

|  |
| --- |
| **LoRaWAN Network IoT Devices Security Test**  *To complete a penetration test on a LoRaWAN network and its related devices and present our findings in a report and presentation covering our investigation.*  **EH8**  **Ryan Petrie, Isaac Potts, Ben Poulton, Annie Place, Mattia Pulvirenti, Joey Hall**  CMP311: Professional Project Development & Delivery  **BSc Ethical Hacking**  2024/25 |

**All work in this document is subject to an NDA. This work is confidential and MUST not be shared with others.**

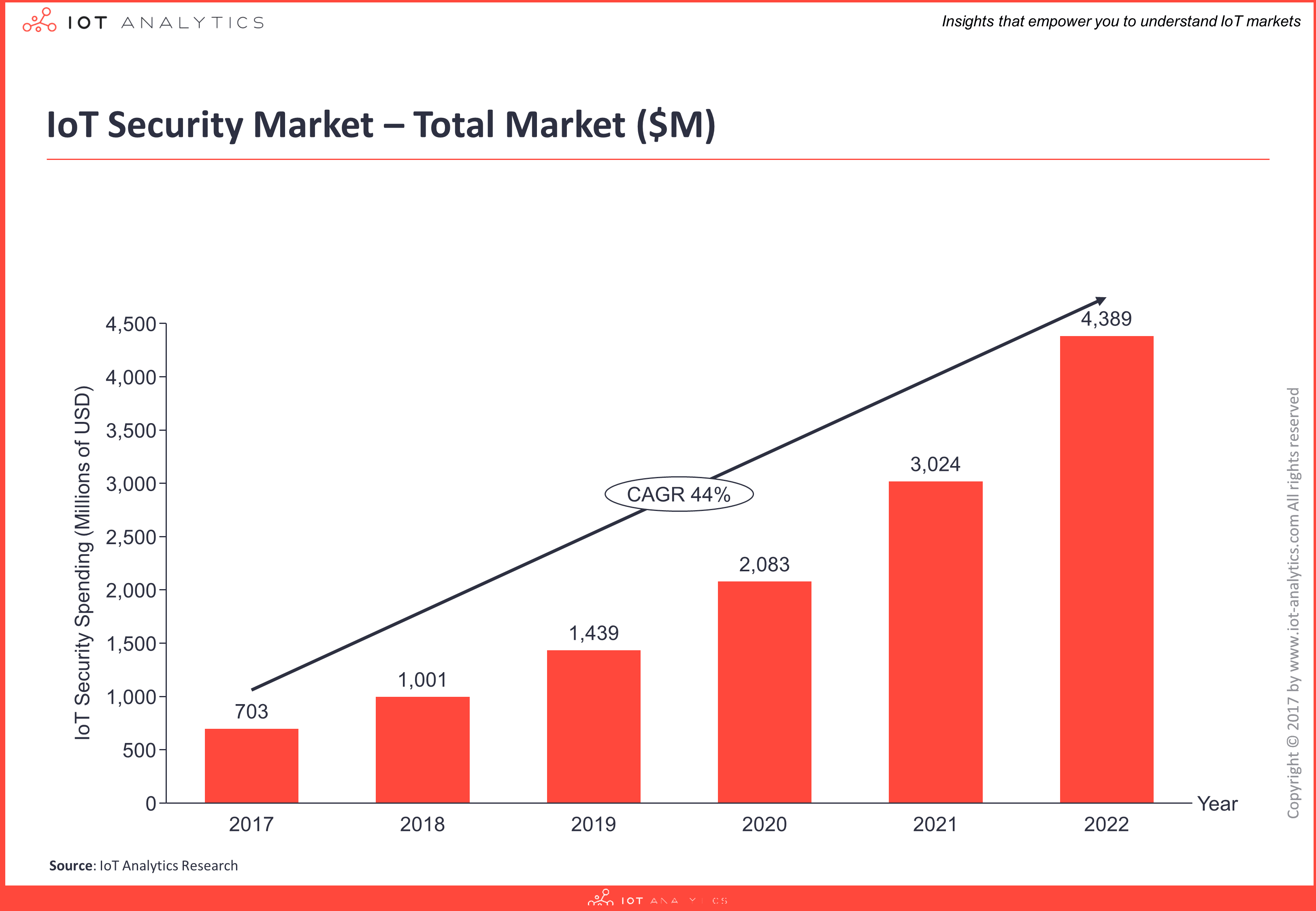
|  |  |  |
| --- | --- | --- |
| Team Member | Section | Technical Contribution (list contributed work, e.g., coded, designed, developed, investigated components etc.) |
| Mattia Pulvirenti | Executive Summary | Security testing and research, particularly related to RF transmission protocols. |
| Isaac Potts | Introduction | Vulnerability scanning, web application testing, tested ssh and http server for CVEs. |
| Ben Poulton | Method/Procedure | Vulnerability scanning, Web app testing specifically in regard to file handling. |
| Annie Place | Method/Procedure | Vulnerability analysis and assistance, LoRaWAN Auditing Framework research and execution. |
| Ryan Petrie | Results | Security Testing  Methodology research  Results writing |
| Joey Hall | Discussion | Network traffic analysis, encryption vulnerability testing with a focus on credential interception. |

