A Comprehensive Review of Security Issues and Solutions in IoT Smart Homes

Manju Bagga[1], Richa Datta[2], Neelima[1], Himanshi Dhamija[1], Ravi Kumar Sharma[1]

[1]*MMICT&BM, Mahrishi Markandeshwar (Deemed to be University), India*
[2]*MMICT&BM (HM)/MMEC, Mahrishi Markandeshwar (Deemed to be University), India*

Abstract: With the proliferation of connected devices and the sensitive data they handle, the need of smart home security is rising. Attacks against smart homes have the potential to cause widespread damage to both consumers and communities, as seen in past cases. Although significant progress has been made in identifying security solutions for the Internet of Things (IoT) and intelligent homes, there is still a lack of agreement over the most effective approaches. This article offers a potential security strategy for smart homes and explains the relevance of relevant technology. Installed in a smart hub, the safety solution is a network-based system that detects harmful activity within a home network. In order to demonstrate the notion, two attack detection methods, namely botnet detection and evil-twin attack detection, are shown. From what we can see, the security supervisor is able to spot the former but not the latter.

Keywords: Internet of things Smart Home, Security, Cloud Based, Hubs

1. Introduction

The number of smart homes and the number of devices connected to them are both on the increase [1]. In the past several years, a plethora of new technologies have entered the market. These include HVAC systems, smart locks, and networking protocols like Z-Wave and Zigbee. Up to 25 billion Internet of Things devices might reach by 2020, according to [2]. The widespread use of these devices will bring technology closer to the average person's home than ever before. Despite this, protecting smart homes was not without its challenges. Instances of actual computer hacking highlight the need for top-notch security in this domain. Some functionalities were removed and false fire alarms were triggered, among other issues, in Samsung SmartThings that were discovered by [3]. Extra information on actual clients and hacking companies was also disclosed. The methods used in these assaults can range from utilizing an aquarium thermometer to accessing the backend systems of casinos to gaining access to baby controls [4][5][6]. It may be difficult to design a smart home device that prioritizes security, even though these results highlight the necessity of safety. [7][8] found that conventional methods, such computer-heavy encryption, fail on these systems due to resource constraints. On the other hand, there are a number of initiatives aiming to secure IoT devices with little resources [9] further work is needed in this area [10]. When it comes to traditional security, smart home intrusion detection systems (IDS) are still in their early stages. Additionally, several novel methods for intrusion detection in systems with limited resources were proposed by the researchers. Nevertheless, the majority of these studies focus on WSNs or generic Internet of Things (IoT) devices [11] [12] [13] with just a handful mentioning the smart home situation. Despite the importance of the smart center—a collection of interconnected smart homes—none of these approaches have taken it into account thus far. Investigating hub-based threat monitoring will improve smart home security by increasing user awareness of potential dangers.

This document has a dual purpose. It begins by outlining the general threats that current and future smart homes face in terms of security. The second part of utilizing this information is taking care of the protection analysis for the smart home community. This is accomplished through the use of a prototype security module that can detect and track harmful actions. This article will examine the smart hub's suitability for this kind of mechanism, looking at its detection rate and resource use.

2. Related Work

There is still a great deal of research on the topic of protecting intelligent homes, even though it is a relatively new field of study. This chapter delves into significant research and clarifies the connections between different studies. Other researchers' risk assessments. The use of risk assessments as a framework for identifying potential dangers has been around for a while. Threats aside, there are a plethora of resources available to do such analyses. While many traditional approaches to risk assessment predate the present cyber-physical networks, contend that new approaches are necessary for conducting risk analysis within IoT systems. Therefore, when it comes to evaluating existing IoT settings, these techniques fall short. For these reasons, we zeroed down on the Internet of Things (IoT) and smart homes as specific targets for our risk study. In 2016, Jacobsson et al. conducted a thorough risk study centered around the Internet of Things (IoT) utilizing the ISRA approach as part of a smart home project. Numerous possible issues, many of which were unique to smart homes, were brought to light by the research. The other safety studies that focus on smart home applications and devices. These research mainly aim at finding system weaknesses and proposing methods to address them. Although it is not their primary emphasis, they frequently discuss system dangers. In order to create an expandable platform for avoiding dangers to smart homes, it is necessary to understand a variety of hazards.

