Vulnerability Analysis Model for IoT Smart Home Camera

Asia Othman Aljahdali*, Nawal Alsaidi, Maram Alsafri

College of Computer Science and Engineering, University of Jeddah, Saudi Arabia

Summary
Today's Internet of Things (IoT) has had a dramatic increase in the use of various daily aspects. As a consequence, many homes adopt IoT technology to move towards the smart home. So, the home can be called smart when it has a range of smart devices that are united into one network, such as cameras, sensors, etc. While IoT smart home devices bring numerous benefits to human life, there are many security concerns associated with these devices. These security concerns, such as user privacy, can result in an insecure application. In this research, we focused on analyzing the vulnerabilities of IoT smart home cameras. This will be done by designing a new model that follows the STRIDE approach to identify these threats in order to afford an efficient and secure IoT device. Then, apply a number of test cases on a smart home camera in order to verify the usage of the proposed model. Lastly, we present a scheme for mitigation techniques to prevent any vulnerabilities that might occur in IoT devices.

Keywords:
Smart camera, vulnerability assessment, threats modelling, mitigation.

1. Introduction

The Internet of Things (IoT) is described as the ability of all things to interact with each other and with people. It is defined and discovered as an interconnected network with a clear identifier and the ability to communicate with any entity in any location and at any moment, anywhere and wherever [4]. The Internet of Things is an evolving and transformational model with extensive interest in several applications, including smart homes, smart environments, and remote healthcare. A Smart Home is an automated system home that includes sensors and device controllers to provide a comfortable, intelligent, and secure system for enhancing the quality of care and easily controlling home appliances, particularly for the elderly and disabled people, as shown in Figure 1 [7]. The smart home appears to be one of the most rapidly growing scientific applications in terms of technology. A smart home provides remote services for the user to control electronic devices and appliances in their home. The provision of security and privacy for the home's owner is a significant feature offered in smart homes, and much of the ongoing research in that field focuses on these issues.

Figure 1. IoT smart home

Smart home security is a significant issue that can threaten the privacy and security of users, as hackers can remotely access, monitor, or stop home appliances. Moreover, it is possible to steal the data on these devices. When it comes to cameras or motion tracking systems, where criminals will know when homes are free from owners to become an easy target for theft, the risk of hacking these devices increases. In implementing IoT technologies, security is a critical issue to consider, requiring comprehensive research on the matter. IoT systems need to ensure the safety of human life, avoid the chain of adverse events, achieve the availability, confidentiality, and integrity of information, and authenticate objects using a set of different mechanisms such as passwords, location, and biometrics [12].

We will provide an efficient model that will overcome the existing vulnerabilities in the current smart home system while taking into account all of the above requirements. Moreover, the proposed model will ensure that IoT devices do not compromise users' privacy and security. The aim of this research is to develop a model for cybersecurity assessment purposes. Since there are many cybersecurity risk assessment approaches and models that are still not

Manuscript received July 5, 2022
Manuscript revised July 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.7.28

available or under study, This paper has several objectives to achieve, as listed below:

- Build and design compensative model for IoT smart home assessment.
- Study the privacy aspect of users and its impact in cybersecurity through assessment.
- Fill the gap of recently model and come up with new advanced model.

2. Background

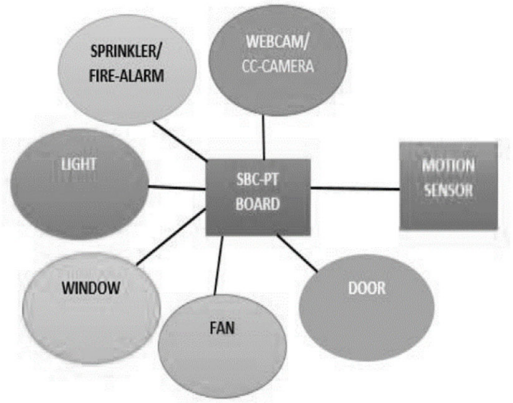
These days, the internet of things (IoT) is becoming more popular in use. The concept of IoT is the interaction between humans and applications using internet connectivity. With the rapid increase in the use of IoT applications, many security concerns are raised readily. Security issues can be defined by the use of the internet, and it plays a major role in security. The general IoT process is divided into four steps. The first step is gathering data from the users, which can be an IoT data source. In the second step, the IoT system processes data based on users' input. Next, data is analysed using some analytics tools such as MapReduce and Spark that analyse and report stored data. Then, the action step is performed, which enables the IoT system to perform actions based on received signals from users; see Figure 2 [9].