# Executive Summary

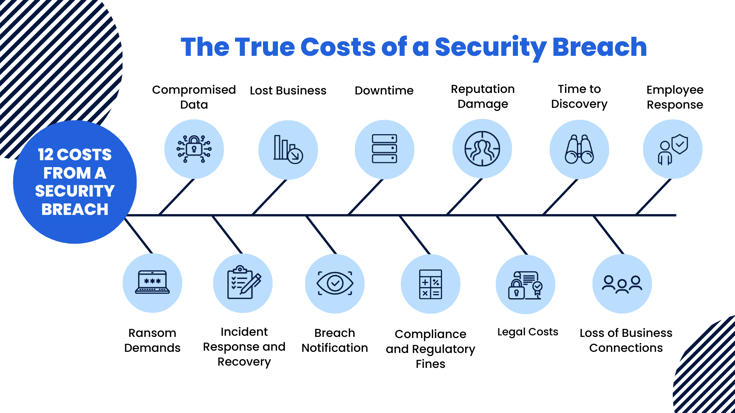
## Background and Objective

The following document covers a comprehensive review of the security framework of a LoRaWAN (Long Range Wide Area Network) IoT setup that has been commissioned by the firm PA Consulting.

LoRaWAN technology has widespread use in various critical industries where security flaws may result in significant financial losses, operational disruption and reputational damage. The financial implications of IoT security vulnerabilities are significant, particularly for businesses managing large networks of connected devices. The National Institute of Standards and Technology (NIST, cited in: JumpCloud (2024) ‘IoT security risks: stats and trends to know in 2025’, JumpCloud Blog, 7 November. Available at: <https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025>) reports that IoT security failures cost businesses an average of $330,000 per incident. This substantial cost highlights the importance of implementing robust security measures to mitigate risks in IoT ecosystems.



IoT Analytics (2017): ***Total IoT Security Market Forecast 2017–2022*.** Available at: <https://iot-analytics.com/wp-content/uploads/2017/11/TotalMarket-min.png> (Last accessed: 6 May 2025).



BitLyft (n.d.): ***True Costs of a Security Breach*.** Available at: <https://www.bitlyft.com/hs-fs/hubfs/True%20Costs%20of%20a%20Security%20Breach.png> (Last accessed: 6 May 2025).

The main goal of this project was to conduct a thorough penetration test of a Dragino LoRaWAN network and all connected devices and communication protocols, more precisely focusing on the Dragino LoRaWAN gateway kit v3 and a variety of remote sensors for soil moisture, electric conductivity, liquid level detection, and temperature and humidity. Areas to be tested included physical security, communications security, web application vulnerabilities, and operating system security. This test followed the guidelines presented in the OWASP IoT Security Testing Guide, which provides a practical, comprehensive framework for testing the security of IoT systems.

## Client Benefits

This security assessment delivers a comprehensive review of gateway firmware, web user interface, and radio communications on the product’s security, including severity of the vulnerabilities detected, their potential impact and recommendation on remediation actions to undertake. The findings enable PA Consulting to safeguard both their internal systems and client implementations against unauthorised access, data theft, and service disruption, that can impact their LoRaWAN implementations or customer deployments. This information is to be used to improve the organization's capability to deliver safe IoT solutions safeguarding confidential information and maintaining the integrity of IoT-dependent systems.

Ultimately, the findings enable the firm to understand specific security vulnerabilities within LoRaWAN deployments, prioritise remediation efforts, and implement appropriate countermeasures, as well as mature awareness about the technology’s weaknesses and criticalities, providing it with the ability to make informed decisions with respective clients, and cut costs.