2.1 Finding intruders in Internet of Things devices

Several intrusion detection systems for the Internet of Things are available. Nevertheless, there are still many unresolved issues that must be addressed before the topic can be deemed mature. Each node in a sensor network may have its own instance of an intrusion detection system (IDS), and many of these systems aim to provide distributed solutions for such networks. The lack of consensus among manufacturers on a common framework and the fact that smart homes might contain a wide variety of gadgets and technologies are two of the main drawbacks of a distributed intrusion detection system in this context. Our method instead looks at a centralized system that detects data violations. It included using a portable Raspberry Pi 2 to run the popular general-purpose intrusion detection system (IDS) Snort on a tiny single-board computer. The authors demonstrated two main characteristics. First of all, the device's mobility and user-friendliness make it ideal for installation in any preferred spot. Second, several Raspberry Pis could cooperate thanks to the design, which boosted detection rate while decreasing false positives. But when the network traffic was very high, they discovered that only one Raspberry Pi was unable to handle it.

3. The main architecture of the smart home

A smart home is an interconnected network of electronic gadgets that may be managed and programmed by a central hub. Any given device, whether it's a sensor, actuator, or hybrid of the two, will likely have limited processing power and random access memory (RAM).

3.1 Architecture based on WiFi

WiFi-based designs, consumer gadgets that can be connected to WiFi also come with a companion app that can be used to keep tabs on them. Even those without technological training will find the applications to be user-friendly.

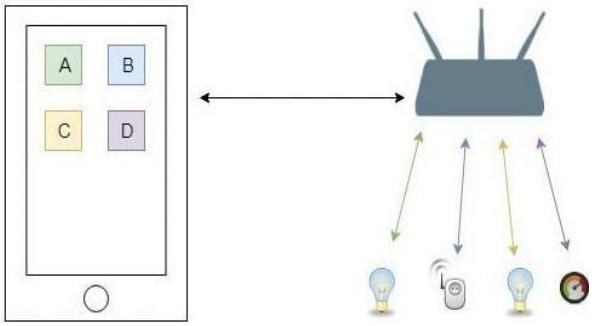

Figure 1 A WiFi-based architecture

3.2 Architectures that are integrated

These days, smart home technologies are an integral part of contemporary house design. The gadget may have HVAC (heating, ventilation, and air conditioning) components, for instance. Dedicated touch

screens, hardware buttons, and sensors are all examples of physical components that make up the user interface.

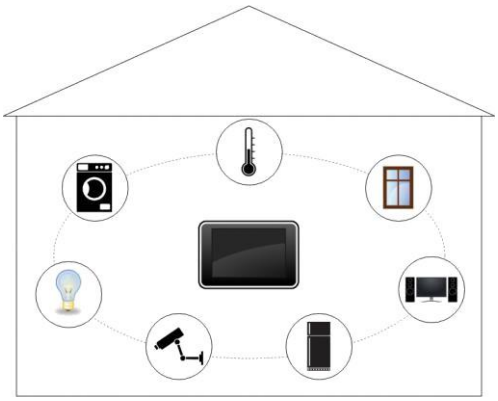

Figure 3 A cloud-based architecture such as Google Assistant

3.3 Cloud-Based designs

Market leaders like Amazon and Google provide smart home cloud support. For these configurations, they offer an interface, like Google Assistant or Amazon Alexa, and users may link compatible devices to that interface. By utilizing a common interface for all devices and ensuring cross-compatibility across different manufacturers, this allows for the house to be expanded. In a few of these cases, the user may keep tabs on all of their smart home gadgets with just one app.

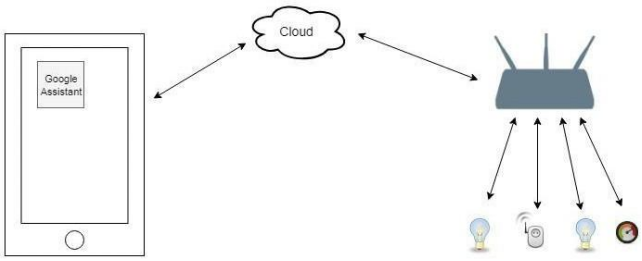

Figure 3 A cloud-based architecture such as Google Assistant

3.4 Infrastructures built around hubs

The last design we provide is a framework based on hubs, such the Home Assistant hub or the Samsung Smart-Stuff hub. In a cloud-supported design, for example, a hub would be the central unit that connects all of the supported devices to a single interface. The end user may have to spend more time and money on the installation and configuration of a physical hub, though.

