Analyzing Network Behavior of IoT Devices* Using MUD Standard

IoT Devices - Smart Siren and WiFi Smart Camera

Alphonse - 3367746 Thanuja - 3230511 Cavwin - 3321533

***Abstract*—This report details the methodology and findings from our analysis of two IoT devices: a smart siren and a WiFi smart camera with light. Using open-source tool WireShark, we captured and analyzed the network behavior of the two IoT devices. Our study focuses on understanding their network interactions, response to external triggers, and the services they utilize, guided by the Manufacturer Usage Description (MUD) standard (RFC 8520). We propose improvements for enhancing the security of the IoT devices and suggest extensions to the MUD specification based on our findings.**

***Index Terms*—MUD profile, protocols, wireshark, Internet of Things, CyberSecurity**

I. Introduction

The Internet of Things (IoT) comprises a diverse array of devices designed to interact with the physical world, performing specific and user defined tasks autonomously. They have transformed various aspects of daily life, from home automation to industrial applications. This rapid proliferation of IoT devices has also given rise to a lot of new security challenges, since most IoT devices lack comprehensive security features which makes them vulnerable to cyber-attacks. As IoT devices become increasingly ubiquitous, understanding the network behavior of these devices is crucial for mitigating such risks and ensuring secure and efficient operation.

The primary objective of this project is to understand the network behavior of the two IoT devices using Manufacturer Usage Description (MUD) standard, which provides a structured language for defining the expected network behavior of such device. The MUD standard, defined in RFC 8520 by the Internet Engineering Task Force (IETF), provides a framework for specifying the expected network behavior of IoT devices. Profiling IoT devices in this manner helps network administrators create precise security policies and in understanding their communication habits, thereby establishing robust security measures to protect against unauthorized access and potential cyber threats and also enhancing the overall security posture of IoT ecosystems.

Profiling the network behavior of IoT devices using the MUD standard also offers several benefits. First, it helps identify and mitigate security vulnerabilities by establishing baseline behaviors and detecting deviations. Second, it enhances network management by enabling automated responses to various traffic patterns, thus preventing potential attacks. Third, it provides insights into the operational patterns of IoT devices, helping in the optimization of network resources and ensuring efficient device performance. In this study, we focus on two IoT devices: a smart siren and a WiFi smart camera. By capturing and analyzing the network traffic of these devices, we aim to develop comprehensive MUD profiles and propose enhancements to the MUD standard for better security and operational efficiency.

II. Methodology

A. *Devices Used*

The devices were chosen in such a way that they represent the most typical applications of IoT in our daily lives, such as surveillance, security measures and lighting. These devices are also user friendly, easy to analyze and also exhibit diverse network behaviors.

1) Smart Siren: The LSC Smart Siren device acts as a loud alarm in response to security breaches or other external inputs as desired by the user. The smart siren's activity and inputs can be easily tracked and set via a dedicated mobile application.

2) Wifi Smart Camera: The RUSFEIDA WiFi Smart Camera combines surveillance capabilities and luminescence, providing both security and lighting. The device can also be remotely accessed by its respective mobile application, where the user can view the recorded videos and turn the light on or off.

B. *Tools Used*

1) Wireshark: [1] It is a network protocol analyzer that allows the user to capture and analyze network traffic in real-time. The output of Wireshark includes detailed packet information, protocol analysis, and statistics on network traffic. In this project it is used for capturing the network traffics of the two IoT devices and generate a Device Traffic Trace(.pcap) file. This file is then used for interactive analysis of their respective network traffics. This helps in troubleshooting network issues, detecting security vulnerabilities, and monitoring network performance.

2) mudgee: [2] This tool is used for generating Manufacture Usage Description(MUD) profiles based on the observed network behaviour from the generated Device Traffic Trace (pcap)file. The generated MUD profiles are in .json format. The tool also gives the IP Flow Data as a .csv file which makes analysis much simpler.

3) LSC Smart Control Application: This mobile application is used to setup and work with the Smart Siren. The application gives the activity of the siren in detail including the time it was turned ON/OFF or the alarm was triggered. The application also allows the user to connect the siren with other LSC Smart devices.

