A credential-less authentication framework for smart home systems. *IEEE Internet of Things Journal*, 2020, 7(9): 7903–7918. DOI: 10.1109/JIOT.2020.3003621.

[8] Zhang G M, Yan C, Ji X Y, Zhang T C, Zhang T M, Xu W Y. DolphinAttack: Inaudible voice commands. In *Proc. the 2017 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2017, pp.103–117. DOI: 10.1145/3133956.3134052.

[9] Yuan X J, Chen Y X, Zhao Y, Long Y H, Liu X K, Chen K, Zhang S Z, Huang H Q, Wang X F, Gunter C A. CommanderSong: A systematic approach for practical adversarial voice recognition. In *Proc. the 27th USENIX Conference on Security Symposium*, Aug. 2018, pp.49–64.

[10] Mi X H, Qian F, Zhang Y, Wang X F. An empirical characterization of IFTTT: Ecosystem, usage, and performance. In *Proc. the 2017 Internet Measurement Conference*, Nov. 2017, pp.398–404. DOI: 10.1145/3131365.3131369.

[11] Wang Q, Datta P, Yang W, Liu S, Bates A, Gunter C A. Charting the attack surface of trigger-action IoT platforms. In *Proc. the 2019 ACM SIGSAC Conference on Computer and Communications Security*, Nov. 2019, pp.1439–1453. DOI: 10.1145/3319535.3345662.

[12] Xiao D, Wang Q Y, Cai M, Zhu Z H, Zhao W M. A3ID: An automatic and interpretable implicit interference detection method for smart home via knowledge graph. *IEEE Internet of Things Journal*, 2020, 7(3): 2197–2211. DOI: 10.1109/JIOT.2019.2959063.

[13] Ding W B, Hu H X. On the safety of IoT device physical interaction control. In *Proc. the 2018 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2018, pp.832–846. DOI: 10.1145/3243734.3243865.

[14] Griffioen H, Doerr C. Examining Mirai's battle over the Internet of Things. In *Proc. the 2020 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2020, pp.743–756. DOI: 10.1145/3372297.3417277.

[15] Kumar D, Shen K, Case B, Garg D, Alperovich G, Kuznetsov D, Gupta R, Durumeric Z. All things considered: An analysis of IoT devices on home networks. In *Proc. the 28th USENIX Conference on Security Symposium*, Aug. 2019, pp.1169–1185.

[16] Tu Y Z, Rampazzi S, Hao B, Rodriguez A, Fu K, Hei X L. Trick or heat?: Manipulating critical temperature-based control systems using rectification attacks. In *Proc. the 2019 ACM SIGSAC Conference on Computer and Communications Security*, Nov. 2019, pp.2301–2315. DOI: 10.1145/3319535.3354195.

[17] Liu X Y, Zhou Z, Diao W R, Li Z, Zhang K H. When good becomes evil: Keystroke inference with smartwatch. In *Proc. the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2015, pp.1273–1285. DOI: 10.1145/2810103.2813668.

[18] Li X P, Zeng Q, Luo L N, Luo T B. T2Pair: Secure and usable pairing for heterogeneous IoT devices. In *Proc. the 2020 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2020, pp.309–323. DOI: 10.1145/3372297.3417286.

[19] Trimananda R, Varmarken J, Markopoulou A, Demsky B. Packet-level signatures for smart home devices. In *Proc. the 27th Annual Network and Distributed System Security Symposium*, Feb. 2020.

[20] Yu L J, Luo B, Ma J, Zhou Z Y, Liu Q Y. You are what you broadcast: Identification of mobile and IoT devices from (public) WiFi. In *Proc. the 29th USENIX Security Symposium*, Aug. 2020, pp.55–72.

[21] Ronen E, Shamir A, Weingarten A O, O'Flynn C. IoT goes nuclear: Creating a ZigBee chain reaction. In *Proc. the 2017 IEEE Symposium on Security and Privacy*, May 2017, pp.195–212. DOI: 10.1109/SP.2017.14.

