Threat Modeling of IoT-based Smart Home Systems

Abdullah Ali Ben-Nakhi*
Kuwait University, KUWAIT

Mostafa Abd El-Barr†
Badr University in Cairo, EGYPT

Kalim Qureshi‡§
Kuwait University, KUWAIT

Abstract

Internet of things has a wide range of applications such as healthcare, agriculture, transportation, and industrial manufacturing. Smart homes automation occupies a large segment of applications. Although these devices are improving constantly, security is still a challenge for them. In this study, Microsoft STRIDE is considered. STRIDE threat modeling is a tool used to simplify threats categorization. STRIDE modeling tool used to design a generic smart home system and analyze the design in terms of vulnerabilities in the design. The tool generated threats compared to the collected threats from the systematic literature review. Comparing STRIDE generated threats with the collected threats is to examine the system from a complete overview, not just examine a single component or attack type.

Key Words: Smart homes, security, threat modeling, IoT, systematic literature review, STRIDE modeling.

1 Introduction

Internet of Things is a broad term that covers a wide range of applications. Examples include smart homes, wearable devices, smart grids, and connected cars [11]. But, IoT-enabled smart homes application stands out as the most prominent application under IoT. By 2022 smart home market share is expected to reach 53.45 billion dollars [22], and by 2023 the number of smart homes is expected to exceed 300 million houses [23]. Smart homes are described as the ability to control and monitor different home devices and appliances remotely via the internet. Smart home applications encompass the needs of the residents to provide comfort, safety, security, and energy-saving for the inhabitants [70]. Although IoT-enabled smart homes devices are used for a wide range of applications, security and surveillance are the most dominant application requirements. According to the statistics, the amount of smart home security and surveillance devices sold is expected to triple between 2017 and 2022 [7].

The reason for the enormous demand for a home security system is that these devices should give a sense of safety and security to homeowners. Another critical application for smart home automation is healthcare automation at home for the elderly and people with disabilities [18]. From the existing statistics, we infer that the demand and the usage of smart home devices are growing over time. Hence, this growth motivates us to:

- Analyze the risk resulting from vulnerability to figure the severity of the vulnerability to households.
- Map the proper mitigation method using threat modeling to simplify the risk overview to the user-level.

Therefore, mitigating the vulnerabilities encountering smart homes is becoming difficult over time and makes smart homes exposed to a wide range of attacks.

The main aim of this study is to find out the current state of the art in smart home devices in terms of their security by simplifying the overall view of these threats to facilitate vulnerabilities mitigation.

The security challenges can be grouped under three categories as follows [1]:

- Data security: IoT devices rely heavily on exchanging data among them. These data can have personal or confidential nature which makes them a valuable target for attackers, therefore, authenticity and confidentiality of data must be guaranteed.
- Communication security: due to the heterogenicity of smart home devices the medium to exchange is diverse, in this case, integrity and access control are required.
- Application security: The collected data from devices finally pour into the application end to be processed, in this case, the application security itself is a concern and the contained data privacy.

*Department of Information Science, College of Life Sciences. Email: bennakhi1@gmail.com.
†Department of Electrical Engineering, College of Engineering. Email: mostafaabdelbarr@gmail.com.
§Corresponding author. Tel: +96597639430, Department of Information Science, College of Life Sciences. Email: kalimuddin.qureshi@ku.edu.kw.

Although the security of smart home device is a critical part of the design of the product, device manufacturers do not take it seriously for many reasons. Manufacturers overlook security features to compete in a very competitive market, which allows them to release products faster and prevent the product from be obsolete in a short period [9].

The multilayered architecture of smart home systems due to hardware architecture design differences according to manufacturer uses different communication standards and protocols in their products. Also, in the application layer, a variety of operating systems and firmware are used to operate these devices [6]. The heterogeneous nature of smart home systems imposes several security challenges [8]. Moreover, IoT-enabled smart home devices are known for their CPU power, memory, storage, and power limitation due to their constraints of the design [14]. These limitations cause difficulties in implementing advanced security mechanisms. Another major security challenge is the human factor. The limited technical knowledge usually led to misconfiguration and misuse of these devices makes them susceptible to social engineering attacks [4]. Unlike traditional information systems, IoT-enabled smart home devices increase security challenges because the cyber and physical threats converge as the application makes demands [25].

The research in this work includes the following. We start by examining related work to our topic to find the shortcomings as well as the strength in the articles. We then consider the STRIDE threat modeling in categorizing extracted threats. We follow that with mapping the proper countermeasures. In addition, the STRIDE threat modeling tool is used to model generic smart homes to generate the potential threat from the STRIDE perspective. The resulting threats from the STRIDE tool are compared to the excreted threats.