Figure 2. IoT process

IoT devices have weak and poor security behaviors if they are not secured well. IoT security focuses on protecting data and networks on the internet of things. If the device is poorly secured, it will affect the nature of the interconnection of IoT devices. Also, when it comes to authentication, it becomes the most significant concern in IoT systems. Authentication can protect you from vulnerabilities such as denial of service attacks. The other concern that IoT technology raises is privacy. It is important to know the user's privacy rights to ensure the users' confidence and assurance while using the IoT system. After addressing the privacy rights, the user will be more comfortable accessing their personal information [1].

3. Related Work

In 2018, Hossain et al. proposed a framework to secure IoT smart homes. They connect motion sensors and other household objects like doors, fans, etc. These sensors are connected to all objects to control the instruments. They use signal broad computers (SBC) to detect sensors, as shown in Figure 5. When a person enters a smart room of a smart home, the sensor is alarmed to perform the action based on received signals. This system has the ability to follow some activities such as lights ON/OFF and doors ON/OFF. In the implementation phase, they use Cisco Packet Tracer to help them with designing the software. Thus, their system is based on controlling all the instruments of a smart home via mobile phone or computer. Also, they highlight that their system is more secure because



they use eye retina scan patterns to detect the owner of the home [5].

Figure 3. A security for IoT based smart home automation system's framework

In 2017, Kang, Moon, and Park proposed an enhanced security framework, which covers both module level and kernel level, as shown in Figure 6. The module level will run the function based on each device, and the kernel level monitors and controls the operation. The framework consists of smart appliances, authentication, and appliance integrity modules. A smart appliance executes a basic function, whereas the authentication module executes access control for all running modules. The appliance integrity module observes all smart device modules. It runs only when the device is signed by the manufacturer by comparing the hash value of the signature with a module name in the list. If the device does not have a manufacturer's signature, it will force an exit [8].

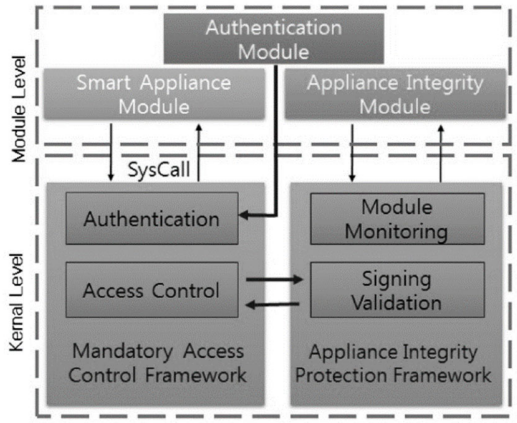


Figure 4. A framework of an enhanced security for home appliances in smart home

In 2019, Chifor, Arseni, Matei, and Bica have designed a framework based on three components: a secure cloud module; an identity bootstrapping module; and a lightweight SDP controller module. The first module acts as an integral part of the cloud platform which is offered by the device manufacturer. The authors assumed that the IoT device's secure cloud (SC) is installed in a secure environment, resulting in a trusted communication link during the registration process. After the registration phase, the SC module starts to mediate between IoT devices and the cloud platform. A user creates a specific policy to address a single or group of IoT devices with an encrypted token.

In the identity bootstrapping module, the second module, authors rely on digital identity to exchange the reliability of IoT devices from the manufacturer's trust domain to the user's trust domain. After the identity bootstrapping, the IoT devices and local network access server obtain a Diffie-Hellman (DH) key. The DH key is used to enhance the security of the IoT network and allows users to send authorized commands to IoT devices. In the lightweight SDP controller module, the last module, the authors used software-defined perimeter (SDP) to obscure the network. They have assumed that each connected device must be authenticated by the SDP controller to establish a connection. This is because the connection might have a malicious risk. A secure connection is established with secure channels like IPSEC to exchange the data with the use of internet key exchange (IKE). This enables users to interact as controllers or trusted third parties between devices and services [2].

A recent study by Sotoudeh et al. has proposed a mechanism to identify and exchange information securely between users and devices. This can record existing objects and services using discovery services and a repository in the directory. These services are connected to a specific main point based on some privileges. The interaction between components in this framework is shown in Figure 7. The authors highlight that vulnerability and threat management is an essential part of security to monitor and detect vulnerabilities. It can deal with threats too [10].