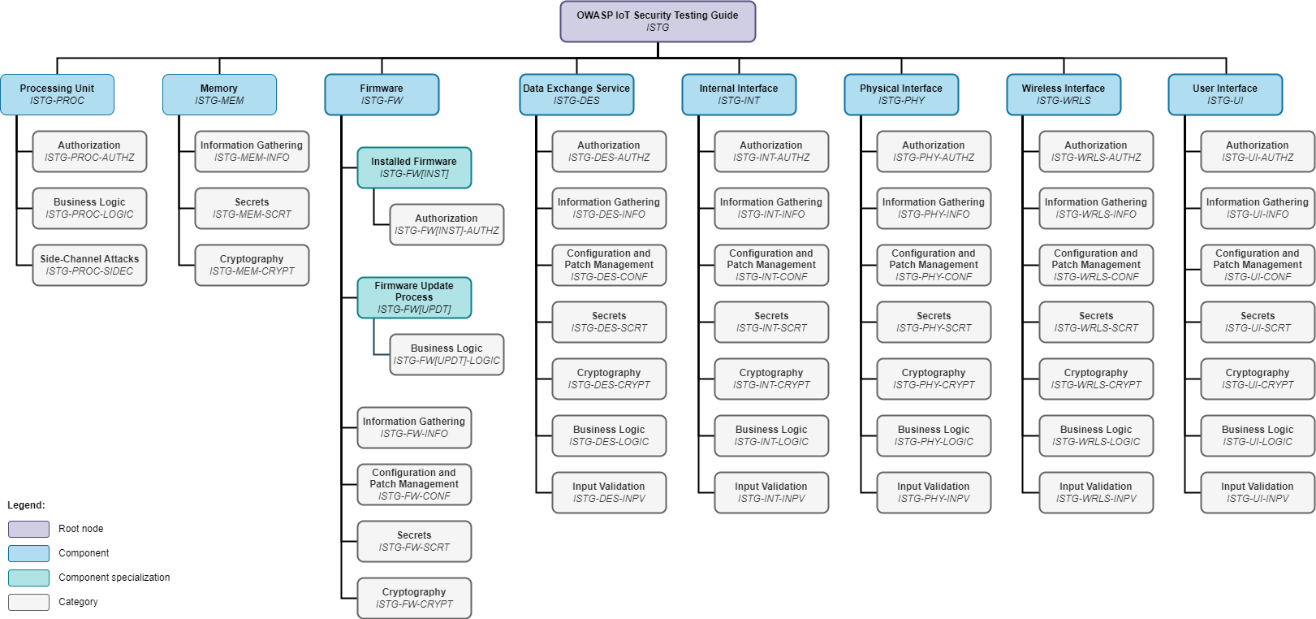
## Testing Methodology

The technical assessment followed the OWASP IoT Security Testing Guide methodology, consisting of several coordinated phases:

* Discovery and Enumeration: the team conducted a thorough inventory of all system components, documenting the Dragino LoRaWAN gateway kit, multiple sensor devices, network infrastructure, and host systems, including hardware and firmware specifications for accurate research.
* Information Gathering: multiple reconnaissance techniques were used to understand the system architecture and identify potential entry points. This included passive network monitoring , active scanning, web interface analysis and OSINT research to evaluate the system’s attack surface and known weaknesses.
* Vulnerability Analysis: the team conducted a systematic security assessment across multiple layers, including web application, networking, firmware, radio communications and transmission protocols.
* Exploitation Verification: exploitation attempts were conducted to validate identified vulnerabilities, including authentication bypass attempts, man-in-the-middle attacks, path traversal and file upload testing, radio signal capture, decryption and replay testing and SSH vulnerability testing.

Each testing phase utilised specialised tools appropriate to the target environment and technique involved. The present assessment combined both passive analysis methods and active exploitation techniques to perform an extensive evaluation of the LoRaWAN system’s security, considering both opportunistic and targeted attack scenarios.

This comprehensive methodology enabled thorough testing and documentation of vulnerabilities, including severity rating and remediation recommendations, providing a complete overview and understanding of the issues.



Base testing framework used as starting point for this project’s testing methodology:

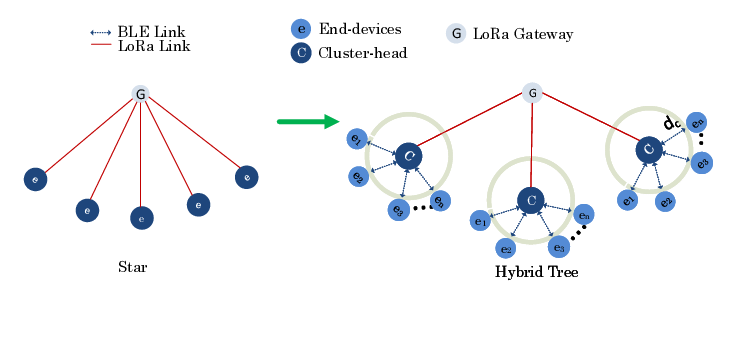
OWASP (n.d.): ***Component Overview – IoT Security Testing Guide*.** Available at: <https://owasp.org/owasp-istg/img/Component_Overview.png> (Last accessed: 6 May 2025).