2 Literature Review

This section studies the related works that appear in the literature. In [10] the researchers classified smart home attacks into main categories according to IoT layers. Each layer is examined separately for security issues and solutions proposed. There was no methodology proposed to elicit attacks. The attacks on each layer were obtained from previous articles in the field of IoT security. A survey of a recent solution is conducted to present state-of-the-art risk mitigations.

The research in [2] states that the increased number of IoT-based devices connected to the internet used in smart homes widen the attack vectors. In this research, they collected 12 common attacks on smart homes presented in related works and explained the possible impact of these threats. They stated that although there are several solutions to improve smart home security, it is difficult to achieve comprehensive security. This is because of the increased number of technologies used in IoT devices.

The researchers in [14] stated that since IoT-based smart homes are connected to the internet they directly or indirectly expose the inhabitant's privacy and data to vulnerabilities. Although inhabitants' physical security is important, they only take into consideration cyber security. They classify attacks into two classes internal and external. Internal attacks are possible when attackers are nearby, and external attacks are conducted through the internet. In the article, they only identified five common attacks on smart homes and no countermeasure was suggested.

In [12] threats are classified into two categories: passive and active attacks. Passive attacks are where the attacks are eavesdropping the information with no intention to manipulate the information. Whereas, in active attacks, the attacker intends to cause harm to the system such as modifying the messages between equipment or interrupting the system functionality. Due to the popularity of smart home devices, house holders are more concerned about security and privacy risks in smart homes. They summarized the most vulnerable attack in three sets: connected objects, cloud, and applications. Within these three categories, security risks are classified into three levels: low, intermediate, and high-security issues. For each of these levels, the proposed countermeasures are derived from other researchers' works.

In [5] a comprehensive survey is conducted in IoT in general and focuses on smart home security issues. With taking into consideration user awareness, this paper analyzes the technical perspective of IoT security risk. Based on the current known IoT attacks, they state that smart home systems are vulnerable to many threats because of a lack of security in the design phase of these systems. Although they identified many attacks in their work, there is no clear taxonomy for categorizing threats. In addition, the suggested solution solely concentrates on protocols used in smart home automation devices.

In [26] a survey on security challenges was taken in a physical/network layer in smart home automation and the exciting proposed solutions for these challenges. Additionally, security attacks on the voice control interface are also examined. Since voice control is one of the most used smart home features, they proposed a two-factor voice command validation framework to improve the voice control interface. However, they did not show how the survey was conducted to summarize the collected attacks.

In [13] the researchers simplify the threat identification by using the attack trees methodology. The attack trees proposed are based on the smart home model with different configurations to identify the different attack's surfaces. The goal of this work is to improve the security of smart homes in terms of hardware and software. The root of the tree represents the attacker's goal, the branches represent the attacker's method to achieve the goal, and the leaves represent the final step to achieve the attacker's goal. However, the attack tree clearly explained that no countermeasures were suggested to mitigate the identified attacks.

In [24] a survey is conducted on IoT-enabled cyber-attacks since 2010 in all IoT application domains. Two types of attacks were examined in the article. They were either based on real-life scenarios or produced in controlled environment published attacks by other researchers, and they exclude attacks that cannot be verified practically. They study these attacks on IoT-enabled devices to find not only the effect on the device itself,

but also on the target system of which the device is part of. In addition, they categorized attacks based on the attacker's goals. Then they assess the threat severity based on risk assessment standards such as ISO 27005 and NIST SP800-30. Therefore, security controls are proposed to mitigate the threats in the short term and long term. The proposed security controls are grouped into six categories: physical access, logical access, hardware, software, network, and procedures. They conclude improving smart home systems needs a comprehensive analysis. Table 1 summarizes this type of work.

3 Threat Modeling

Data was collected in the previous section from studies using systematic literature review and conducting a survey with experts in the field. In this section, threat modeling is conducted to simplify attacks categorization. According to [17] threat modeling applies to a wide range of applications such as software, systems, networks, and things in the Internet of Things. In this section, a threat model is designed to facilitate the mitigation of risk in smart homes from the user perspective to understand how the system works. Threat modeling in our case was conducted to identify and understand the threats in smart home systems and then decide on the proper mitigation method in a simple manner. Threat modeling is useful in clarifying at which point the element in the system is vulnerable to attacks and analyzing the type of attack that could be conducted. Also, threat modeling helps to anticipate potential threats that might be missed by users and understand the risks from the attacker's perspective. Threat modeling is important in the system design phase. There are many threat modeling frameworks such as PASTA, OCTAVE, and LINDDUN. PASTA is designed specifically for organizations planning to merge their strategic objectives with the anticipated risks, and OCTAVE is a complex threat modeling tool that requires great effort and dedicated time to examine the information assets [15]. Whereas the LINDDUN framework focuses solely on privacy risks in the system [20].