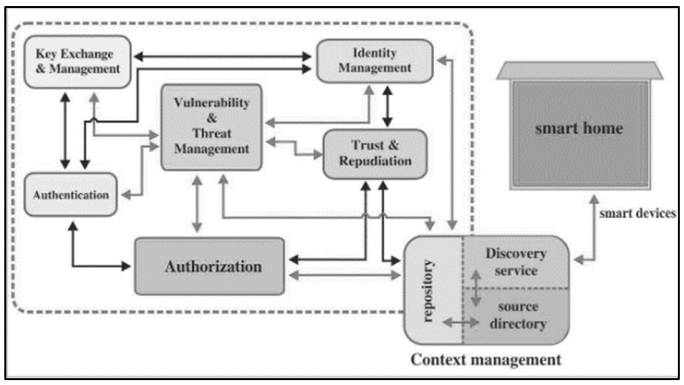


Figure 5. Components of security of IoT-based smart home's framework

4. Critical Analysis

In this section, we will analyze the strengths and limitations of the discussed studies in the related work section. The authors of "A Security Framework for IoT-based Smart Home Automation System" focus on security issues for authentication, such as sensors may detect undesired people. Thus, they add a special feature for hardening, which is the eye retina scan. This increases the security of their framework, but it costs more. It may have a negative rate in scanning as well. Another limitation is using motion sensors since they have some issues. One of these issues is that it may not work as intended due to improper installation. Lastly, this framework can be used by either beginner or expert developers due to the complexity of the framework.

In the "An enhanced security framework for home appliances in smart homes" article, the framework has a medium complexity in understanding the components compared with the security for IoT-based smart home automation systems' framework. Developers must have some knowledge to follow the framework. This framework has a limit in function deterioration because it may lead to device overloading, which results in financial losses such as increasing electricity rates. On the other hand, the strong point of this framework is that it provides integrity by using the encryption algorithm to harden security.

Table 1. Comparison between mentioned security frameworks

Article	Limitations	Strengths
A Security Framework for IoT based Smart Home Automation System	• Costly because the use of retina eye scan. • Motion sensors sometimes have issues. • The negative impact rate in scanning eye retina.	• High- security with the use of eye retina scan. • Faster in recognizing the objects. • The homeowner can monitor all the home appliances remotely by using mobile or computer.
An enhanced security framework for home appliances in smart homes	• Security range is limited because the functions are deteriorated.	• Provide integrity through encryption. • It can provide availability by preventing any malicious actions. • Provide authentication in pairing process. It will check the permission if it is not permitted, it will not be executed.
Security-oriented Framework for Internet of Things Smart-Home applications	• Missing non-repudiation because the scheme shares the same DH key. • Missing IoT devices capabilities in term of energy consumption. • It is not providing a user to smartphone authentication. • It is only for experienced users.	• More secure because it relies on secure communication channels. • It provides authentication of smartphone to IoT devices.
Security Framework of IoT-Based Smart Home	• The authors did not take into their account the issues of cloud platform.	• A proper use of vulnerability and threat management. • Context management for identifying the information privacy. • It provides distributed authorization between smart home and smart health.

The complexity of the framework of "Security-oriented Framework for Internet of Things Smart-Home applications" comes from its complex structure. Since it should be used by an experienced developer who has enough knowledge of how a security framework can be used, It provides an authentication of smartphones to IoT devices but does not offer an authentication for users' smartphones. Also, it uses a secure communication channel, which is IPSEC, to add more security to the framework. The limitation of this framework is using the same shared Diffie-Hellman key, and this will miss the use of non-repudiation security goal.

The framework of the "Security Framework of IoT-Based Smart Home" has no complexity since any developer can use it even without knowledge. The designers of this framework did not solve the security issues of cloud platforms, such as compromising credentials, but they tried to mitigate this issue with the use of context management. It can manage the system's vulnerability and threats by enhancing the privacy of its information. Table 1 summarizes the limitations and strengths of each of the studies discussed.

5. Proposed Model

In general, our proposed model provides security tests for IoT smart home devices, including ensuring use of a secure protocol, checking input validation and filtering, authentication of entities, session, and password management, discovering vulnerabilities and threats, and hardening of systems against attack.

*Ensure use of a secure protocol***.** The primary goal of network security protocols is to prevent unauthorized users, applications, services, or devices from accessing network data. This holds true for nearly all data types, regardless of the network medium. Among the most widely used network

Manuscript received August 2005.
Manuscript revised August 22, 2005.

security protocols are Secure Hypertext Transfer Protocol (HTTPS) and Secure Socket Layer (SSL).