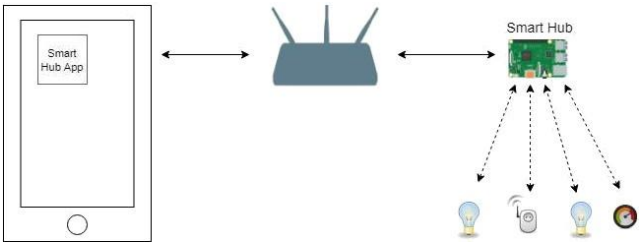

Figure 4 A hub-based architecture, such as Samsung SmartThings and Home Assistant

The need for smart homes has led to the development of many communication technologies and protocols. Of them, Zigbee, Z-Wave, CoAP, and MQTT are comprised. Wi-Fi and Bluetooth, two commonplace technologies, find extensive application in smart homes. This leads us to assume that these characteristics are present in the typical smart home user. Fear and reluctance have generally been confronted with technology, despite evidence suggesting that smart homes offer many benefits for the elderly and the disabled. On the other hand, the majority of smart home users are likely to be young, well-off men. If a smart home gadget wants to be popular with consumers, it needs to be easy to use and have high availability.

4. Security Risk

The terms risk, danger, and vulnerability appear often in articles on smart home security. They are often thought to signify the same thing, and it's not always clear what the exact meaning is. The following definitions are employed in this research paper: Any potential source of damage to the device is known as a hazard, and any current system vulnerability is known as an exploitable weakness. The combined likelihood of a hazard and the cost of its consequences is known as a danger.Many of the identified concerns in the Internet of Things (IoT) study are relevant to the smart home scenario.You can find a more detailed list of the most pressing safety concerns for smart homes—those with a mean risk value higher than 8—in Table 1 of this research report. Inadequate security measures across the board and careless user actions are the two main types of these dangers. The field also considers these threats to be urgent. In 2014, the renowned Open Web Application Security Project (OWASP) identified ten of the most serious security holes in Internet of Things (IoT) devices. Although the domains of the Internet of Things and smart homes do not entirely overlap, the fundamental security issues of the IoT may also be applied to smart home environments. In Table 2, you can see the top five vulnerabilities that OWASP has documented.

5. Real world attack on smart homes

Distributed denial of service (DDoS) assaults are one type of cyberattack that can take advantage of the proliferation of smart home gadgets. An example of this is the widespread impact of the Mirai worm, which compromised smart home devices and hundreds of thousands of other Internet of Things (IoT) devices. Many major distributed denial of service (DDoS) assaults originated from Mirai, which was found in 2016. An assault with a peak throughput of 1.1 Tbps was far more powerful than what the majority of internet nodes are capable of handling. Although Mirai targets innocent Internet of Things (IoT) device weaknesses—like using default passwords—it has the potential to significantly impact the internet's underlying infrastructure. An assault on the service provider Dyn in October 2016 rendered several popular websites inaccessible. News reports have also focused on a few of smaller assaults that only targeted one person or organization. In 2014, a someone broke into a networked child monitor and repeatedly yelled out, "wake up boy," to a youngster who was sound asleep (Best, 2014). Two Finnish buildings had their thermostats hacked in 2016, rendering the heating systems inoperable. The outdoor temperature was at about -5°C when this happened. The widely-discussed incident in 2018 did not target a residence but rather a gambling establishment. After breaking into the network using a smart aquarium thermostat, the perpetrators were able to compromise the high-roller database.