3.1 Microsoft STRIDE Threat Modeling

We adopted the Microsoft STRIDE framework since it applies to IoT threats and provides an easier overview of risks [21]. STRIDE is an acronym that stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of privilege. STRIDE utilizes data-flow diagrams to illustrate the flow of data between elements in the system and interaction with external entities. STRIDE simplifies interactions between elements for easier to understand threat modeling.

This data flow diagram identifies threats encountered during transitions and interactions. STRIDE framework maps the element to the potential threat category. Also, it rates threat severity to provide risk level [3]. In our case, when a house owner purchases a system or devices, threat modeling provides an overview about what the households are facing, and the proper mitigations needed to take into consideration. Table 2 is based on Table 2 from [21] STRIDE threat categories presented and defined with which security property was violated.

Threat modeling in our case includes: a layout design of a typical smart home system, threat list, countermeasures list and the action undertaken to combat each threat. Conducting threat modeling using STRIDE framework must consider these four steps [16]:

a) Identify the assets of the system
b) Identification of threats
c) Rating of the threats
d) Propose countermeasures

In this section, steps a-d are implemented using STRIDE threat modeling to simplify threats extracted in Section 4 categorization, risk rating, and countermeasure mapping. After that, a generic smart home system data flow diagram was designed using the STRIDE modeling tool to analyze potential threats, understand the data transactions and countermeasures suggested. In the end, the extracted threats from Section 4 are

Table 1: Security challenges reviews and surveys

Article	Type	Threats Number	Threat Type	The Future
Smart Home Is Not Smart Enough to Protect You - Protocols, Challenges and Open Issues [10].	Review	5	Perception layer Network layer Application layer	Investigate smart homes components
A review on smart home present state and challenges: linked to context-awareness internet of things (IoT) [2].	Review	12	Physical attacks Malicious code Eavesdropping Personal information abuse	Develop smart home solution
IoT-based smart homes: A review of system architecture, software, communications, privacy, and security [14].	Review	3	Data breaches Authorization User privacy	Computer engineers and specialist involves in smart homes development

Table 2: STRIDE threats [22]

Threat	Property Violated	Definition
Spoofing	Authentication	Pretending to be something or someone other than yourself
Tampering	Integrity	Modifying something on disk, ona network, or in memory
Repudiation	Non-Repudiation	Claiming that you did not do something or were not responsible.
Information Disclosure	Confidentiality	Providing information to someone not authorized to see it
Denial of Service	Availability	Absorbing resources needed to provide service
Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do

compared to threats generated from STRIDE tool and discussed.

3.2 Identify Assets of the System

There are several implementations of smart homes. This implementation depends on the needs of the household. But there is a basic infrastructure that is mutual among various implementations. The common assets are central hub or gateway, devices such as surveillance cameras, cloud service, and control software (Figure 1). According to Microsoft IoT security architecture [19] the best practice for STRIDE threat modeling is to divide IoT layout into zones: devices, field gateway, cloud gateway, and services. Zone separations provide data boundaries that facilitate threat detection through data transition. Table 3 maps the generic smart home IoT layout into STRIDE model layout.

Table 3: IoT layout conversion to STRIDE model

IoT layout	STRIDE layout
Gateway or Hub	Field gateway zone
IoT devices	Device zone
Cloud service	Cloud gateway zone
Control software	Services zone

STRIDE framework streamlines the threat categories for easier user understanding. In Table 4, 23 extracted threats classified into STRIDE categories according to definition and property were violated. This conversion facilitates understanding of the risk from the non-security expert