Check input validation and filtering. Input validation is the process of thoroughly testing any input provided by a user or program. Input validation prevents incorrectly formed data from accessing an information system. *Authentication of entities* is a process of verifying the claimed identity of a network in several ways, such as using multi-factor authentication features, one-time password, or OTP to ensure authenticity. *Session and password management* refers to the method of securely managing several requests from a single user or entity to a web-based application or service. Typically, a session is initiated when a user authenticates their identity with a password or another authentication protocol.

Discovering vulnerabilities and threats is understanding the risk of a system by identifying, classifying, remediating, and mitigating weaknesses in an IT environment. It also includes discovery, reporting, prioritization, and response to vulnerabilities in your network.

*Hardening of systems against attack***.** More enabled features mean more potential exploits and decreased security. The goal of system hardening is to reduce security risk by eliminating potential attack vectors and condensing the system's attack surface, such as turning off all unnecessary services by default.

The proposed security model consists of four main components to accomplish the required security function for secure access to IoT smart home devices. These elements are registration, authentication, discovery, and data transmission. registration mechanism allows the integration of new smart objects based on different technologies. After devices are registered, the authentication process is carried out based on verifying the identity of the users using a proper authentication method. The registration and authentication processes share the same key, identity, and context management with the use of either the authentication manager or the registration manager.

The discovery process depends on two types of servers: app web servers and smart home servers. The App web server is used to deploy secure applications that restrict internet access to the applications. The smart home server is responsible for transmitting data to a smart home device through the transmitting channel as intended. The last component is data in transit, which represents a secure channel between a smart home server and devices for exchanging data. Refer to Figure 6, which explains the flow of data in the model.

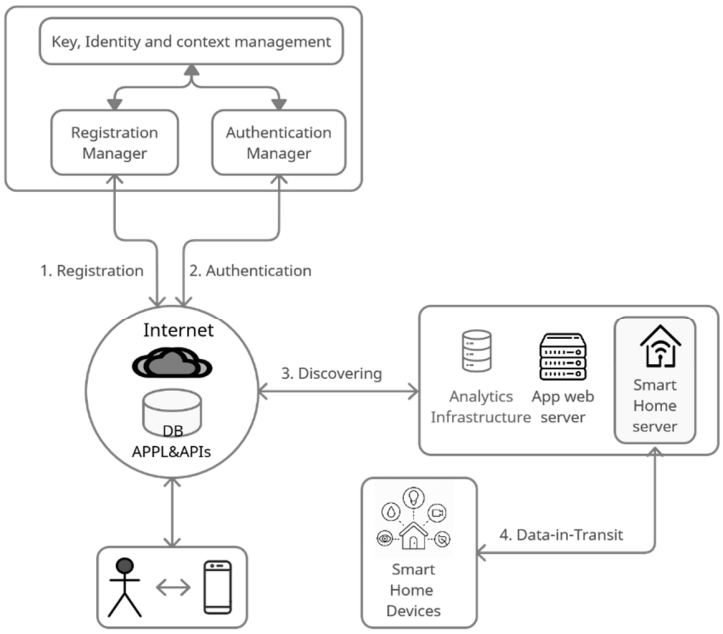


Figure 6. Comments of the Proposed Model

5.1 Threats Modelling

First, we will briefly describe how IoT devices work. IoT devices have sensors and mini-computer processors that interact with collected data by the sensors using machine learning. Basically, IoT devices are connected to the internet, so they will be vulnerable to some malware and attacks [11]. In our suggested model, we will use a camera as a smart home device. Figure 7 presents the components of the smart home camera: the camera itself, the web interface, and the cloud server that the user interacts with. We divided the components into three tiers: top, middle, and bottom tier based on the attack surface of the smart home camera with a dotted line. An attack surface in threat modelling can analyse the risk area in the system and make developers aware of what parts of the system are vulnerable to attack.

After describing the smart home camera structure, we have some assets that need to be protected against any attacks on the smart home camera, which are:

Asset 1: Personal information like the user's home address, phone number, etc.

Asset 2: User Credentials, which consist of a username and password for the smart home system.

Asset 3: Video, picture, and voice information that is transmitted from the smart home devices to the web application either directly or through the server.