6. Smart home security measures

This section discusses the present danger scenario and how it relates to the realm of smart homes, as well as traditional security regulations. Additionally, it provides several security measures. Moreover, techniques adapted to a smart home context. The field of smart home security is still in its infancy, but new ideas and methods are starting to emerge. In continuation of the part on traditional methods, this one presents a couple of them for comparison's sake. Either way, users' lack of technical knowledge or limited resources will be addressed. Transport layer security (TLS), one of the most used encryption protocols, sits above TCP in the TCP/IP stack. Nevertheless, DTLS, a comparable protocol that offers support for UDP encryption, may be utilized with the CoAP protocol, which is efficient and uses little resources. This makes it possible for some nodes to encrypt data transmissions, which in turn increases protection. The complexity of the encryption techniques, however, means that most devices with limited resources will also be unable to use this feature. One protocol that is occasionally utilized in smart homes, MQTT, is now the subject of research aimed at ensuring its security. The SMQTT protocol l was designed by researchers in 2015 using the lightweight attribute-based encryption (ABE) technique to establish secure communications in the MQTT broadcast domain. Support for devices with limited power consumption was also added for MQTT-SN, which stands for MQTT for sensor nodes. Several novel approaches to user authentication have been investigated. Patents for voice authentication systems may be traced back to the year 2000. Nevertheless, this approach did not gain traction until recently, when major players like on a massive scale. To counter playback attacks utilizing pre-recorded audio files, This idea to incorporate motion authentication as well as voice authentication. Voice features

should be available only when the user is physically present at home. The end user will be informed about potential breaches of specific devices in their smart home setup by an intrusion detection system, however the system cannot prevent exploiting vulnerabilities. Customers, even those without much technical knowledge, might be able to use this data to take action, such as taking the item to a repair shop or even just taking it off. Reduced risk of infection and subsequent mitigation of viral transmission in a given network is the consequence of a temporal constraint on the infected system's ability to transmit the virus.

7. Prototype

In order to identify suspicious activity in a smart home network, this article details the process of creating a protection module. This module, which will be linked to the well-known Home Assistant Open Source Smart Hub Platform, will be called the security supervisor.

7.1 Household aid design

In this part, we see how the Home Assistant and the security supervisor are built, and we also see how they talk to each other. The security supervisor is built to seamlessly interact with any smart hub, including the Home Assistant, as indicated in this article. The software design of the app is both simple and scalable. Home automation, a user interface, and components for communicating with other smart home gadgets make up its main components. Figure 5 shows that the shaded areas correspond to elements of the Home Assistant source code, while the unshadowed areas represent actual devices and external libraries.

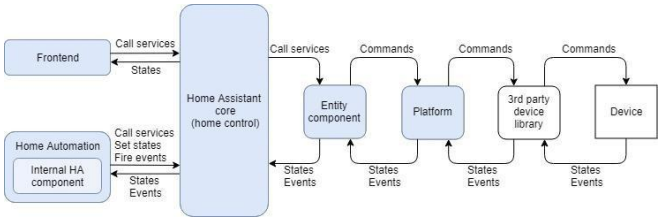

Figure 5 Architecture of Home Assistant

7.2 Security supervisor architecture

The danger detection system now includes a built-in home helper. It can include the particulars of the smart home configuration into its threat detection algorithms since it has access to the hub's internal information and the event bus. There are three primary levels to the threat detection component's tiered and modular architecture: data display, threat analysis, and collection and pre-processing. Layers one and two are the main focus of this article. Gathering and preprocessing data is done at the first layer. Not only is this data from the network, but it also shows the current state of the smart home's gadgets. The ability to intercept and analyze network data in order to look for dangers is essential for the security supervisor. In Figure 6, we can see how this interface component gathers data from several sources and merges it into one stream

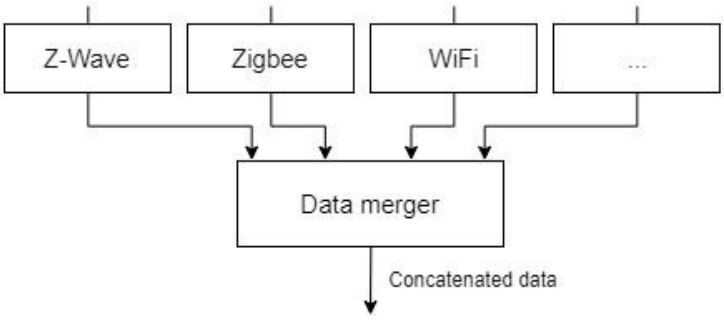

Figure 6 The traffic concatenation module provides a generic interface for multiple technologies

Profiling is a fundamental principle used by the security supervisor. At the highest level, Layer 1, you'll find a set of tools for managing system profiles. Figure 7 shows the profiling approach and its effects on the other security supervisor layers. Take note of how layer 2 is split into two sections to match the profiling: one section for doing the analysis and another for conducting the profiling.