[22] Zuo C S, Wen H H, Lin Z Q, Zhang Y Q. Automatic fingerprinting of vulnerable BLE IoT devices with static UUIDs from mobile apps. In *Proc. the 2019 ACM SIGSAC Conference on Computer and Communications Security*, Nov. 2019, pp.1469–1483. DOI: 10.1145/3319535.3354240.

[23] Cominelli M, Gringoli F, Patras P, Lind M, Noubir G. Even black cats cannot stay hidden in the dark: Full-band de-anonymization of bluetooth classic devices. In *Proc. the 2020 IEEE Symposium on Security and Privacy*, May 2020, pp.534–548. DOI: 10.1109/SP40000.2020.00091.

[24] Zhu Y Z, Xiao Z J, Chen Y X, Li Z J, Liu M, Zhao B Y, Zheng H. Et Tu Alexa? When commodity WiFi devices turn into adversarial motion sensors. In *Proc. the 27th Annual Network and Distributed System Security Symposium*, Feb. 2020.

[25] Jia Y, Xing L Y, Mao Y H, Zhao D F, Wang X F, Zhao S R, Zhang Y Q. Burglars' IoT paradise: Understanding and mitigating security risks of general messaging protocols on IoT clouds. In *Proc. the 2020 IEEE Symposium on Security and Privacy*, May 2020, pp.465–481. DOI:

10.1109/SP40000.2020.00051.

[26] Cheng L, Wilson C, Liao S, Young J, Dong D, Hu H X. Dangerous skills got certified: Measuring the trustworthiness of skill certification in voice personal assistant platforms. In *Proc. the 2020 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2020, pp.1699–1716. DOI: 10.1145/3372297.3423339.

[27] Antonioli D, Tippenhauer N O, Rasmussen K B. Nearby threats: Reversing, analyzing, and attacking Google's 'nearby connections' on Android. In *Proc. the 26th Annual Network and Distributed System Security Symposium*, Feb. 2019.

[28] Zhang W, Meng Y, Liu Y G, Zhang X K, Zhang Y Q, Zhu H J. HoMonit: Monitoring smart home apps from encrypted traffic. In *Proc. the 2018 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2018, pp.1074–1088. DOI: 10.1145/3243734.3243820.

[29] Celik Z B, Tan G, McDaniel P D. IoTGuard: Dynamic enforcement of security and safety policy in commodity IoT. In *Proc. the 26th Annual Network and Distributed System Security Symposium*, Feb. 2019.

[30] Ding W B, Hu H X, Cheng L. IoTSafe: Enforcing safety and security policy with real IoT physical interaction discovery. In *Proc. the 28th Annual Network and Distributed System Security Symposium*, Feb. 2021.

[31] Liu R J, Wang Z Q, Garcia L, Srivastava M B. RemedioT: Remedial actions for Internet-of-Things conflicts. In *Proc. the 6th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation*, Nov. 2019, pp.101–110. DOI: 10.1145/3360322.3360837.

[32] Hsu K H, Chiang Y H, Hsiao H C. SafeChain: Securing trigger-action programming from attack chains. *IEEE Transactions on Information Forensics and Security*, 2019, 14(10): 2607–2622. DOI: 10.1109/TIFS.2019.2899758.

[33] Yuan B, Jia Y, Xing L Y, Zhao D F, Wang X F, Zou D Q, Jin H, Zhang Y Q. Shattered chain of trust: Understanding security risks in cross-cloud IoT access delegation. In *Proc. the 29th USENIX Conference on Security Symposium*, Aug. 2020, Article No. 67.

[34] Schuster R, Shmatikov V, Tromer E. Situational access control in the Internet of Things. In *Proc. the 2018 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2018, pp.1056–1073. DOI: 10.1145/3243734.3243817.

[35] Tian Y, Zhang N, Lin Y H, Wang X F, Ur B, Guo X Z, Tague P. SmartAuth: User-centered authorization for the Internet of Things. In *Proc. the 26th USENIX Conference on Security Symposium*, Aug. 2017, pp.361–378.