We used the STRIDE approach to identify threats in IoT smart home cameras, which helped us identify the types of attacks that smart home cameras commonly face. STRIDE stands for spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. The STRIDE threats concerned about important properties that any developers would like to have in their system: authentication, integrity, non-repudiation, confidentiality, availability, and authorization [10]. Table 2 shows the STRIDE and how the attacker pretends to be in a role.

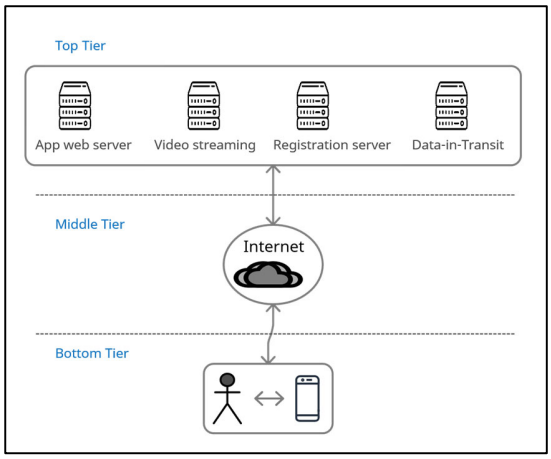


Figure 7. IoT Smart Home Camera Structure

5.2 Walkthrough the Model

In this section, we will present the proposed model for vulnerability analysis of IoT smart home cameras. We have distributed the threats based on the top, middle, and bottom tires of the camera's structure and linked them with the STRIDE threats that we have described previously. As shown in Table 3, the model is based on the Web Application Security Project (OWASP) security testing guide V4.2 to test threats in smart home cameras. The proposed model would help the analyst or developer to harden the smart home camera by finding the vulnerabilities and then mitigating these threats.

6. Case Studies

After developing the vulnerability assessment model, the next phase is to test the efficiency of the proposed model by applying it to a camera device to verify its usage. When the test is done, a description of prevention techniques to harden the tested smart home camera system is given after applying the proposed model. To apply pen testing, we have used an indoor smart camera to discover the vulnerabilities. The selected camera supports Wi-Fi technology for image, video, and audio streaming. It also has some features like motion detection and tracking, and it is capable of working on IOS and Android platforms. We have used a special app provided with the smart camera for connecting a smart home device to the company's cloud server. It allows the user to access its services at any time and from any location. It has the functionality of protecting, capturing, sharing, and saving what the user needs. Lastly, this app helps in installing the camera on the IOS platform to start pen testing.

Burp Suit Professional is used for penetration testing. It is an advanced tool kit for testing web security. It enables the analyst to find vulnerabilities that exist in a web application. With the use of the burp suit professional version, the analyst can minimize false positives by finding many invisible vulnerabilities. Finally, after completing the pen testing process, it produces the reports of discovered vulnerabilities in a simple way, and it simplifies the documentation and remediation process. Additionally, we have used Testssl.sh, which is a free command-line tool that can be used in penetration testing. This tool checks the server's services for any ports that support the TLS/SSL protocol. Also, using this tool will enable the tester to discover the vulnerabilities of weak encryption on any port.

6.1 Testing Analysis and Evaluation

To test the proposed model's efficiency, we applied the model to a smart home camera. We have installed the camera and started the penetration testing accordingly via Burp Suit Pro software based on the proposed model. The result of the testing is summarized in Table 4.
The number of vulnerabilities found using the proposed threat model and the smart-camera model on smart homes indicates the effectiveness of the analytical model components and test cases. Table 5 depicts the smart-camera research model in general as well as the vulnerabilities that were discovered.

6.2 Summary of the Result

In this section, we would present the vulnerabilities that have been found in the camera:

- **URL session hijacking**

Session Hijacking is a type of attack that takes advantage of the web session control mechanism, which is usually used to handle session tokens. A session token is usually a variable-length string that can be used in a variety of ways, including the URL, the header of the http request

as a cookie, other sections of the header of the http request,
or the body of the http request.

Table 2. The STRIDE Threats

	Threat	Property violated	What the attacker does
S	Spoofing identity	Authentication	• Unauthorized access to a user's credentials can be done by an attacker who can retrieve the account information by brute-forcing the user's account passwords
T	Tampering with data	Integrity	• Tampering with video, picture, and voice information: attackers can gain access to this information, and he/she can reset, remove, or edit this stored information.
R	Repudiation	Non-repudiation	• The attacker can use another's account information to gain access to the smart home camera
I	Information disclosure	Confidentiality	• Sensitive data exposure: attackers can steal any exchanged data with the browser by capturing it, such as credit cards, user identities, and so on.
D	Denial of service	Availability	• When an attacker makes several requests to the target server, overloading it with traffic until the target cannot respond or crashes, legitimate users are unable to access the system
E	Elevation of privilege	Authorization	• Injection: attackers can execute unintended commands or access sensitive data without proper authorization.