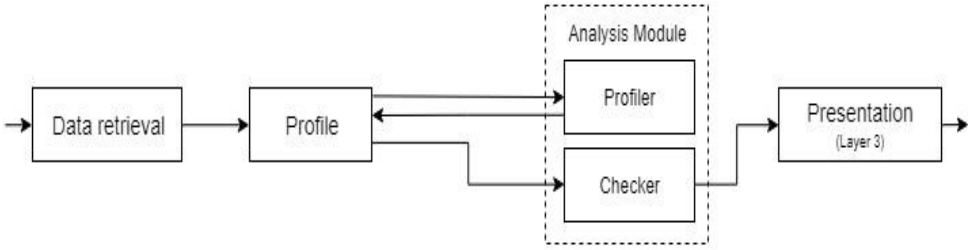

Figure 7 Data flows through the profiling functionality

There are security modules inserted into the second layer review module. As mentioned earlier, each module is designed to help identify specific threats and then gives a philtre that matches those threats' overall traits. In order to determine whether smart home devices are being utilized by botnets, the botnet detection module must be activated. We zero in on WiFi-enabled devices and those utilizing the TCP/IP stack since that's where most botnet-based distributed denial of service assaults go. If the device communicates with an inappropriate destination, the module will notify the user and monitor the device's outgoing data. All targets that the system did not engage with during profiling are considered inappropriate in our implementation. This module is responsible for protecting the smart home from so-called evil-twin assaults, in which an AP controlled by an attacker takes control of all of the devices. A lot of private information may be leaked, and the smart home or network could be easily compromised. This module checks if an access point is an evil twin by using the RSSI. An attacker would have a harder time forging this statistic than data from network protocols. Here are the details of how the algorithm is designed to function. You may get a complete inventory of all connected devices and their coordinates in the evil-twin module. It verifies these devices' locations on a regular basis and alerts the user to potential attacks if any device's location doesn't match its declared position. But the module will think the smart hub has moved if the RSSI readings from every device suddenly shift.

8. Functionality tests and experiment

1. Botnet component Testing the botnet module's functionality aims to determine the level of malicious traffic that the security supervisor is able to identify. This will be implemented in three stages. After that, we use a stream of network data to extract actual data and store it in a register. To add insult to injury, we are tagging this file with packets that indicate its potential danger. Last but not least, the file is embedded into the network packet stream to mimic malicious activity, and the module's detection count may be maintained. To test the device's resilience to various packet compositions, the research modelled a range of DDoS assault types.
2. Overlap of IP fragment,
3. ping floods,
4. SYN/FIN flood of TCP,
5. flood of UDP DNS,
6. attack of the mud, smurf attack (MAC address spoofing),
7 and flood of IPv6 are all attacks that have been tested. The functionality tests of the evil-twin analysis module aimed to find out if it could distinguish between an AP controlled by an attacker. In any case, finding out if there is any variation in the apparent signal strength that would impede the solution was crucial. Finally, we had to think about whether the home's inhabitants or obstacles may substantially impact the outcomes. In order to ensure fair comparison, the studies were conducted in an environment free of obstacles and with minimal involvement from locals.

Module 8.2: Evil-twin

Following this protocol, we ran the evil-twin research module test. In this scenario, an Android smartphone in hotspot mode was utilized as a mobile computer to mimic an AP that was acting maliciously. Although it shared our test network's SSID and password, it refrained from impersonating our network or taking any other steps that the malicious AP may have anticipated. This is a minor consideration, though, because our defense against the evil-twin attack does not depend on these characteristics. The test result was derived from the total number of times the analysis module recognized the presence of the villain device, which was activated at different points across the room.

