https://doi.org/10.37528/FTTE/9788673955056/POSTEL.2025.23

POSSIBILITIES OF UNAUTHORIZED DATA COLLECTION IN THE SMART HOME ENVIRONMENT

Ivan Cvitić, Dragan Peraković, Mihaela Maturanec
University of Zagreb - Faculty of Transport and Traffic Sciences,
ivan.cvitic@fpz.unizg.hr, dragan.perakovic@fpz.unizg.hr,
mihaela.maturanec@gmail.com

Abstract: *The increasing adoption of Internet-connected devices exposes smart home users to security challenges and threats. Therefore, it is important to pay attention to the collection of user data in the smart home environment. The purpose of this research is to show smart home users in which ways it is possible to collect and use their data in such an environment. The research is based on the collection of data from IoT devices within the smart home environment and on the display of unauthorized data collection, that is, the display of attacks that can occur in the smart home environment. The data set on intrusions into the IoT network was used for research. For this network dataset, the authors created different types of network attacks in an IoT environment for academic purposes. Two typical smart home devices were used: an intelligent voice assistant and a smart camera. Research results show where: Man-in-the-middle attacks, SYN, UDP, ACK and HTTP flooding attacks occurred*.

Keywords*: data collection; smart home; Internet of Things; digital forensics; cyberthreats*

1. Introduction

A smart home can be defined as a place that includes a series of sensors, systems, and devices that can be remotely accessed, controlled, and monitored via a communication network. However, the increasing use of internet-connected devices exposes smart home users to security challenges and threats. Therefore, it is important to pay attention to the collection of user data in the smart home environment.

In addition to the convenience and automation benefits, the integration of numerous IoT devices within smart homes introduces new layers of privacy and security risks. Many devices operate continuously, exchanging data with cloud platforms and external servers, often without the user’s explicit awareness or consent. Even when encrypted communication is used, metadata such as connection timing, frequency of access, or device identifiers can be exploited to infer user behavior patterns and household activities. Furthermore, the lack of standardized security protocols and insufficient authentication mechanisms increase the potential for unauthorized data interception and misuse. Understanding these risks is crucial for designing safer smart home ecosystems and raising awareness among users about possible forms of unauthorized data collection and surveillance. The purpose of this research is to show smart home users in what ways their data can be collected and used in such an environment.

Based on the identified challenges and security threats, the structure of this paper is designed to provide users and researchers with a comprehensive overview of the problem and the results of the conducted analysis. Following the introductory section, Chapter 2 presents an overview of previous research relevant to security and privacy in the smart home environment. Chapter 3 analyzes key vulnerabilities of typical smart home devices, with emphasis on smart cameras and intelligent voice assistants. Chapter 4 outlines the research methodology and presents the results of experimental attacks and network traffic analysis. Finally, the conclusion summarizes the main findings and highlights the need for enhanced security mechanisms and more responsible use of IoT technologies in smart homes.

2. Previous research

IoT devices present security challenges because most of them do not have built-in encryption. In addition, they can serve as access points for sensitive data. Manufacturers of smart home devices and platforms collect consumer data to better customize their products and offer new and improved services to customers. However, many smart homeowners are concerned about the privacy of their data. As IoT devices become more ubiquitous, clarifying their privacy implications is of utmost importance so that users are aware of privacy risks and can minimize these risks [1].

Participants in research often assume that their privacy is protected by device manufacturers [2]. Other works highlight the privacy implications of the large volumes of data generated by smart devices in smart homes, frequently without explicit user consent or awareness of how this data is used [3]. It is said that information security has become a social problem because it is not so much what users use that causes difficulties, but the way they use devices. Video cameras are viewed as the most privacy-intrusive sensors, followed by microphones [4].

In addition to privacy concerns, several studies have examined security risks and vulnerabilities of IoT devices that may lead to unauthorized data access. A classification of IoT security risks by architectural layers identifies the physical, network, and application layers as the most exposed [5]. Detection approaches for DDoS (Distributed Denial of Services) attacks applicable to resource-constrained IoT devices such as smart cameras and voice assistants are also documented [6]. An overview of IoT-generated DDoS detection methods further emphasizes the importance of analyzing network-behavioral patterns to identify malicious communication from compromised smart devices [7].

This research aims to provide an overview of the vulnerabilities of smart devices in a smart home environment. As a result, malicious attacks on smart devices in the smart home environment that have been performed can be displayed.