Table 3. Model Test Cases

Tiers	Threat Imposed	Security Test Case Name	Security Test Case Objectives	Test Case Description
Top Tier	Tampering with data	Business Logic Test	Test Integrity Checks *4.10.3	• It tests the data integrity to check if the users can make changes or not.
	Information disclosure	Testing for weak cryptography	Testing for Sensitive Information Sent via Unencrypted Channels *4.9.3	• Testing whether the sensitive data is protected when transmitted over the network.
	Elevation of privilege	Authorization Testing	Testing for Privilege Escalation *4.5.3	• It tests the privilege escalation attacks to know what the degree of escalation is authorized for each user.
Middle Tier	Denial of service	Input Validation Testing	Testing for code injection *4.7.11	• It assesses the level of severity of the injection to protect against injection attacks that can lead to DOS attacks, too.
Bottom Tier	Spoofing identity	Identity management testing	Testing for Account Enumeration and Guessable User Account *4.3.4	• It tests the authentication mechanism to verify if it is possible to guess the credential information or not.
	Repudiation	Identity management testing	Testing for Weak or Unenforced Username Policy *4.3.5	• It tests the application's error message to see if it is permitting account enumeration or not, to protect against non-repudiation.

*Section number in OWASP testing guide.

Table 4. Model applied to camera

Security Test Case Name	The selected Camera Test Case Comments
Top Tier	
Business Logic Test	• We did a test for session token handling, and we were able to hijack user sessions because tokens are disclosed.

Testing for weak cryptography	• We tested the TLS protocol using the Test SSL tool and found a weak encryption of TLS 1.0, 1.1, and 1.2.
Test for privileges escalation	• N/A • We could not perform privilege escalation through the cookies. We did test the cookies by only trying to manipulate the cookies.
Middle Tier	
Testing for code injection	• We use crafted input to modify user information in the code and inject arbitrary code that will be executed by the server. As a result, this demonstrates that user data is not strictly validated.
Bottom Tier	
Identity management testing (Testing for Account Enumeration and Guessable User Account)	• We brute forced the username with a list of passwords that were generated by the user itself, and we got one with a 302 response. This suggests the login attempt was successful.
Identity management testing (Testing for Weak or Unenforced Username Policy)	• N/A • We could not enforce weak or unenforced username policies. We did test by trying to change the password to '123123' but the website rejected this change due to its application of a policy for passwords. (includes 8-digit and mixed-character numbers, as well as aliphatic and special characters)

Table 5. Model and test case evaluation

Tiers	Threat Imposed	Security Test Case Name	Vulnerabilities Discovered
Top Tier	Tampering with data	Business Logic Test	Session hijacking in URL
	Information disclosure	Testing for weak cryptography	TLS cookie without secure flag
	Elevation of privilege	Authorization Testing	No privilege escalation
Middle Tier	Denial of service	Input Validation Testing	Code injection with username
Bottom Tier	Spoofing identity	Identity management testing	Flaw in account enumeration with users' password
	Repudiation	Identity management testing	Adequate password policy

After testing the underling camera using Burp Suite, we were able to find the session token. This vulnerability is classified as medium severity. In Figure 8, the URL in the request appears to contain a session token within the query string:

https://p28caldav.icloud.com/mm/sub?token=6fdacae2add0860e552485067692cbe2afe7be2ebb09a444ad89c8ba00b4a40e&key=932585515

Request

Figure 8 Session's request

As a result, this sensitive information contained in the URLs can be used to log in to a variety of places,

including the user's browser, the web server, and any forward or reverse proxy servers that exist between the two endpoints. Users can also view URLs on their screens, bookmark them, and send them via email. When off-site links are followed, their contents can be revealed to third parties via the referrer header. The probability of an attacker capturing session tokens increases when they are included in the URL.

- **TLS cookie without a secure flag**

If the user visits any HTTP URLs inside the cookie's reach, the cookie will be transmitted in plain text. An attacker can trigger this event by providing appropriate links to the user, either directly or via another website. Even if the domain that provided the cookie does not host any

HTTP-accessible content, an attacker may be able to execute the same attack by using the form's links.