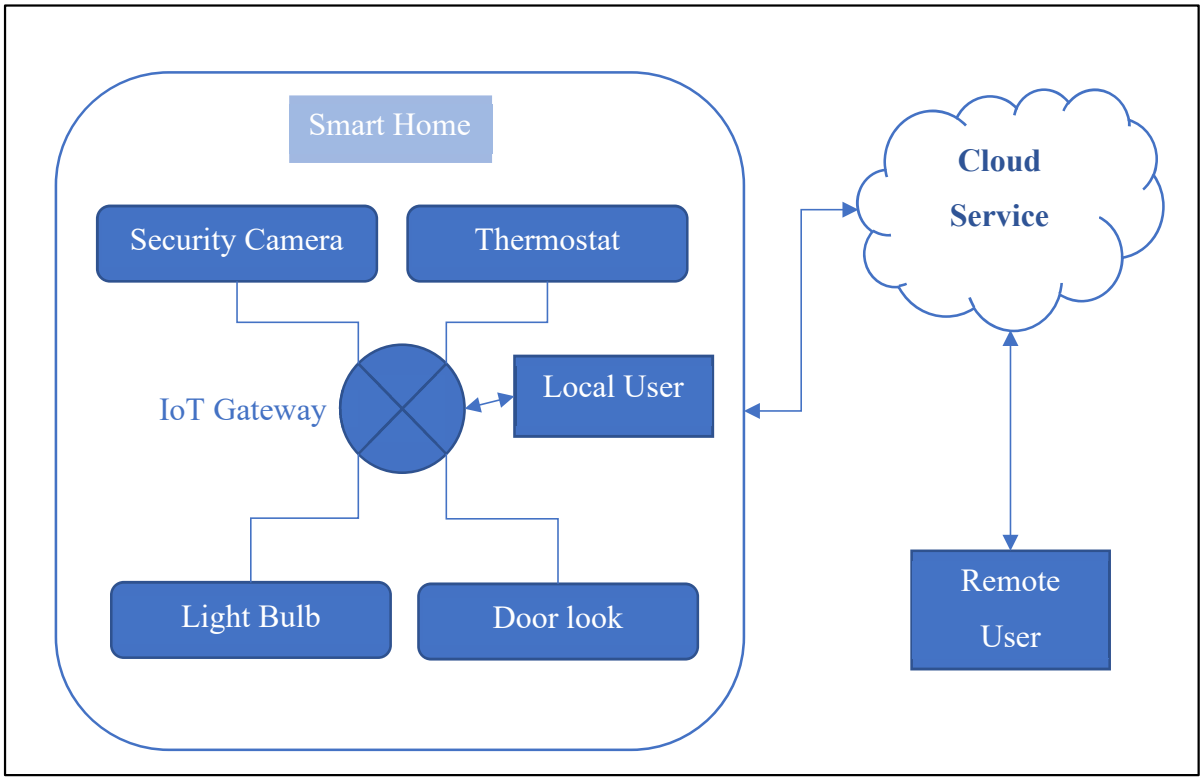

Figure 1: Smart home layou

Table 4: Threats STRIDE conversion

STRIDE Categories	Property Violated	Extracted Threats
Spoofing	Authentication	Spoofing, impersonation, brute force attack, MITM, masquerade attack, unauthorized access
Tampering	Integrity	Forgery, malicious code injection, physical attack, unsecured interfaces, gain initial access
Repudiation	Non-Repudiation	No repudiation threats were mentioned in the selected papers
Information Disclosure	Confidentiality	Data leakage, eavesdropping, insecure communication, abuse attack, open ports, replay attack
Denial of Service	Availability	DoS, DDoS, jamming, or interruption attacks
Elevation of Privilege	Authorization	Over privileged, lack of authentication,

background. Also, a threat with similar methods is grouped into the same category. For example, man-in-the-middle (MITM) and spoofing attacks both intercept messages between two parties and alter them, which is called active eavesdropping. Unlike, replay attack which is passive eavesdropping with no modification done to the transmitted messages. The extracted threats are classified according to the attacker's goal, needing a medium to reach the final goal. However, in the non-repudiation category, there are no threats mentioned from the extracted threat.

3.3 Rating of the Threats

After the risk is identified, threat assessment is conducted to rate the threats and prioritize the mitigation process. In some cases, not all threats are feasible to mitigate. Some of the threats can be ignored. Threat assessment conducted using Microsoft DREAD framework. DREAD acronym for Damage potential, Reproducibility, Exploitability, Affected users, Discoverability. In Table 5 DREAD risk factor was explained in [14], each question answered with a range of severity from 1-3. Then after scoring all the risk factors, calculate the total of each threat. If scores are 5-7 the risk is low, 8-11 risk is medium, 12-15 risk is high.

Table 6 shows the threats rating for the extracted 23 threats.

4 Proposed Countermeasures

After classifying risk into SRTIDE classes we select the proper countermeasures from Table 6 to threats in Table 7.