4) iCSee: This application is used to connect with the Smart camera. It allows the user to record /view the recorded videos with detailed timestamps stored in the SD card of the device and also used as ON/OFF light as the user desires.

C. Process

a) Setup: The IoT devices were set up according to the user manuals and paired to the controlled network environment via their respective mobile applications. This environment included a mobile hotspot shared from a laptop, which acted as the local network and the IoT devices were connected to this environment allowing us to capture all their network interactions. The laptop runs the Wireshark tool for traffic capture. The controlled network environment ensures accurate and repeatable results.

b) Traffic Capture: Using the mobile applications, various interactions with the IoT devices were conducted. Network traffic was captured during these interactions via Wireshark. The results were captured and stored in a .pcap file to be used for analysis later.

- Smart Siren: The traffic was captured when the alarm was turned ON/OFF manually, and alarm triggers. The siren was triggered both manually and via a simulated breach to observe different traffic patterns.
- WiFi Smart Camera: The traffic is captured when the device was in use and the video transmission occurred. The interactions with the attached light were also captured.

c) Traffic Analysis: The captured traffic was analyzed using external sites and additional tools to identify the common communication patterns, protocols used, endpoints and the interactions with external services. Major analyses include,

- Identifying the Key traffic Flows, which can be mapped by identifying the IP and MAC addresses of the IoT devices and gateway. We can observe specific interactions that are mapped to the corresponding packets based on the timestamps.
- Analyzing which protocols such as HTTP, UDP, TCP, TLS and DNS are being used by the devices to communicate with external services. The communication frequency and context of each protocol can be observed and used for further examination.
- Identifying all the external services which the devices connect to. This includes the cloud servers for command and control, firmware updates servers, and also DNS servers for address resolving.

d) MUD Profile Creation : Using the captured network traffic data of both the IoT devices, and the mudgee tool, we can create a MUD profile for each device individually. These profiles include the device information (manufacturer, model, etc.) and other device-specific details. They also contain a list of all the allowed communication patterns which include the IP addresses, protocols, and all the ports the device is allowed to use. The MUD file also contains all the security protocols followed by the device, which ensures secure communication by restricting or blocking unauthorized access. For example, the smart siren's MUD profile restricted communication to the cloud service's IP address, while blocking all other outbound connections.

The .json file generated by the MUDgee, are then compared with the MUD standards of the device and various results and improvements are proposed for each MUD file. These improvements range from addition of anomaly detection methods to making the devices more context-aware. This ensures improved reliability and authenticity.

III. Results

A. Smart Siren

*1) **Traffic Characteristics**:* The smart siren exhibited a predictable network behavior, mainly communicating with a cloud service managed by its manufacturer, Tuya Smart. The siren also establishes a quick communication sequence with the cloud service, confirming the trigger and initiating the alarm. This behavior was consistent across multiple tests. The siren sent periodic heartbeat messages to the cloud service approximately every 5 seconds to indicate its operational state. When triggered, the siren communicates with the cloud to confirm the trigger event and to receive activation commands. Although the last process was less frequent, it takes a bit higher data than normal operations.

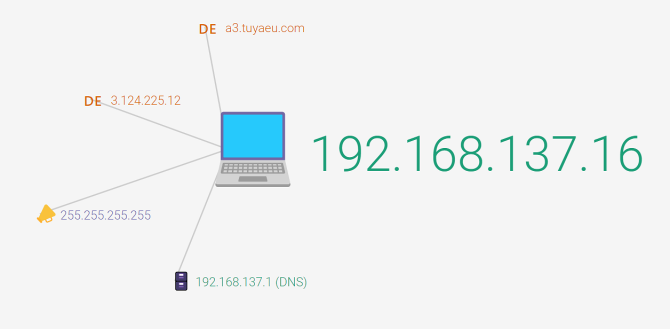

Fig. 1. [3]The visual representation of the Smart Siren network

Protocols Used: The smart siren predominantly uses the TCP and UDP protocol for communication

- TCP and TLSv1.2: For command and control communication with the cloud service, particularly for activation and acknowledgment.
- UDP: For maintaining the connection with the application.
- HTTPS: For secure firmware updates, ensuring the integrity and authenticity of the update files.
- DNS: For resolving the cloud service's IP address, ensuring the siren could always connect to the correct server.
- SSL: To encrypt data transmitted between clients and servers, ensuring privacy and security.