3. Vulnerabilities of smart devices in a smart home environment

This chapter provides an analysis of the vulnerabilities of smart cameras and intelligent voice assistants used in a smart home environment. The main types of threats to smart cameras are unauthorized download of video surveillance, unauthorized intrusion into the smart camera, unauthorized account theft, and unauthorized data recording. The most common vulnerabilities of intelligent voice assistants are: constant listening to conversations, weak authentication, replay attacks and integration of IoT devices. The mentioned vulnerabilities of smart cameras and intelligent voice assistants will be described in more detail in the rest of this paper.

3.1. Smart camera vulnerabilities

Smart home surveillance cameras are widely used and come from various manufacturers. They are typically used to monitor a home while the users are not present. The cameras can be used for internal or external security. However, they can also cause harm to property or the lives of people using them. According to [8], the main types of threats in a smart camera system are shown in Table 1.

Table 1. Main types of threats in a smart camera system [8]

Threat	Threat description
Unauthorized download of video surveillance	A malicious attacker can obtain video surveillance by capturing traffic exchanged between the smart camera and other destinations.
Tampering with a smart camera	A malicious attacker can collect information about the device, reboot it, access the device's system logs, or remove external storage.
Unauthorized account theft	A malicious attacker can access user account passwords through a brute force attack.
Unauthorized data recording	Poorly designed Android app can compromise personal data

Table 2. Smart camera vulnerabilities [8]

Vulnerability	Vulnerability description
Unauthorized download of video surveillance	- unencrypted video surveillance - encrypted video surveillance that has poor key management - launching a MiTM (Man in the Middle) attack.
Tampering with a smart camera	- open port running an outdated version of dnsmasq, accessible websites revealing system information - use of default credentials with username = "admin"; password = "admin" during setup - user videos exposed via external removable storage, devices may be put into an insecure state.
Unauthorized account theft	- No password policies and no-account lockout mechanisms
Unauthorized data recording	- incorrect implementation of the SSL (Secure Socket Layer) protocol that caused video surveillance to be exposed and enabled MiTM attacks - data revealing the user's identity was leaked due to poor developer logging mechanisms.

The first and fourth threats represent a breach of user confidentiality and privacy, while the second and third threats jeopardize the availability of smart cameras as well as user confidentiality. Table 2 will show the vulnerabilities discovered in the research [8] according to the above types of threats.

When they are connected, the vulnerabilities allow an attacker to remotely control the camera, download images and decrypt them. Exploitation of these vulnerabilities can pass authentication and potentially execute code remotely, further compromising the integrity of affected cameras.

3.2. Vulnerabilities of intelligent voice assistants

Intelligent Voice Assistants (IVAs) are Internet-connected devices that listen to their environment and respond to the user's spoken commands to retrieve information from the Internet, control household devices, or notify the user of incoming messages and reminders. Although they are ubiquitous in the smart home environment, their presence raises concerns about user security and privacy as they monitor the user in their smart home. To justify the trust placed in the devices, they must be secure from unauthorized access. The backend infrastructure responsible for speech analysis and conversion to text, interpretation of commands, and connectivity to other services and devices must maintain data confidentiality [9].

The most common vulnerabilities of intelligent voice assistants are constant listening to conversations, weak authentication, replay attacks and integration of IoT devices [9].

Research [9] has revealed that continuous monitoring of sound through the integrated microphones of intelligent voice assistants creates a potential violation of the user's personal privacy. Although a device that supports intelligent voice assistants records the user's voice and transmits the recording to the cloud only when the wake word is spoken, i.e., when the assistant is launched, the device still continuously monitors conversations and typical sounds around the device. If a malicious attacker gains access to a compromised, enabled intelligent voice assistant, all recorded sounds or voices can be sent to the attacker in real time. Continuous recording of sounds surrounding an intelligent voice assistant allows for non-attack-based intrusion. Although Amazon, Apple, Google, and Microsoft claim that their devices record only when users speak a command to wake up the assistant, according to [7] there has been at least one incident where the device recorded and sent recordings back to the vendor at times when the user did not use the wake word to wake the device. In such cases, it is easy for the vendor to analyze the user's conversations and create a profile of the user's typical daily activities using household noise analysis. It is even possible to associate a user's location using IP address and geolocation data.