After testing the underling camera using Burp Suite, we were able to detect TLS cookies without a secure flag in the camera website. This vulnerability is classified as medium severity. The following cookie was issued by the application and does not have the secure flag set: JSESSIONID, so, the cookie appears to contain a session token, which could raise the risk of this issue. See figure 9. To take advantage of this flaw, an attacker must be in a position to eavesdrop on the victim's network traffic.

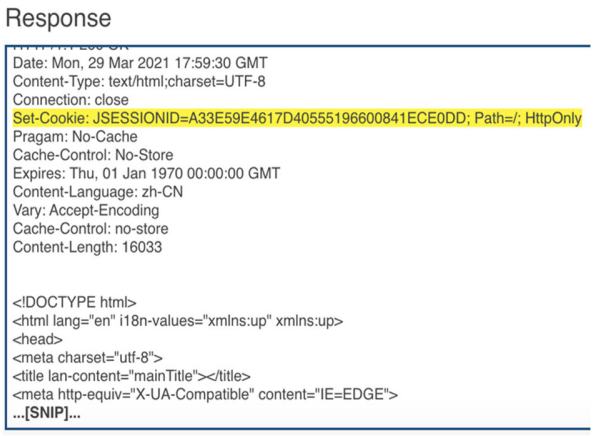


Figure 91 TLS cookie response

- **Code injection with username information**

Code injection is injecting code that is then interpreted/executed by the target program. This form of attack takes advantage of the way untrusted data is handled. These attacks are normally possible because of a lack of proper input/output data validation, such as: amount of expected data, allowed characters, and data format. Figure 10 shows the personal information that we injected into it with malicious code.

Figure 102 Targeted personal information

Here is an example of detecting code injection flaws in underling camera software that we are testing using Burp Suite.

Username=Maram&indexCode=nbxs9s&category=0&contact=&area=110101&companyAddress=&phone=96659484xxxx

We edited the phone parameters, then we were able to affect the response below:

Username=Maram&indexCode=nbxs9s&category=0&contact=&area=110101&companyAddress=&phone=966552183xxxx

Username=Maram&indexCode=nbxs9s&category=0&contact=&area=110101&companyAddress=&phone=isFinite(0)

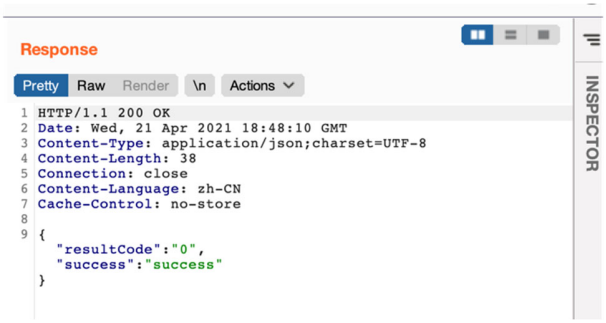


Figure 11 Response of code injection

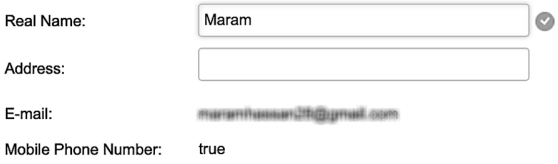


Figure 12 Injected mobile number successfully

The isFinite() function checks if the value passed in is a finite number of characters. True indicates that user data is not strictly validated, allowing an attacker to manipulate the code to be executed and insert arbitrary JavaScript code into the server.

- **Flaw in account enumeration with users' password**

Web applications often expose the existence of a username on the system, either as a result of misconfiguration or as a design decision. When we send incorrect credentials, for example, we can receive a message stating that either the username is already in use on the system, or the given password is incorrect. This information could be used to launch a brute force or default username and password attack against the web application.

We were able to detect a flow in account enumeration with users' passwords after applying the proposed model and testing the underling camera website using Burp Suite. We will perfume the following steps:

- Run the burp to investigate the login page and submit an invalid username and password.
- Then go to the "Proxy" tab, then "HTTP history" and find the POST/login request and send this to Burp Intruder.
- In the Intruder tab, go to the "Positions" and select the "Sniper" attack type.
- Add a payload position to the password parameter like this:

username=MaramH &password=§Mmm12345§

- On the "Payloads" tab, select "Simple List" and paste candidate passwords, then click "Start attack".
- When the attack was finished, we got one with a 302 response. This suggests the login attempt was successful.