Endpoints: The siren frequently communicates with cloud servers at a3.tuyaeu.com

Behavior Patterns: The device remains silent when it's not actively receiving inputs from the user. There is a sharp peak in packet transmission when the user triggers an alarm.

*2) **Network Traffic Analysis**:* Fig. 1 shows the network traffic peaks corresponding to the various control actions. For example, the siren triggers are represented by the discontinuous signals while the siren up time is represented by the continuous signals.

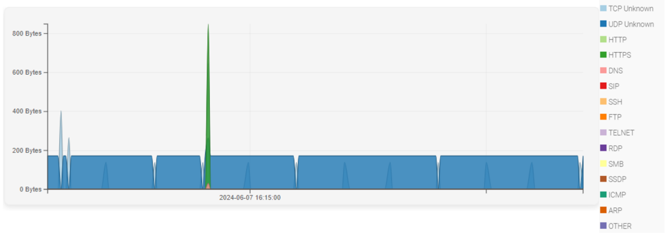

Fig. 2. [3]The captured network traffic of the Smart Siren device

Timestamp	Event	Endpoint	Protocol	Data volume
16:14:08	Siren Turned On	a3.tuyaeu.com	DNS	13
16:14:09	Siren Volume changed	a3.tuyaeu.com	TCP	54

TABLE I
SUMMARIZES THE COMMON ENDPOINTS AND SERVICES USED BY THE SMART SIREN

B. *Wifi Camera*

*1) **Traffic Characteristics**:* The WiFi smart camera exhibited a complex network behavior compared to the smart siren due to its multifunctional nature. The camera streamed video to the cloud throughout its uptime using the UDP protocol. The camera responded to the presence of the user and let out a voice message to welcome them. The light and camera were controlled through the mobile application using TCP protocols. The camera was able to initiate video recording upon user authorization. The light also responded to the manual commands as well as scheduled events.

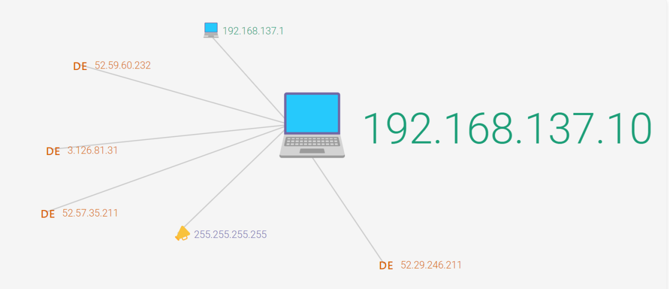

Fig. 3. [3]The visual representation of the WiFi Camera Network

Protocols Used:

- UDP: For video streaming to the cloud storage service.
- TCP: For control commands and alert notifications.
- DNS: For resolving the IP addresses of the cloud services.

Endpoints: The camera communicates with tls3.cryptohack.org frequently to perform DNS lookups and resolve this endpoint.

Behavior Patterns: There is an increased network traffic observed due to the live streaming and recording taking place, even when there are no human triggers.