Due to weak authentication, intelligent voice assistants do not have the ability to determine whether they are being operated by the owner or another authorized party with a wake word. Anyone with access to a voice-activated device could ask it questions and collect information about the services and accounts associated with the device. A malicious attacker who comes close to a targeted intelligent voice assistant can potentially trick the system into believing that the real owner is speaking to it. This allows the attacker to access calendar details, email, and other personal information [10].

A consequence of weak authentication of an intelligent voice assistant can be that synthesized speech imitating a legitimate user makes the device vulnerable to replay attacks. Replay attacks can be achieved by recording authorized users or synthesizing a reasonable approximation of their voice. This works in such a way that silent signals can be incorporated into the audio signal of a TV or radio broadcast to attack multiple targets simultaneously. These attacks can be used to take control of a user's device and perform unauthorized actions, such as making phone calls, thereby allowing personal information to be sent to a medium controlled by the malicious attacker [10].

According to research [10], vulnerabilities arising from the integration of IoT devices with intelligent voice assistants are considered. When the network is attacked, an attacker can direct the infected device to send spoofed Address Resolution Protocol (ARP) messages. The goal is to associate the MAC address of the smart mobile device with the IP address of the default gateway and direct the network traffic to be sent to the attacker. In this way, the attacker can inspect packets and collect information without being detected, by sending traffic to the real default gateway. After a software agent is installed on a personal computer to access the surveillance system from the web interface, the credentials are sent over the network without HTTPS encryption. This allows the malicious gateway to access the credentials and allows the attacker to access the surveillance system. The attacker can change the configuration of the surveillance system so that it can be accessed from the Internet [10].

4. Research methodology and results

The research is based on the collection of data from IoT devices within the smart home environment and on the display of unauthorized data collection, i.e. the display of attacks that can occur in the smart home environment. The IoT network intrusion dataset was used for research. For this network dataset, the authors created different types of network attacks in an IoT environment for academic purposes. Two typical smart home devices were used: SKT NUGU (NU 100), an intelligent voice assistant and EZVIZ Wi-Fi smart camera (C2C Mini O Plus 1080P). All devices used, including some laptops or smart mobile devices, were connected to the same wireless network. The network data set consists of 42 raw network packet files (eng. Packet Capture - pcap) at different time points. Packet files were collected using wireless network adapter mode and wireless headers are stripped by Aircrack-ng. All attacks except the Mirai Botnet category are packets captured during attack simulation using the Nmap software tool. In the case of the Mirai Botnet category, attack packets were generated on a laptop and then manipulated to appear to originate from an IoT device [11].

4.1. Man-in-The-Middle – ARP spoofing attacks

A MiTM attack was carried out on the example of the EZVIZ smart camera. By analyzing network traffic, it is possible to show that such an attack has occurred. The attack was analyzed in the Wireshark program and the packets representing the attack are displayed. The EZVIZ smart camera has its IP address: 192.168.0.13 and MAC address: bc:1c:81:4b:ae:ba. When a MiTM attack occurs, it is visible that the MAC address has changed. This is visible in Figure 1. The warning that one IP address has two MAC addresses is shown in yellow, which is usually not the case except in the case of a MiTM attack.

```
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Apple_5e:ff:9f (f0:18:98:5e:ff:9f)
    Sender IP address: 192.168.0.16
    Target MAC address: SichuaniLink_4b:ae:ba (bc:1c:81:4b:ae:ba)
    Target IP address: 192.168.0.13
v [Duplicate IP address detected for 192.168.0.16 (f0:18:98:5e:ff:9f) - also in use by 48:4b:aa:2c:d8:f9 (frame 1322)]
  > [Frame showing earlier use of IP address: 1322]
    [Seconds since earlier frame seen: 1]
v [Duplicate IP address detected for 192.168.0.13 (bc:1c:81:4b:ae:ba) - also in use by f0:18:98:5e:ff:9f (frame 1322)]
  v [Frame showing earlier use of IP address: 1322]
    v [Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.0.13)]
        [Duplicate IP address configured (192.168.0.13)]
        [Severity level: Warning]
        [Group: Sequence]
    [Seconds since earlier frame seen: 1]
```

Figure 1. Man in The Middle attack [11]

In addition to the EZVIZ smart camera, the MiTM attack was also carried out on the SKT NUGU intelligent voice assistant. SKT NUGU device has IP address: 192.168.0.24 and MAC address: 04:32:f4:45:17:b3. When the packets are filtered, it can be seen that the source address is: 88:36:6c:d7:1c:56, and the destination address is from the SKT NUGU device. In Figure 2, the conversations option is visible, where it is visible that the MAC address: f0:18:98:5e:ff:9f appears, which represents a MiTM attack, i.e. that communication is now transmitted via the last-mentioned MAC address.