5 Implementing STRIDE Threat Model

In this section the STRIDE threat modeling tool is used to implement smart home generic data flow architecture. Designing a home system using a threat modeling tool is important to understand the potential threats encountering households. Furthermore, the modeling aims to understand the vulnerabilities from the attacker's perspective. Threat modeling is conducted before deploying the system to identify potential threats. When modeling the system these elements are taken into consideration: processes, data stores, data flow, and external entities. Based on Figure 2 and Table 7 common IoT-enabled smart home design uses Microsoft STRIDE threat modeling tool as shown in Table 8.

According to [19] it is recommended that IoT architecture be divided into zones, where each zone has its data and authentication method needs. Then zones are separated by trust boundaries (dotted lines) to represent data transition from one source to another. As shown in Figure 2 device zone and local user zone interact with the home gateway. Then the data is transferred to the cloud gateway through an internet connection to the service provider cloud to store, analyze data and allow the remote user to interact with the home system.

Using a threat modeling tool, a report is generated based on the designed system. The report states that this design posed 97 threats and examples depicted on how the attacker conducts the attack are included. These threats are summarized into spoofing, forgery, DoS, data leakage, data repudiation, sniffing, interruption, impersonation, code injection, lack of authentication, lack of authorization. The modeling tools do not only depict potential threats but also often suggest countermeasures as shown in Table 8. All the identified threats generated from the modeling tool are included in the threats list extracted from selected prime studies in Section 4, except for repudiation which was not mentioned as a threat before in 35 selected prime studies.

6 Results and Analysis

The motivation behind this research was the growth of the use of IoT devices specifically in smart home applications. Such systems give the households a sense of security and control over the house. The smart home system consists of newly emerged IoT-enabled devices known for their limitations. IoT device limitations have imposed security concerns because security control mechanisms require major computational power. For this reason, we conducted a rigorous systematic literature review to identify the recent vulnerabilities threatening smart home systems and security control proposed to mitigate these vulnerabilities.

6.1 Threat Modeling Findings

As stated previously, there is heterogeneity in threats categorizations in different articles proposed. Different

Table 5: DREAD risk factors

Risk Factor	Meaning
Damage potential	How great is the damage if the vulnerability is exploited?
Reproducibility	How easy is it to reproduce the attack?
Exploitability	How easy is it to launch an attack?
Affected users	As a rough percentage, how many users are affected?
Discoverability	How easy is it to find the vulnerability?

Table 6: DREAD threat rating

Vulnerability	D	R	E	A	D	Total	Priority
DDoS or DoS	1	3	3	3	3	13	High
Data leakage	3	2	3	2	1	11	Medium
Eavesdropping	2	2	3	2	1	10	Medium
Forgery	2	2	1	2	2	9	Medium
MITM	2	3	2	1	2	10	Medium
Lack of authentication	3	3	2	3	1	12	High
Unauthorized access	3	3	2	3	1	12	High
Malicious code injection	3	1	1	3	1	9	Medium
Over privileged	2	2	2	1	2	9	Medium
Replay attack	3	2	2	3	1	11	Medium
Physical attack	3	1	1	3	1	9	Medium
Impersonation	2	3	3	2	3	13	High
Spoofing	3	3	2	3	3	14	High
Brute force attack	3	1	2	2	3	11	Medium
Insecure communication	3	3	2	3	3	14	High
Abuse attack	2	3	1	2	2	10	Medium
Jamming or interruption attacks	3	2	3	3	3	14	High
Lack of encryption	3	2	3	3	2	13	High
Open ports	2	2	2	2	2	10	Medium
Masquerade attack	3	3	2	3	1	12	High
Gain initial access	3	3	1	3	1	11	Medium
Unsecured interfaces	2	2	2	2	2	10	Medium

Table 7: Map countermeasures to STRIDE

STRIDE Categories	Extracted Threats	Countermeasures
Spoofing	Spoofing, impersonation, brute force attack, MITM, masquerade attack, unauthorized access	Authentication solutions
Tampering	Forgery, malicious code injection, physical attack, unsecured interfaces, gain initial access	Detection and identification and authentication solutions
Repudiation	No repudiation threats were mentioned in the selected papers	No counter measures introduced
Information Disclosure	Data leakage, eavesdropping, insecure communication, abuse attack, open ports, replay attack	Secure communication and Blockchain-based solutions
Denial of Service	DoS, DDoS, jamming, or interruption attacks	Detection and identification solutions
Elevation of Privilege	Over privileged, lack of authentication	Authentication solutions