*2) **Network Traffic Analysis**:* Figure 2 illustrates the network traffic peaks during camera recording and live streaming. Each peak indicates a period of increased data transfer, reflecting the device's active state. The accompanying is also observed,

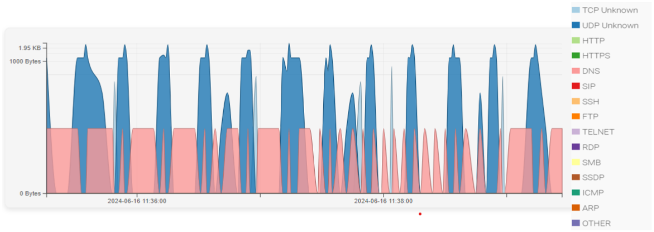

Fig. 4. [3]The captured network traffic of the WiFi Camera

Timestamp	Event	Endpoint	Protocol	Data volume (in kB)
11:35:17	Camera Connected	secu100.net	DNS	11
11:36:58	Live Video Streaming	access-dss.secu100.net	HTTP	363

TABLE II
SUMMARIZES THE COMMON ENDPOINTS AND SERVICES USED BY THE SMART CAMERA

IV. ANALYSIS AND OBSERVATIONS

A. *Smart Siren*

Protocol Usage: The smart siren primarily used TCP and UDP for command and control . Periodic DNS lookups were observed for resolving cloud service addresses.

Traffic Patterns: The traffic patterns observed for the smart siren were highly consistent and predictable:

- Regular Heartbeats: The siren sends heartbeat messages to the cloud service every 5 seconds. This regular pattern helps in monitoring the device’s operational status but also makes it easier to detect anomalies when these heartbeats are disrupted.
- Activation Events: During manual triggering, the traffic spiked as the siren communicated the activation event to the cloud service and awaited a response. This spike was immediate and short-lived, indicating an efficient communication protocol for urgent actions.

B. *WiFi Smart Camera*

Protocol Usage: The wifi smart camera primarily used UDP for video streaming and TCP for control commands and alert notifications. Frequent DNS lookups were observed for resolving cloud service addresses.

Traffic Patterns: Traffic spikes were observed during trigger events from the application and scheduled operations, indicating high data transfer during these periods. The traffic patterns for the WiFi smart camera and light were more complex due to its multifunctionality:

- Idle State:When not actively recording, the device generated minimal traffic, since the only task consisted of periodic status updates to the cloud service.
- Video Recording: When the device was actively recording the video, there were distinguishable spikes in traffic, as the camera initiates video recording and sends alert notifications. These spikes were consistent throughout the uptime, until turned OFF.
- Video Streaming: Continuous video streaming results in a high amount of packet transfer thus leading to high traffic. This reflects the real-time transfer of video data to the cloud storage service. This pattern was consistent during active streaming sessions.
- Light Control: Commands from the mobile app to control the light (on/off, etc.) resulted in brief traffic bursts over HTTP.

C. *Recommendations for MUD Profiles*

Based on the above result, observations and analysis, we can make some relevant MUD profile improvements to the devices.

1) Smart Siren:

- Allowed Protocols: HTTPS for all communications ensuring that all data transmitted between the siren and the cloud service is encrypted. Upgrade the TLSv1.2 to the latest TLS 1.3
- Authorized Endpoints: Specific cloud service IP addresses to limit connections to trusted servers.
- Heartbeat Monitoring: Rules to detect and alert on disruptions in regular heartbeat messages.
- Anomaly Detection: Rules to monitor and alert on unusual traffic patterns, such as unexpected spikes or sustained high traffic outside of normal streaming sessions.

2) WiFi Smart Camera:

- Allowed Protocols: RTSP for video streaming, HTTPS for control commands and alerts.
- Authorized Endpoints: Specific cloud storage and control service IP addresses.
- Anomaly Detection: Rules to monitor and alert on unusual traffic patterns, such as unexpected spikes or sustained high traffic outside of normal streaming sessions.

V. Proposal for MUD usage

Based on our analysis of the Smart Siren and Wifi Camera, we propose the following enhancements to the MUD profiles.

A. *Real-time Anomaly Detection*

Implementing real-time anomaly detection within MUD profiles would significantly enhance IoT security. Administrators can quickly identify and respond to potential threats, by monitoring traffic patterns and comparing them to the expected behavior specified in the MUD profiles. This approach helps in mitigating risks before they can escalate into serious breaches.