Ethernet · 3 | IPv4 · 17 | TCP · 107

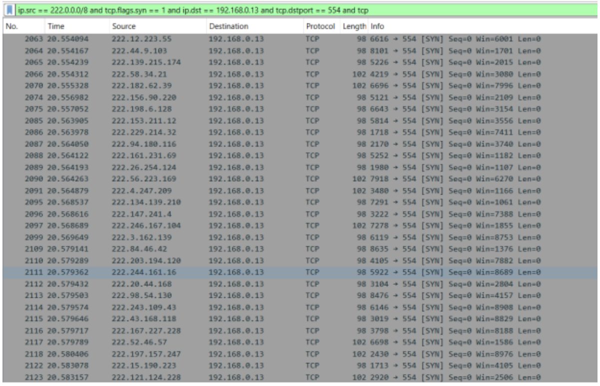
Address A	Address B	Packets	Bytes
f0:18:98:5e:ff:9f	db:3b:f4:45:17:b3	1	2 kB
f0:18:98:5e:ff:9f	04:32:f4:45:17:b3	13.208	13 MB
88:36:6c:d7:1c:56	f0:18:98:5e:ff:9f	2	3 kB

Figure 2. Conversations option [8]

4.2. DoS SYN flooding attacks

By analyzing the network traffic of the EZVIZ smart camera, it is possible to demonstrate the SYN flooding attack method. In a SYN flooding attack, the attacker sends many SYN packets to the server, using different, fake IP addresses. This is visible in Figure 3. It can be seen that many SYN packets are sent in a very short period of time to the same port 554, to the destination address of the smart camera.

The SYN flooding attack method was also implemented on the SKT NUGU intelligent assistant. In addition to the previously mentioned methods, a SYN flooding attack can also be recognized using the TCP Retransmission option in the Wireshark program. In this attack, TCP Retransmission means the attacker resends the TCP SYN packet to the target device without completing the TCP three-way handshake. In this case, it refers to the NUGU device located on port 19 604. This is shown in Figure 4.



ip.src == 222.0.0.0/8 and tcp.flags.syn == 1 and ip.dst == 192.168.0.13 and tcp.dstport == 554 and tcp