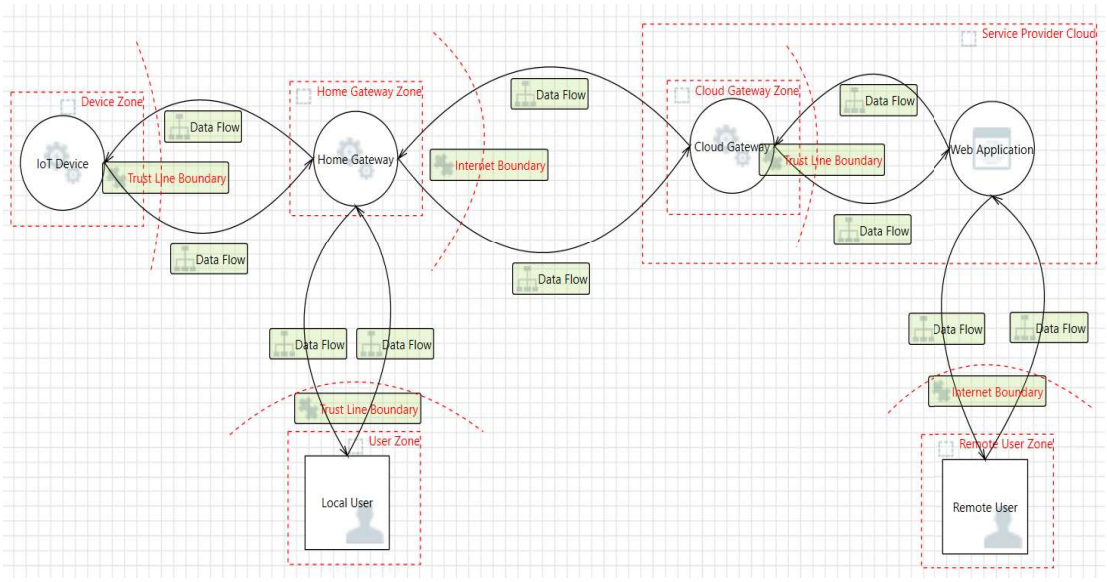

Figure 2: Smart home model

Table 8: STRDE generated threats

Category	**Threat**	**Countermeasure**
Spoofing	Spoofing	Authentication mechanism
Tampering	Forgery	Input validation mechanism
Repudiation	Data repudiation	Logging or auditing to record
Information Disclosure	Sniffing	Encrypting the data flow (secure communication)
Denial Of Service	DoS attack	Input validation mechanism
Elevation Of Privilege	Impersonation	No mitigation provided
Elevation Of Privilege	Code injection	No mitigation provided
Denial Of Service	Interruption of service	No mitigation provided
Elevation Of Privilege	Lack of authorization	Authenticated state-changing requests mechanism

articles have different threat analysis methodologies, and these methodologies are based on threats detected after incidents occurred. These approaches lack identifying vulnerabilities in the system overall when all elements are connected. Using threat modeling in our research simplified threat categorizations and identified the vulnerabilities in the system.

Microsoft STRIDE threat modeling gives threat classification with a simplified viewpoint. Using STRIDE threat modeling simplifies classifying the collected threats into six categories according to the violated security property to cope with heterogeneity in classification presented in the collected studies. Threat modeling identifies vulnerabilities in early stages such as design or deployment, in addition to mapping the countermeasures in a simplified view from the user perspective. It provides a threat rating framework that helps users to stress the highest risks in smart home systems when deployed. The researchers encompassed all threats in the STRIDE model except for repudiation. Although repudiation is important to audit activities in the system, it was overlooked by researchers. Repudiation could be at risk of data forgery. Smart home devices work as a system. It needs a basic element to operate as a communication medium and gateway hub. For this reason, we took a step forward to design a generic smart home system in the STRIDE modeling tool to find vulnerabilities as a whole system. The designed data flow diagram shows not only the risk at elements of the system, but it shows the risk data exposed to when in transition from element to others in the system. The tool generated 9 unique threats across the system. These generated threats are included in the collected threats. Repudiation was recognized as a threat even though it was neglected by studies collected.

7 Limitation of Research Work

The lack of security standardization and hardware limitations resulted in a slow or lack of security practices in these devices.

In this study, we conduct a systematic literature review to identify the exposed threats in the last five years in these devices and introduce novel countermeasures to mitigate the security issues. IEEE, ACM, Scopus, Science Direct, Springer, and MDPI databases were selected for the systematic review but we have to add more database to get more stable results.