6.3 Mitigation Techniques

After applying the proposed model and performing penetration testing to identify vulnerabilities, we suggest mitigation techniques for each vulnerability. In the proposed model, this is the last step that needs to be followed to have a secure and efficient application. Table 6 summarizes the mitigation techniques for the vulnerabilities that have been discovered in the tested device.

Table 6 Mitigation techniques applied to proposed model

Tiers	Threat Imposed	Security Test Case Name	Security Test Case Objectives	Mitigation Techniques
Middle Tier	Denial of service	Input Validation Testing	Testing for code injection	• Sanitizing and validating the user input. • Treat all data as untrusted in a place where the user can enter or edit any data.
Bottom Tier	Spoofing identity	Identity management testing	Testing for Account Enumeration and Guessable User Account	• During the login process, an application should return an error message in response to an invalid username or other account information. • Delete the default and testing accounts before releasing the application.
	Repudiation	Identity management testing	Testing for Weak or Unenforced Username Policy	• During the login process, an application should return an error message in response to an invalid username or other account information.

7. Conclusion

Smart home systems are one of the most critical aspects of the Internet of Things (IoT). Applying IoT technology to smart homes yields many security concerns, since they're vulnerable to many security threats. Therefore, we followed an appropriate test guide to help us in designing the proposed model. The test guide is an OWASP web security testing guide to assist in identifying the security risks of IoT-based smart homes. Since we cannot afford a new vulnerability analysis model for the developers, we designed a mitigation technique in order to harden the IoT devices for each security threat in our proposed model.

References

[1] Aldowah, Hanan, Shafiq Ul Rehman, and Irfan Umar. "Security in internet of things: issues, challenges and solutions." International Conference of Reliable Information and Communication Technology. Springer, Cham, 2018.

[2] Chifor, Bogdan-Cosmin, et al. "Security-oriented framework for internet of things smart-home applications." 2019 22nd International Conference on Control Systems and Computer Science (CSCS). IEEE, 2019.

[3] Devi, T. Rajani. "Importance of Testing in Software Development Life Cycle." International Journal of Scientific & Engineering Research 3.5 (2012): 1-5.

[4] Gan, Gang, Zeyong Lu, and Jun Jiang. "Internet of things security analysis." 2011 international conference on internet technology and applications. IEEE, 2011.

[5] Hossain, Nazmul, et al. "A Security Framework for IoT based Smart Home Automation
[6] System." Global Journal of Computer Science and Technology (2018).
[7] Jabbar, Waheb A., et al. "Design and implementation of IoT-based automation system for smart home." 2018 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2018.
[8] Kang, Won Min, Seo Yeon Moon, and Jong Hyuk Park. "An enhanced security framework for home appliances in smart home." Human-centric Computing and Information Sciences 7.1 (2017): 1-12.
[9] Marjani, Mohsen, et al. "Big IoT data analytics: architecture, opportunities, and open research challenges." ieee access 5 (2017): 5247-5261.
[10] Shostack, Adam. Threat modeling: Designing for security. John Wiley & Sons, 2014.
[11] Sobin, C. C. "A survey on architecture, protocols and challenges in IoT." Wireless Personal Communications 112.3 (2020): 1383-1429.
[12] Sotoudeh, Shahrouz, Sattar Hashemi, and Hossein Gharaee Garakani. "Security Framework of IoT-Based Smart Home." 2020 10th International Symposium on Telecommunications (IST). IEEE, 2020.

Asia Othman Aljahdali She received her Ph.D. degree in computer science at Florida State University in 2017 and a master's degree in information security in 2013. Later on, she worked at King Abdul-Aziz University as an assistant professor. Then, she worked at the University of Jeddah as an assistant professor in the cybersecurity department. In 2020, besides her academic work, she worked as a cybersecurity consultant for the administration of cybersecurity at Jeddah University. . In 2022, she worked as an associate professor at the University of Jeddah. Her current research interests include information security, cryptography, data hiding, network security, IoT security, and cloud security.

Nawal Alsaidi received her bachelor's degree in information technology (IT) from King Abdul-Aziz University (KAU), and her master's degree at Jeddah University (JU) from the cybersecurity department, KAS. Her current research interest include IoT security, and blockchain technology.

Maram Alsafri received her bachelor's degree in information technology (IT) from King Abdul-Aziz University (KAU), and her master's degree at Jeddah University (JU) from the cybersecurity department, KAS. Her current research interest include information security, and IoT security.