No.	Time	Source	Destination	Protocol	Length	Info
2063	20.554094	222.12.223.55	192.168.0.13	TCP	98	6616 → 554 [SYN] Seq=0 Win=6001 Len=0
2064	20.554167	222.44.9.103	192.168.0.13	TCP	98	8101 → 554 [SYN] Seq=0 Win=1701 Len=0
2065	20.554239	222.139.215.174	192.168.0.13	TCP	98	5226 → 554 [SYN] Seq=0 Win=2015 Len=0
2066	20.554312	222.58.34.21	192.168.0.13	TCP	102	4219 → 554 [SYN] Seq=0 Win=3080 Len=0
2070	20.555328	222.182.62.39	192.168.0.13	TCP	102	6696 → 554 [SYN] Seq=0 Win=7996 Len=0
2074	20.556982	222.156.90.220	192.168.0.13	TCP	98	5121 → 554 [SYN] Seq=0 Win=2109 Len=0
2075	20.557052	222.198.6.128	192.168.0.13	TCP	98	6643 → 554 [SYN] Seq=0 Win=3154 Len=0
2085	20.563905	222.153.211.12	192.168.0.13	TCP	98	5814 → 554 [SYN] Seq=0 Win=3556 Len=0
2086	20.563978	222.229.214.32	192.168.0.13	TCP	98	1718 → 554 [SYN] Seq=0 Win=7411 Len=0
2087	20.564050	222.94.180.116	192.168.0.13	TCP	98	2170 → 554 [SYN] Seq=0 Win=3740 Len=0
2088	20.564122	222.161.231.69	192.168.0.13	TCP	98	5252 → 554 [SYN] Seq=0 Win=1182 Len=0
2089	20.564193	222.26.254.124	192.168.0.13	TCP	98	1980 → 554 [SYN] Seq=0 Win=1107 Len=0
2090	20.564263	222.56.223.169	192.168.0.13	TCP	102	7918 → 554 [SYN] Seq=0 Win=6270 Len=0
2091	20.564879	222.4.247.209	192.168.0.13	TCP	102	3480 → 554 [SYN] Seq=0 Win=1166 Len=0
2095	20.568537	222.134.139.210	192.168.0.13	TCP	98	7291 → 554 [SYN] Seq=0 Win=1061 Len=0
2096	20.568616	222.147.241.4	192.168.0.13	TCP	98	3222 → 554 [SYN] Seq=0 Win=7388 Len=0
2097	20.568689	222.246.167.104	192.168.0.13	TCP	102	7278 → 554 [SYN] Seq=0 Win=1855 Len=0
2099	20.569649	222.3.162.139	192.168.0.13	TCP	98	6119 → 554 [SYN] Seq=0 Win=8753 Len=0
2109	20.579141	222.84.46.42	192.168.0.13	TCP	98	8635 → 554 [SYN] Seq=0 Win=1376 Len=0
2110	20.579289	222.203.194.120	192.168.0.13	TCP	98	4105 → 554 [SYN] Seq=0 Win=7882 Len=0
2111	20.579362	222.244.161.16	192.168.0.13	TCP	98	5922 → 554 [SYN] Seq=0 Win=8689 Len=0
2112	20.579432	222.20.44.168	192.168.0.13	TCP	98	3104 → 554 [SYN] Seq=0 Win=2804 Len=0
2113	20.579503	222.98.54.130	192.168.0.13	TCP	98	8476 → 554 [SYN] Seq=0 Win=4157 Len=0
2114	20.579574	222.243.109.43	192.168.0.13	TCP	98	6146 → 554 [SYN] Seq=0 Win=8908 Len=0
2115	20.579646	222.43.168.118	192.168.0.13	TCP	98	3019 → 554 [SYN] Seq=0 Win=8829 Len=0
2116	20.579717	222.167.227.228	192.168.0.13	TCP	98	3798 → 554 [SYN] Seq=0 Win=8188 Len=0
2117	20.579789	222.52.46.57	192.168.0.13	TCP	102	6698 → 554 [SYN] Seq=0 Win=1586 Len=0
2118	20.580406	222.197.157.247	192.168.0.13	TCP	102	2430 → 554 [SYN] Seq=0 Win=8976 Len=0
2122	20.583078	222.15.190.223	192.168.0.13	TCP	98	1713 → 554 [SYN] Seq=0 Win=4105 Len=0
2123	20.583157	222.121.124.228	192.168.0.13	TCP	102	2920 → 554 [SYN] Seq=0 Win=2506 Len=0

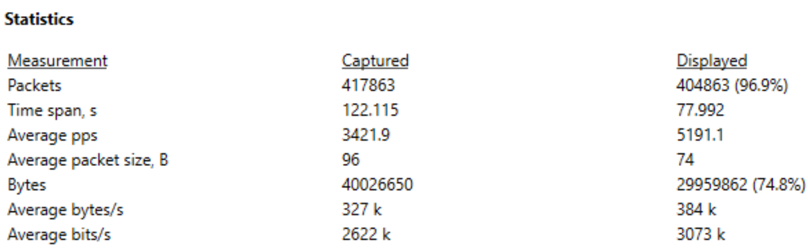
Figure 3. SYN flooding attack [11]