The security of smart home devices is a critical part of the design of the product, but device manufacturers do not take it seriously for many reasons. Manufacturers overlook security features to compete in a very competitive market, which allows them to release products faster to prevent the product from being obsolete in a short period.

8 Conclusion and Future Works

In conclusion, this study discussed the security challenges encountered by IoT-enabled smart homes. A survey was conducted to elicit the latest challenges from experts in the field. The result was 22 unique threats that were identified. Because of variations in threats classification STRIDE threat model is used to simplify categorization from the house owner viewpoint. Furthermore, the STRIDE tool is used to design a generic smart home system layout using a dataflow diagram. The design helps with finding threats in the system as a whole, unlike the collected studies. Then a comparison is made between the generated threats from the tool with the extracted threats from the studies. Threat modeling plays a significant role when a house owner decides to design a smart home system. As future work, we are planning to create a framework that enables the user to design a smart home system by selecting the components of the smart home system from a predefined list such as smart lock, smoke detectors, or surveillance camera. This tool identifies the threats for each component by checking the CVE database for vulnerabilities and how to mitigate them. If a threat exists for such a component, the framework enables the user to download the patch to mitigate the issue. Otherwise, the framework suggests a proper mitigation procedure to combat the threat. Also, the framework guides the user on how to configure the available features in devices to enhance security. This method adds an active layer of protection for the smart home system and enhances the overall security of the smart home system.

References

[1] H. Abbas, W. Iqbal and M. Daneshmand, “An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security,” *IEEE Internet of Things Journal*, 7(10):10250-10276 2020. DOI:10.1109/JIOT.2020.2997651.

[2] Zahrah A. Almusaylim and Noor Zaman, “A Review on Smart Home Present State and Challenges: Linked to Context-Awareness Internet of Things (IoT),” *Wireless Networks*, 25:3193-3204, 2019.

[3] P. Aufner, “The IoT Security Gap: A Look Down into the Valley Between Threat Models and Their Implementation,” *International Journal of Information Security*, 19(3):3-14, 2020.

[4] A. Awad and B. Ali, “Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes,” *Sensors*, 18(3):817, 2018.

[5] B. Bastos, S. Shackleton, and M. El-Mosssa, “Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments,” IET: Living in the Internet of Things: Cybersecurity of the IoT - 2018, 7 pp. 2018.

[6] J. M. Batalla and F. Gonciarz, “Deployment of Smart Home Management System at the Edge: Mechanisms and Protocols,” Neural Computing and Applications, pp 1301-1315, 2019.

[7] M. Burhan, R. A. Rehman, B, Khan, and B.-S. Kim, “IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey,” *Sensors*, 18(9):2796-2833, 2018.

[8] Resul Das, Muhammed Zakeriya Gunduz, Analysis of Cyber-Attacks in IoT-based Critical Infrastructure, International Journal of Information Security Science, 8(4):122-133, 2019.

[9] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, “Evaluating Critical Security Issues of the IoT World: Present and Future Challenges,” *IEEE Internet of Things Journal*, 5(4):2483-2495, Aug. 2018. doi: 10.1109/JIOT.2017.2767291.

[10] I. Hmeidi, F. Shatnawi, W. Mardini, and Y. Khamayseh, “Smart Home Is Not Smart Enough to Protect You - Protocols, Challenges and Open Issues,” *Procedia Computer Science*, 160:134-141, 2019.

[11] K. Karimi and G. Atkinson, “What the Internet of Things (IoT) Needs to Become a Reality,” Retrieved June 3, 2020, from https://www.mouser.cn/pdfdocs/INTOTHNGSWP.PDF.

[12] K. Khawla and T. Tomader, “A Survey on the Security of Smart Homes: Issues and Solutions,” *ICSDE'18: Proceedings of the 2nd International Conference on Smart Digital Environment*, pp. 81-87, October 2018. https://doi.org/10.1145/3289100.3289114.

[13] D. Meyer, J. Haase, M. Eckert, and B. Klauer, "A Threat-Model for Building and Home Automation," IEEE 14th International Conference on Industrial Informatics (INDIN), Poitiers, France, pp. 860-866, 2016. doi: 10.1109/INDIN.2016.7819280.

[14] D. Mocrii and Y. Chen, “IoT-Based Smart Homes: A Review of System Architecture, Software, Communications, Privacy and Security,” *Internet of Things*, 1(2):81-98, 2018.

[15] L. O. Nweke and S. Wolthusen, “A Review of Asset-Centric Threat Modelling Approaches,” *International Journal of Advanced Computer Science and Applications*, 11(2):1-6, 2020.