9. Results

Module 9.1: Botnet
The module recorded all packet occurrences when the departing address was not already profiled, provided that the source IP and MAC addresses belonged to a legitimate device. The module can detect instances when the originating IP address is spoofing, meaning it is not the IP address of a legitimate device. This capability is demonstrated in the smurf-type assaults row. Unfortunately, the module is unable to identify assaults that involve a spoof of both the IP address and the MAC address, as demonstrated by the smurf entry (with faked MAC).

10. Conclusions

Evidently, cybercriminals will find smart houses appealing, and this trend will only grow. Cybercrime has the potential to impact people and society in profound ways, and security failures in smart homes are a stepping stone toward it. We have focused on developing and evaluating a smart home security system that can reduce societal and individual security risks in this effort. We have successfully implemented solutions to address two different threats. The assaults in question involve botnets that leverage smart home devices and evil-twin attacks, in which the adversary attempts to take devices from the access point in order to steal information. We both believe that a smart hub is a good location for a smart home's IDS from a resource-conservation standpoint. Our research leads us to believe that a Raspberry Pi-level smart hub can manage a tiny intrusion detection system (IDS) without sacrificing its capacity to serve as a smart hub.

References

1. Denning, T., Kohno, T. and Levy, H.M. (2013) ‘Computer security and the modern home’, Communications of the ACM, Vol. 56, No. 1, pp.94–103.
2. Ravi Kumar Sharma & Parul Gandhi, “Quality Assurance of Component Based Software Systems”, 2016 International Conference on Computing for Sustainable Global Development (INDIACom), 978-9-3805-4421-2/16$31.00@2016 IEEE.
3. Fernandes, E., Jung, J. and Prakash, A. (2016) ‘Security analysis of emerging smart home applications’, 2016 IEEE Symposium on Security and Privacy (SP).
4. Ravi Kumar Sharma, Parul Gandhi,” Study of Reliability of Object-Oriented Structure Consuming CK Metrics”, “2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)”, 828-831, IEEE.
5. Singh, T., Sharma, R. K., Kamboj, D., Gandhi, P., & Bhatia, D. (2023, November). Using SVM Classification and Reverse Engineering to Generate Trustworthy Code in Software Development. In Proceedings of the 5th International Conference on Information Management & Machine Intelligence (pp. 1-7).
6. Hossain, M.M., Fotouhi, M. and Hasan, R. (2015) ‘Towards an analysis of security issues, challenges, and open problems in the internet of things’, 2015 IEEE World Congress on Services.
7. Jacobsson, A., Boldt, M. and Carlsson, B. (2016) ‘A risk analysis of a smart home automation system’, Future Generation Computer Systems, Vol. 56, pp.719–733.
8. Forzin, A., Marmol, F.G., Conti, M. and Bohli, J. (2016) ‘RPiDS: Raspberry Pi IDS – a fruitful intrusion detection system for IoT’, 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld).
9. Mittal, S., Singh, T., Sharma, R. K., & Gandhi, P. (2023, November). Soft Computing Methods for Predicting Component Development System Through Software Reusability. In 2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 166-172). IEEE.
10. Singh, M., Rajan, M., Shivraj, V. and Balamuralidhar, P. (2015) ‘Secure MQTT for Internet of things (IoT)’, 2015 Fifth International Conference on Communication Systems and Network Technologies.
11. Sivaraman, V., Gharakheili, H.H., Vishwanath, A., Boreli, R. and Mehani, O. (2015) ‘Network-level security and privacy control for smart-home IoT devices’, 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).
12. Sharma, R. K., Brar, T. P. S., & Gandhi, P. (2021). Defense and Isolation in the Internet of Things. Internet of Things in Business Transformation: Developing an Engineering and Business Strategy for Industry 5.0, 141-168.
13. Summerville, D.H., Zach, K.M. and Chen, Y. (2015) ‘Ultra-lightweight deep packet anomaly detection for Internet of things devices’, 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC).
14. Sung, D. (2018) Smart Home Visions through the Ages: The History of Home Automation, January 2018.
15. Tang, Z., Zhao, Y., Yang, L., Qi, S., Fang, D., Chen, X., Gong, X. and Wang, Z. (2017) ‘Exploiting wireless received signal strength indicators to detect evil-twin attacks in smart homes’, Mobile Information Systems, pp.1–14.