10436	45.170457	111.70.83.13	192.168.0.24	TCP	98	[TCP Retransmission] 3948 → 19604 [SYN] Seq=0 Win=2641 Len=0
10437	45.170531	111.196.67.139	192.168.0.24	TCP	98	[TCP Retransmission] 6784 → 19604 [SYN] Seq=0 Win=3522 Len=0
10438	45.170605	111.137.251.90	192.168.0.24	TCP	98	[TCP Retransmission] 6030 → 19604 [SYN] Seq=0 Win=4999 Len=0
10439	45.170675	111.26.156.231	192.168.0.24	TCP	102	[TCP Retransmission] 1447 → 19604 [SYN] Seq=0 Win=5045 Len=0
10440	45.170746	111.70.83.13	192.168.0.24	TCP	98	[TCP Retransmission] 3948 → 19604 [SYN] Seq=0 Win=2641 Len=0
10441	45.170820	111.196.67.139	192.168.0.24	TCP	98	[TCP Retransmission] 6784 → 19604 [SYN] Seq=0 Win=3522 Len=0
10442	45.170893	111.137.251.90	192.168.0.24	TCP	98	[TCP Retransmission] 6030 → 19604 [SYN] Seq=0 Win=4999 Len=0
10443	45.170966	111.26.156.231	192.168.0.24	TCP	102	[TCP Retransmission] 1447 → 19604 [SYN] Seq=0 Win=5045 Len=0
10444	45.171148	111.70.83.13	192.168.0.24	TCP	98	[TCP Retransmission] 3948 → 19604 [SYN] Seq=0 Win=2641 Len=0
10445	45.171221	111.196.67.139	192.168.0.24	TCP	98	[TCP Retransmission] 6784 → 19604 [SYN] Seq=0 Win=3522 Len=0
10446	45.171294	111.137.251.90	192.168.0.24	TCP	98	[TCP Retransmission] 6030 → 19604 [SYN] Seq=0 Win=4999 Len=0
10447	45.171368	111.26.156.231	192.168.0.24	TCP	102	[TCP Retransmission] 1447 → 19604 [SYN] Seq=0 Win=5045 Len=0
10448	45.171441	111.70.83.13	192.168.0.24	TCP	98	[TCP Retransmission] 3948 → 19604 [SYN] Seq=0 Win=2641 Len=0
10449	45.171514	111.196.67.139	192.168.0.24	TCP	98	[TCP Retransmission] 6784 → 19604 [SYN] Seq=0 Win=3522 Len=0
10450	45.171595	111.137.251.90	192.168.0.24	TCP	98	[TCP Retransmission] 6030 → 19604 [SYN] Seq=0 Win=4999 Len=0
10451	45.171669	111.26.156.231	192.168.0.24	TCP	102	[TCP Retransmission] 1447 → 19604 [SYN] Seq=0 Win=5045 Len=0
10452	45.171793	111.70.83.13	192.168.0.24	TCP	79	[TCP Retransmission] 3948 → 19604 [SYN] Seq=0 Win=2641 Len=0
10453	45.175688	111.196.67.139	192.168.0.24	TCP	79	[TCP Retransmission] 6784 → 19604 [SYN] Seq=0 Win=3522 Len=0
10454	45.176459	111.137.251.90	192.168.0.24	TCP	79	[TCP Retransmission] 6030 → 19604 [SYN] Seq=0 Win=4999 Len=0
10455	45.177139	111.26.156.231	192.168.0.24	TCP	79	[TCP Retransmission] 1447 → 19604 [SYN] Seq=0 Win=5045 Len=0

Figure 4. TCP retransmission [11]

4.3. UDP flooding attack

By analyzing network traffic, it is possible to see where and how a UDP flooding attack occurred on the example of a smart camera. A UDP flooding attack attempts to saturate the bandwidth in order to deny service on the network. This DoS (Denial of Service) attack is usually performed by sending a rapid series of UDP datagrams with spoofed IP addresses to a server within the network via different ports, forcing the server to respond with ICMP traffic. Bandwidth saturation occurs in both the inbound and outbound directions. An unexpected increase in UDP packets can be an indicator of an attack. In Figure 5, it is possible to see that out of a total of 417,863 packets, 404,863 contain the attack, which is 96.9% of the total packets [12].



Statistics

Measurement	Captured	Displayed
Packets	417863	404863 (96.9%)
Time span, s	122.115	77.992
Average pps	3421.9	5191.1
Average packet size, B	96	74
Bytes	40026650	29959862 (74.8%)
Average bytes/s	327 k	384 k
Average bits/s	2622 k	3073 k

Figure 5. UDP flooding attack [12]

4.4. ACK flooding attack

ACK is an abbreviation for Acknowledgment. An ACK packet is any TCP packet that acknowledges the receipt of a message or sequence of packets. ACK flooding attacks target devices that need to process every packet they receive. Legitimate and illegitimate ACK packets tend to look the same, making ACK flooding attacks difficult to stop without using the content delivery network to filter out unnecessary ACK packets. ACK flooding attack can also be detected via RST packets. When the server receives unsolicited ACK packets, it may respond with RST packets, which means that there is no active connection. In order to identify such packets in research, the filter: tcp.flags.reset==1 will be used. Figure 6 shows such packages. In Figure 6, the packet numbered 41436 is marked and it is evident that it is an RST packet, and that the marked packet indicates that the segment does not contain a full TCP header, which means that perhaps Nmap or someone else is sending unusual packets on purpose.