[16] B. A. Omotosho, “Threat Modeling of Internet of Things Health Devices” *Journal of Applied Security Research*, 14(1):1-16, 2019.

[17] OWASP. (n.d.). "Application Threat Modeling," (OWASP) Retrieved July 2, 2021, from https://owasp.org/www-community/Application_Threat_Modeling#.
[18] S. U. Rehman and S. Manickam, "A Study of Smart Home Environment and its Security Threats" *International Journal of Reliability*, Quality and Safety Engineering, 23(3):1640005-1640014, 2015.
[19] R. Shahan and P. Meadows, "Internet of Things (IoT) Security Architecture," (Microsoft), Sept 10, 2018. Retrieved July 4, 2021, from https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture.
[20] N. Shevchenko, "Threat Modeling: 12 Available Methods," Retrieved from SEI Blog - Carnegie Mellon University, December 3, 2018. https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/
[21] A. Shostack, *Threat Modeling: Designing for Security*, Wiley, 2014.
[22] "Smart Home Market Size & Share will hit $53.45 Billion by 2022," April 12, 2017. (Zion Market Research) Retrieved June 3, 2020, from https://www.globenewswire.com/news-release/2017/04/12/959610/0/en/Smart-Home-Market-Size-Share-will-hit-53-45-Billion-by-2022.html.
[23] "Smart home - Statistics & Facts," March 3, 2020). (Statista) Retrieved June 3, 2020, from https://www.statista.com/topics/2430/smart-homes/.
[24] I. Stellios, P. Kotzanikolaou, and M. Psarakis, "A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services," *IEEE Communications Surveys & Tutorials*, 20(4):3453-3495, 2018.
[25] K. Taghizad-Tavana, M. Mohsen Ghanbari-Ghalehjoughi, N. Razzaghi-Asl, and S. Sayyad Nojavan, "An Overview of the Architecture of Home Energy Management System as Microgrids, Automation Systems, Communication Protocols, Security, and Cyber Challenges," *Sustainability*, 14(23):159382022. https://doi.org/10.3390/su142315938.
[26] Y. Yang, L. Wu, G. Yin, and L. Li, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet of Things Journal*, 4(5):1250-1258, 2017.

Abdullah Ali Ben-Nakhi is an Associate Computer Engineer at State Audit Bureau of Kuwait, September 2015 – Present where he completed computing security projects; Servers and virtual machine administrator, Disasters recovery planning, Access control and managing users' permissions on different level of systems, Harden operating systems security, Harden operating webservers security, Prototyping and designing mobile application, Maintaining electronic archiving system and, etc. Mr. Adullah graduated in 2014 from Portland State University, Portland, Oregon, USA. He also completed his master in Computing Information Systems in 2022 and his email: bennakhi1@gmail.com.

Mostafa Abd-El-Barr received his PhD degree from the Department of Electrical and Computer Engineering, University of Toronto, Canada in 1986. He was with the Department of Information Science, College of Computing Sciences and Engineering (CCSE), Kuwait University 2003-2020. He was also an Adjunct Professor with the ECE Department, University of Victoria (UVic), BC, Canada 2009-2020. He is now the Chairman of the Electrical Engineering Department, Badr University in Egypt. His research interests include Information Security, Design and Analysis of Reliable & Fault-Tolerant Computer Systems, Computer Networks Optimization, Parallel Processing/Algorithms, Multiple-Valued Logic (MVL) Design & Analysis, VLSI System Design, and Digital Systems Testing.

He is the author and/or co-author of more than 185 scientific papers published in journals and conference proceedings/symposia. He has three books published (two are translated to the Chinese Language). Professor Abd-El-Barr is a Senior IEEE Member and a member of the International Association of Engineers (IAENG). He is a Senior International Associate Editor of the International Journal of Information Technology & Web Engineering and a member of the Editorial of the International Journal of Computer Science and Security (IJCSS). He is also an official IEEE/EAC/ABET evaluator. Dr. Abd-El-Barr is a Certified Professional Engineer in Ontario, Canada.

Kalim Qureshi is an Associate Professor of Information Science Department, Kuwait University, Kuwait. His research interests include network parallel distributed computing, thread programming, concurrent algorithms designing, task scheduling, performance measurement and medical imaging. Dr. Qureshi receive his Ph.D. and MS degrees from Muroran Institute of Technology, Hokkaido, Japan in (2000, 1997). He published more than 70 journal papers in reputed journals. His email address: kalimuddin.qureshi@ku.edu.kw.