[36] Jia Y J, Chen Q A, Wang S Q, Rahmati A, Fernandes E, Mao Z M, Prakash A, Unviersity S J. ContexIoT: Towards providing contextual integrity to appified IoT platforms. In *Proc. the 24th Annual Network and Distributed System Security Symposium*, Feb. 2017.

[37] Ghosh N, Chandra S, Sachidananda V, Elovici Y. SoftAuthZ: A context-aware, behavior-based authorization framework for home IoT. *IEEE Internet of Things Journal*, 2019, 6(6): 10773–10785. DOI: 10.1109/JIOT.2019.2941767.

[38] Fernandes E, Rahmati A, Jung J, Prakash A. Decentralized action integrity for trigger-action IoT platforms. In *Proc. the 25th Annual Network and Distributed System Security Symposium*, Feb. 2018.

[39] He W J, Golla M, Padhi R, Ofek J, Dürmuth M, Fernandes E, Ur B. Rethinking access control and authentication for the home Internet of Things (IoT). In *Proc. the 27th USENIX Conference on Security Symposium*, Aug. 2018, pp.255–272.

[40] Yan Q B, Liu K H, Zhou Q, Guo H Q, Zhang N. SurfingAttack: Interactive hidden attack on voice assistants using ultrasonic guided waves. In *Proc. the 27th Annual Network and Distributed System Security Symposium*, Feb. 2020.

[41] Zhang Y Y, Xu L, Mendoza A, Yang G L, Chinprutthiwong P, Gu G F. Life after speech recognition: Fuzzing semantic misinterpretation for voice assistant applications. In *Proc. the 26th Annual Network and Distributed System Security Symposium*, Feb. 2019.

[42] Mao J, Zhu S S, Dai X, Lin Q X, Liu J W. Watchdog: Detecting ultrasonic-based inaudible voice attacks to smart home systems. *IEEE Internet of Things Journal*, 2020, 7(9): 8025–8035. DOI: 10.1109/JIOT.2020.2997779.

[43] Meng Y, Zhu H J, Li J L, Li J, Liu Y. Liveness detection for voice user interface via wireless signals in IoT environment. *IEEE Transactions on Dependable and Secure Computing*, 2021, 18(6): 2996–3011. DOI: 10.1109/TDSC.2020.2973620.

[44] Bastys I, Balliu M, Sabelfeld A. If this then what?: Controlling flows in IoT apps. In *Proc. the 2018 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2018, pp.1102–1119. DOI: 10.1145/3243734.3243841.

[45] Fernandes E, Paupore J, Rahmati A, Simionato D, Conti M, Prakash A. FlowFence: Practical data protection for emerging IoT application frameworks. In *Proc. the 25th USENIX Security Symposium*, Aug. 2016, pp.531–548.

[46] Sun K, Chen C, Zhang X Y. "Alexa, stop spying on me!": Speech privacy protection against voice assistants. In *Proc. the 18th Conference on Embedded Networked Sensor Systems*, Nov. 2020, pp.298–311. DOI: 10.1145/3384419.3430727.

[47] Shoshitaishvili Y, Wang R Y, Hauser C, Kruegel C, Vigna G. Firmalice-automatic detection of authentication bypass vulnerabilities in binary firmware. In *Proc. the 22nd Annual Network and Distributed System Security Symposium*, Feb. 2015.

[48] Alrawi O, Lever C, Valakuzhy K, Court R, Snow K Z, Monrose F, Antonakakis M. The circle of life: A large-scale study of the IoT malware lifecycle. In *Proc. the 30th USENIX Security Symposium*, Aug. 2021, pp.3505–3522.

[49] Chen D D, Woo M, Brumley D, Egele M. Towards automated dynamic analysis for Linux-based embedded firmware. In *Proc. the 23rd Annual Network and Distributed System Security Symposium*, Feb. 2016.

[50] Zheng Y W, Davanian A, Yin H, Song C Y, Zhu H S, Sun L M. FIRM-AFL: High-throughput greybox fuzzing of IoT firmware via augmented process emulation. In

Proc. the 28th USENIX Conference on Security Symposium, Aug. 2019, pp.1099–1114.