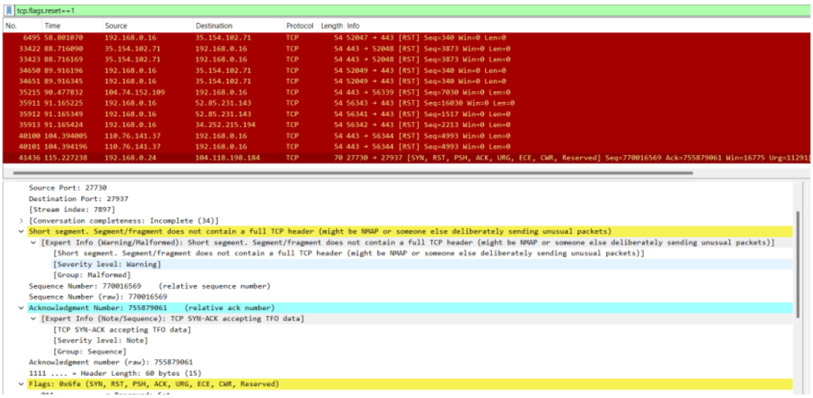


Figure 6. TCP header [11]

4.5. HTTP flooding attacks

HTTP flooding attacks target web servers and applications. These attacks are designed to overwhelm a web server's resources by continuously requesting one or more Uniform Resource Locators (URLs) from many source attack machines. Such machines simulate HTTP clients, such as web browsers. An HTTP flooding attack can consist of: GET – images and scripts, POST – files and forms, or a combination of GET and POST requests. When the server's concurrent connection limits are reached, the server can no longer respond to legitimate requests from other clients attempting to connect, causing a denial of service. HTTP flooding attacks use standard URL requests, so it can be quite difficult to distinguish from legitimate traffic [13].

In Figure 7, it is evident that an HTTP flooding attack is being carried out because a large amount of HTTP traffic is coming to the same server in a very short period of time. It can also be seen that the attack is occurring due to the warning marked yellow, which indicates excess data after the body that is neither a request nor a response.

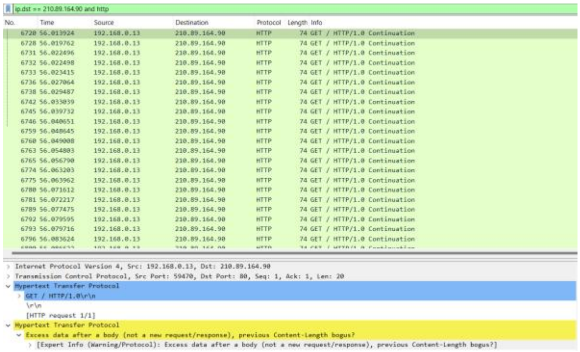


Figure 7. HTTP flooding attack [11]

5. Conclusion

By analyzing the vulnerabilities of various IoT devices, such as smart cameras and intelligent voice assistants, it was determined that user data is easily accessible if the devices are not properly protected. Research has shown that users on IoT devices do not use adequate security measures, such as weak authentication, unencrypted communication and inappropriate software upgrades. This further increases the risk of unauthorized data collection.

As part of the research, a synthesis of the results collected during network traffic analysis and experimental attacks on the EZVIZ smart camera and the SKT NUGU intelligent voice assistant was carried out. Emphasis is placed on: Man-in-The-Middle attacks, DoS SYN flooding attacks and Mirai Botnet attacks. It has been observed that the above-mentioned attacks can be carried out very easily if IoT devices are not properly protected, and this indicates the need to improve security mechanisms.

Although smart homes bring numerous advantages in terms of comfort and energy efficiency, it is necessary to introduce comprehensive security measures to ensure the safety and privacy of users. Continuous research of new threats and development of advanced security solutions are key factors in reducing unauthorized data collection in the smart home environment.