The updated MUD profile can be presented in this format,

```
”conditions”: {
  ”frequency”: {
    ”max-events”: 10,
    ”time-period-seconds”: 3600
  },
  ”traffic-volume”: {
    ”max-volume-kb”: 1000,
    ”time-period-seconds”: 3600
  }
}
```

B. *Context-Aware MUD Profiles*

Another enhancement involves making the IoT devices more context-aware, by adjusting the allowed behavior based on the operational context of the device. For instance, the smart siren might have different network behaviors based on contextual information such as time of day, user presence, or specific events. This can enhance security by tailoring the device’s network permissions to its operational context.

The updated MUD profile can be presented in this format,

```
”conditions”: {
  ”time-range”: {
    ”end-time”: ”06:00”,
    ”start-time”: ”18:00”
  }
},
”matches”: {
  ”ipv4”: {
    ”destination-ipv4-network”: ”192.168.1.11/32”,
    ”destination-port”: 80,
      ”protocol”: 6,
      ”source-ipv4-network”: ”0.0.0.0/0”,
      ”source-port”: 0
    }
  },
  ”name”: ”allow-nighttime-http”
  }
```

C. Automated Incident Response

We can also extend the MUD profiles to include automated incident response rules. For example, if any anomaly is detected, the profile could specify actions such as temporarily blocking the device's network access, alerting administrators, or triggering security measures. This automated response can help contain threats and minimize the impact of security incidents.

D. Security Enhancements

The use of HTTPS for control and alerts enhances the overall security of the device, but the high amount of transfer in video streaming poses a potential risk if the channel is not properly monitored. This can be improved by only allowing authorized devices and users to access the shared network, to initiate streaming sessions. Also, implementation of anomaly detection methods allows the user to monitor the traffic and detect any unusual activities thus enhancing the device's security posture.

VI. Conclusion

It is important to understand and manage the network behavior of IoT devices, to enhance their security and operational reliability. Our detailed analysis of the smart siren and the WiFi smart camera revealed how the Manufacturer Usage Description (MUD) standard can be effectively used to capture and profile device behaviors. Future updates to could include advanced context-aware rules and automated incident response mechanisms to dynamically adapt to security policies. Enhancements in anomaly detection, leveraging AI and machine learning, will only improve real-time threat identification. Integrating IoT devices with broader security ecosystems and continuous updating encryption standards will be crucial. Additionally, designing more user-friendly interfaces for creating and managing MUD profiles can help users secure their IoT devices more effectively.

References

[1] *Wireshark*. URL: https://www.wireshark.org/.

[2] *MUDgee tool*. URL: https://github.com/ayyoob/mudg.

[3] *PCAP visualizer*. URL: https://apackets.com.

Reflection

A. Team Reflection

Our collaboration as a team was instrumental in successfully completing this IoT Device Network Behavior Analysis project. Working together allowed us to leverage each team member's strengths and tackle challenges more efficiently. Each member brought unique skills and perspectives to the project, enhancing the overall quality of our work.

B. Individual Reflections

1) Alphonse: I focused primarily on the initial setup and capturing network traffic data and ensuring its accuracy. Collaborating with the team helped me understand the complexities of network behavior analysis, and I appreciate the detailed discussions we had about interpreting encrypted traffic and MUD standards.

2) Cavwin: I contributed mainly with analyzing the captured traffic data using Wireshark and online tools. Working closely with Alphonse and Thanuja, I was able to identify patterns and document them effectively and represent our discussions in the report efficiently. I felt this project was an excellent opportunity to apply theoretical knowledge in a practical setting.

3) Thanuja: I mainly worked on traffic capturing using wireshark and successfully contributed to the process of creating MUD profiles using Mudgee from the pcap generated. I also worked closely with the teammates on the report,ensuring we accurately represent the devices' expected behavior.I gained hands-on experience from traffic analysis and this helped in increasing my practical understanding of network management and security.

AUTHOR DECLARATION

During the preparation of this work we as authors used ChatGPT to improve the language of our report. We confirm that we alone wrote the original text in full and that we then reviewed and edited the content using ChatGPT. We,the authors jointly take full responsibility for the content of this work.