[51] Wang X Q, Sun Y Q, Nanda S, Wang X F. Looking from the mirror: Evaluating IoT device security through mobile companion apps. In *Proc. the 28th USENIX Conference on Security Symposium*, Aug. 2019, pp.1151–1167.

[52] Redini N, Continella A, Das D, de Pasquale G, Spahn N, Machiry A, Bianchi A, Kruegel C, Vigna G. Diane: Identifying fuzzing triggers in apps to generate under-constrained inputs for IoT devices. In *Proc. the 2021 IEEE Symposium on Security and Privacy*, May 2021, pp.484–500. DOI: 10.1109/SP40001.2021.00066.

[53] Birnbach S, Eberz S, Martinovic I. Peeves: Physical event verification in smart homes. In *Proc. the 2019 ACM SIGSAC Conference on Computer and Communications Security*, Nov. 2019, pp.1455–1467. DOI: 10.1145/3319535.3354254.

[54] Sikder A K, Aksu H, Uluagac A S. 6thSense: A context-aware sensor-based attack detector for smart devices. In *Proc. the 26th USENIX Security Symposium*, Aug. 2017, pp.397–414.

[55] Cameranesi M, Diamantini C, Mircoli A, Potena D, Storti E. Extraction of user daily behavior from home sensors through process discovery. *IEEE Internet of Things Journal*, 2020, 7(9): 8440–8450. DOI: 10.1109/JIOT.2020.2990537.

[56] Bianchi V, Bassoli M, Lombardo G, Fornacciari P, Mordonini M, de Munari I. IoT wearable sensor and deep learning: An integrated approach for personalized human activity recognition in a smart home environment. *IEEE Internet of Things Journal*, 2019, 6(5): 8553–8562. DOI: 10.1109/JIOT.2019.2920283.

[57] Sami S, Dai Y M, Tan S R X, Roy N, Han J. Spying with your robot vacuum cleaner: Eavesdropping via lidar sensors. In *Proc. the 18th Conference on Embedded Networked Sensor Systems*, Nov. 2020, pp.354–367. DOI: 10.1145/3384419.3430781.

[58] Li X P, Yan F Y, Zuo F, Zeng Q, Luo L N. Touch well before use: Intuitive and secure authentication for IoT devices. In *Proc. the 25th Annual International Conference on Mobile Computing and Networking*, Aug. 2019, Article No. 33. DOI: 10.1145/3300061.3345434.

[59] Lee S, Choi W, Lee D H. Usable user authentication on a smartwatch using vibration. In *Proc. the 2021 ACM SIGSAC Conference on Computer and Communications Security*, Nov. 2021, pp.304–319. DOI: 10.1145/3460120.3484553.

[60] Iqbal W, Abbas H, Deng P, Wan J F, Rauf B, Abbas Y, Rashid I. ALAM: Anonymous lightweight authentication mechanism for SDN-enabled smart homes. *IEEE Internet of Things Journal*, 2021, 8(12): 9622–9633. DOI: 10.1109/JIOT.2020.3024058.

[61] Wazid M, Das A K, Odelu V, Kumar N, Susilo W. Secure remote user authenticated key establishment protocol for smart home environment. *IEEE Transactions on Dependable and Secure Computing*, 2020, 17(2): 391–406. DOI: 10.1109/TDSC.2017.2764083.

[62] Zhang Y X, Huang X Y, Chen X F, Zhang L Y, Zhang J, Xiang Y. A hybrid key agreement scheme for smart homes using the Merkle puzzle. *IEEE Internet of Things Journal*, 2020, 7(2): 1061–1071. DOI: 10.1109/JIOT.2019.2949407.

[63] Lin C, He D B, Kumar N, Huang X Y, Vijayakumar P, Choo K R. HomeChain: A blockchain-based secure mutual authentication system for smart homes. *IEEE Internet of Things Journal*, 2020, 7(2): 818–829. DOI: 10.1109/JIOT.2019.2944400.

[64] Huang Z G, Zhang L, Meng X Y, Choo K R. Key-free authentication protocol against subverted indoor smart devices for smart home. *IEEE Internet of Things Journal*, 2020, 7(2): 1039–1047. DOI: 10.1109/JIOT.2019.2948622.