Literature

[1] TechTarget. Smart home. Available: https://www.techtarget.com/iotagenda/definition/smart-home-or-building [Accessed: June 2024]

[2] Zheng S, Apthorpe N, Chetty M, Feamster N. User Perceptions of Smart Home IoT Privacy. Proceedings of the ACM on Human-Computer Interaction. 2018;2(200): 1-20. Available: https://www.researchgate.net/publication/345546605_User_Perceptions_of_Smart_Home_IoT_Privacy [Accessed: June, 2024]

[3] Arabo A, Brown I, El-Moussa F. Privacy in the age of Mobility and Smart Devices in Smart Homes. International Conference on Privacy, Security, Risk and Trust and International Conference on Social Computing. 2012: 819-826. Available: https://www.researchgate.net/publication/254934189_Privacy_in_the_Age_of_Mobility_and_Smart_Devices_in_Smart_Home [Accessed: June, 2024]

[4] Bugeja J, Jacobsson A, Davidsson P. On Privacy and Security Challenges in Smart Connected Homes. Internet of Things and People Research Center and Department of Computer Science. 2016: 172-175. Available:

https://www.researchgate.net/publication/314266078_On_Privacy_and_Security_Challenges_in_Smart_Connected_Homes [Accessed: June, 2024]
[5] Cvitic I, Vujic M, Husnjak S. Classification of Security Risks in the IoT Environment. Annals of DAAAM and Proceedings of the International DAAAM Symposium, 2016, p. 0731–40. https://doi.org/10.2507/26th.daaam.proceedings.102.
[6] Cvitić I, Peraković D, Periša M, Botica M. Novel approach for detection of IoT generated DDoS traffic. Wireless Networks 2019. https://doi.org/10.1007/s11276-019-02 043-1.
[7] Cvitić I, Peraković D, Periša M, Husnjak S. An overview of distributed denial of service traffic detection approaches. Promet - Traffic - Traffico 2019;31:453–64. https://doi.org/10.7307/ptt.v31i4.3082.
[8] Alharbi R, Aspinall D. An IoT Analysis Framework: An Investigation of IoT Smart Cameras' Vulnerabilities. Living in the Internet of Things: Cybersecurity of the IoT. 2018. Available: https://chooser.crossref.org/?doi=10.1049%2Fcp.2018.0047 [Accessed: February 2024]
[9] Sharif K, Tenbergen B. Smart Home Voice Assistants: A Literature Survey of User Privacy and Security Vulnerabilities. Complex Systems Informatics and Modeling Quarterly. 2020;(24): 15-30. Available: https://csimq-journals.rtu.lv/csimq/article/view/csimq.2020-24.02 [Accessed: February, 2024]
[10] Hoy S.M.B. Alexa, Siri, Cortana, and more: an introduction to voice assistants. Medical reference services quarterly 2018;37(1): 81-88. Available: http://dx.doi.org/10.1080/02763869.2018.1404391 [Accessed: February 2024]
[11] IEEEDataPort. IoT network intrusion dataset. Retrieved from: https://ieee-dataport.org/open-access/iot-network-intrusion-dataset [Accessed: February 2024]
[12] Mazebolt. UDP Flood. Available: https://kb.mazebolt.com/knowledgebase/udp-flood/ [Accessed: February 2024]
[13] Mazebolt. HTTP Flood. Available: https://kb.mazebolt.com/knowledgebase/http-flood/ [Accessed: February 2024]

Rezime: *Sve veća upotreba uređaja povezanih na internet izlaže korisnike pametnih kuća bezbednosnim izazovima i pretnjama. Stoga je važno obratiti pažnju na prikupljanje korisničkih podataka u okruženju pametne kuće. Cilj ovog istraživanja je da se korisnicima pametnih kuća pokaže na koje načine je moguće prikupljati i koristiti njihove podatke u takvom okruženju. Istraživanje se zasniva na prikupljanju podataka sa IoT uređaja unutar okruženja pametne kuće i na prikazu neovlašćenog prikupljanja podataka, tj. prikazu napada koji se mogu dogoditi u okruženju pametne kuće. Za istraživanje je korišćen skup podataka o upadima u IoT mrežu. Za ovaj skup podataka mreže, autori su kreirali različite vrste mrežnih napada u IoT okruženju u akademske svrhe. Korišćena su dva tipična uređaja pametne kuće: inteligentni glasovni asistent i pametna kamera. Rezultati istraživanja pokazuju gde su se dogodili: napadi „čovek u sredini", SYN, UDP, ACK i HTTP poplave.*

Ključne reči: *prikupljanja podataka; pametna kuća; Internet stvari; digitalna forenzika, kibernetičke ugroze*

MOGUĆNOSTI NEOVLAŠĆENOG PRIKUPLJANJA PODATAKA U OKRUŽENJU PAMETNIH KUĆA

Ivan Cvitić, Dragan Peraković, Mihaela Maturanec