[65] Neto A L M, Souza A L F, Cunha I *et al.* AoT: Authentication and access control for the entire IoT device life-cycle. In *Proc. the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, Nov. 2016. DOI: 10.1145/2994551.2994555.

[66] Jia Y, Yuan B, Xing L Y *et al.* Who's in control? On security risks of disjointed IoT device management channels. In *Proc. the 2021 ACM SIGSAC Conference on Computer and Communications Security*, Nov. 2021, pp.1289–1305. DOI: 10.1145/3460120.3484592.

[67] Yu H, Lim J, Kim K, Lee S B. Pinto: Enabling video privacy for commodity IoT cameras. In *Proc. the 2018 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2018, pp.1089–1101. DOI: 10.1145/3243734.3243830.

[68] Fang L, Wu Y, Wu C, Yu Y Z. A nonintrusive elderly home monitoring system. *IEEE Internet of Things Journal*, 2021, 8(4): 2603–2614. DOI: 10.1109/JIOT.2020.3019270.

[69] Javaid U, Aman M N, Sikdar B. BlockPro: Blockchain based data provenance and integrity for secure IoT environments. In *Proc. the 1st Workshop on Blockchain-Enabled Networked Sensor Systems*, Nov. 2018, pp.13–18. DOI: 10.1145/3282278.3282281.

[70] Lee S S, Shi H, Tan K, Liu Y X, Lee S K, Cui Y. S2Net: Preserving privacy in smart home routers. *IEEE Transactions on Dependable and Secure Computing*, 2021, 18(3): 1409–1424. DOI: 10.1109/TDSC.2019.2924624.

[71] Zhang Y, Weng J, Dey R, Jin Y E, Lin Z Q, Fu X W. Breaking secure pairing of Bluetooth low energy using downgrade attacks. In *Proc. the 29th USENIX Security Symposium*, Aug. 2020, pp.37–54.

[72] Lei X Y, Tu G H, Li C Y, Xie T, Zhang M. SecWIR: Securing smart home IoT communications via Wi-Fi routers with embedded intelligence. In *Proc. the 18th Int. Con. Mobile Systems, Applications, and Services*, Jun. 2020, pp.260–272. DOI: 10.1145/3386901.3388941.

[73] Brunisholz P, Rousseau F, Duda A. DataTweet for user-centric and geo-centric IoT communications. In *Proc. the 2nd Workshop on Experiences in the Design and Implementation of Smart Objects*, Oct. 2016, pp.29–34. DOI: 10.1145/2980147.2980152.

[74] Wilson J, Wahby R S, Corrigan-Gibbs H, Boneh D, Levis P A, Winstein K. Trust but verify: Auditing the secure Internet of Things. In *Proc. the 15th Annual Int. Con.*

Mobile Systems, Applications, and Services, Jun. 2017, pp.464–474. DOI: 10.1145/3081333.3081342.

[75] Luo Z Q, Wang W, Qu J, Jiang T, Zhang Q. ShieldScatter: Improving IoT security with backscatter assistance. In *Proc. the 16th ACM Conference on Embedded Networked Sensor Systems*, 2018, pp.185–198. DOI: 10.1145/3274783.3274841.

[76] Zhang Y X, Zhao H, Xiang Y, Huang X Y, Chen X F. A key agreement scheme for smart homes using the secret mismatch problem. *IEEE Internet of Things Journal*, 2019, 6(6): 10251–10260. DOI: 10.1109/JIOT.2019.2936884.

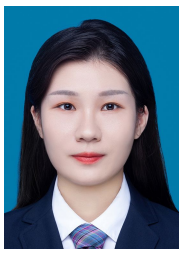
[77] Sciancalepore S, Capossele A, Piro G, Boggia G, Bianchi G. Key management protocol with implicit certificates for IoT systems. In *Proc. the 2015 Workshop on IoT challenges in Mobile and Industrial Systems*, May 2015, pp.37–42. DOI: 10.1145/2753476.2753477.

[78] Kar P, Misra S, Mandal A K, Wang H. SecureioT: Hop-count based service-oriented efficient security solution for IoT. In *Proc. the 1st International Workshop on Future Industrial Communication Networks*, Oct. 2018, pp.15–20. DOI: 10.1145/3243318.3243323.

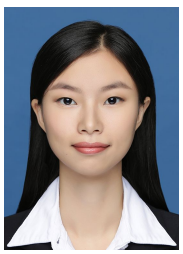
[79] Borgia E, Bruno R, Passarella A. MobCCN: A CCN-compliant protocol for data collection with opportunistic contacts in IoT environments. In *Proc. the 11th ACM Workshop on Challenged Networks*, Oct. 2016, pp.63–68. DOI: 10.1145/2979683.2979695.

[80] Beyer S M, Mullins B E, Graham S R, Bindewald J M. Pattern-of-life modeling in smart homes. *IEEE Internet of Things Journal*, 2018, 5(6): 5317–5325. DOI: 10.1109/JIOT.2018.2840451.

Bin Yuan is currently an associate professor at Huazhong University of Science and Technology (HUST), Wuhan. Bin received his B.S. and Ph.D. degrees in computer science and technology from HUST, Wuhan, in 2013 and 2018, respectively. His research interests include software-defined network security, network function virtualization, cloud security, privacy and IoT security. He has published several technical papers in top conferences/journals, such as USENIX Security, IEEE TSC, IEEE TNSM, IEEE TNSE, IEEE IoT Journal and FGCS.

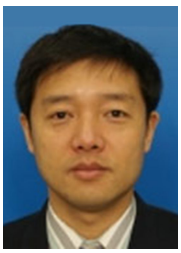


Jun Wan is a Master student at Huazhong University of Science and Technology (HUST), Wuhan. Jun received her B.S. degree in network engineering from Heilongjiang University, Harbin, in 2020. Her research interests include cloud security, privacy and IoT security.



Yu-Han Wu is currently a Master student at Huazhong University of Science and Technology (HUST), Wuhan. She received her B.S. degree in software engineering from Hunan University, Changsha, in 2019. Her research interests include cloud security, privacy and IoT security.

De-Qing Zou is a professor of computer science at Huazhong University of Science and Technology (HUST), Wuhan. He received his Ph.D. degree in computer software and theory at HUST, Wuhan, in 2004. His main research interests include system security, trusted computing, virtualization and cloud security. He has been the leader of one "863" Project of China and three NSFC (National Natural Science Foundation of China) projects, and the core member of several important national projects, such as National 973 Basic Research Program of China. He has applied almost 20 patents, published two books and more than 50 high-quality papers, including papers published by IEEE Transactions on Dependable and Secure Computing, IEEE Symposium on Reliable Distributed Systems and so on. He always served as a reviewer for several prestigious journals, such as IEEE TPDS, IEEE TOC, IEEE TDSC, IEEE TCC, and so on. He is on the editorial boards of four international journals, and has served as PC chair/PC member of more than 40 international conferences.



Hai Jin is a Cheung Kung Scholars Chair Professor of computer science and engineering at Huazhong University of Science and Technology (HUST), Wuhan. Jin received his Ph.D. degree in computer engineering from HUST, Wuhan, in 1994. In 1996, he was awarded a German Academic Exchange Service fellowship to visit the Technical University of Chemnitz, Chemnitz. Jin worked at The University of Hong Kong, Hong Kong, between 1998 and 2000, and as a visiting scholar at the University of Southern California, Los Angeles, between 1999 and 2000. He was awarded Excellent Youth Award from the National Science Foundation of China in 2001. Jin is the chief scientist of ChinaGrid, the largest grid computing project in China, and the chief scientist of National 973 Basic Research Program Project of Virtualization Technology of Computing System, and Cloud Security. Jin is a fellow of CCF and IEEE, and a lifetime member of ACM. He has coauthored 22 books and published over 700 research papers. His research interests include computer architecture, virtualization technology, cluster computing and cloud computing, peer-to-peer computing, network storage, and network security.