## Findings and Implications

The security audit revealed several critical vulnerabilities in the Dragino LoRaWAN gateway that pose a risk to the entire network's integrity, here reported by cathegory:

* Administrative Access Vulnerabilities: The gateway has default credentials (root/dragino) easily available online. This allows unauthorised users to access critical system configurations, including firmware information, network setup, and administration of services.
* Insecure Communications: The gateway's web interface uses HTTP instead of HTTPS, thus allowing the interception of credentials through man-in-the-middle attacks using tools like Wireshark. This security vulnerability was successfully exploited, disclosing the administrative username and password.
* File Upload Vulnerability: MQTT Forwarder web page of the gateway has improper file validation that allows the upload of most file extensions without any limitation. Further inspection revealed path traversal flaws that permit files to be written to unintended directories in the device, potentially enabling code execution.
* Radio Communications Evaluation: While radiocommunications from sensors to the gateway can be intercepted and replayed with HackRF, the embedded AES-128 encryption that is part of the LoRaWAN protocol has proven effective in keeping the data payload contents secure. OpenSSH that exists on the gateway is affected by CVE-2024-6387; nonetheless, because the vulnerability involves exploiting a race condition in the code, the success rates are very low and POC is statistically hard to accomplish.

The findings show that while the encryption offered by the LoRaWAN protocol is robust, deployment-specific configurations seriously compromise the overall security of the system. The star topology of LoRaWAN networks (characterised by a central connection point) means that a gateway breach would affect all the connected devices and data communications. The discovered flaws could in fact allow attackers to gain administrative access to gateways, capture network traffic, run malicious code, and disrupt network activity. Due to these discoveries, it is advised to use separate and secure credentials, enable HTTPS, upgrade the firmware to patch CVE-2024-6387, and conduct proper file upload verification and constant security monitoring in LoRaWAN deployments.



Ayele, E.D. (2017): ***Proposed generic tree topology compared with the conventional star network of LoRa*.** Available at: <https://www.researchgate.net/figure/Proposed-generic-tree-topology-compared-with-the-conventional-star-network-of-LoRa_fig3_321170201> (Last accessed: 6 May 2025).

Table of Contents

[1 Executive Summary 4](#_Toc197264288)

[1.1 Background and Objective 4](#_Toc197264289)

[1.2 Client Benefits 4](#_Toc197264290)

[1.3 Testing Methodology 5](#_Toc197264291)

[1.4 Findings and Implications 6](#_Toc197264292)

[2 Introduction 9](#_Toc197264293)

[2.1 Background 9](#_Toc197264294)

[2.2 Aim 11](#_Toc197264295)

[3 Method 12](#_Toc197264296)

[3.1 Vulnerability Analysis 12](#_Toc197264297)

[3.1.1 Publicly available admin account credentials 12](#_Toc197264298)

[3.1.2 Weak cryptography through http protocol 13](#_Toc197264299)

[3.1.3 CVE-2024-6387 13](#_Toc197264300)

[3.1.4 Insecure File Upload 14](#_Toc197264301)

[3.1.5 HackRF Radio Wave Interception 15](#_Toc197264302)

[4 Procedure 18](#_Toc197264303)

[4.1 Network/Device Overview 18](#_Toc197264304)

[4.1.1 Overview of Network 18](#_Toc197264305)

[4.1.2 Router 18](#_Toc197264306)

[4.1.3 Switch 19](#_Toc197264307)

[4.1.4 Moisture and EC Sensor 20](#_Toc197264308)

[4.1.5 Liquid Level Sensor 20](#_Toc197264309)

[4.1.6 Temperature and Humid Sensor 21](#_Toc197264310)

[4.1.7 High Gain USB Adapter 22](#_Toc197264311)

[4.1.8 Host Machine 1 22](#_Toc197264312)

[4.1.9 Host Machine 2 22](#_Toc197264313)

[4.1.10 Laptop 22](#_Toc197264314)

[4.2 Information gathering 23](#_Toc197264315)

[4.2.1 Nikto 23](#_Toc197264316)

[4.2.2 Nmap 23](#_Toc197264317)

[4.2.3 LoRaWAN Auditing Framework 23](#_Toc197264318)

[5 Results 24](#_Toc197264319)

[5.1 Summary 24](#_Toc197264320)

[5.2 Exploits and Vulnerabilities 25](#_Toc197264321)

[5.2.1 Publicly available admin account credentials 25](#_Toc197264322)

[5.2.2 Weak cryptography through http protocol 25](#_Toc197264323)

[5.2.3 CVE-2024-6387 26](#_Toc197264324)

[5.2.4 Insecure File Upload 26](#_Toc197264325)

[5.2.5 LoRaWAN Auditing Framework 27](#_Toc197264326)

[5.3 Communications Analysis 27](#_Toc197264327)

[5.3.1 HackRF and Radio Waves 27](#_Toc197264328)

[6 Discussion 28](#_Toc197264329)

[6.1 General Discussion 28](#_Toc197264330)

[6.2 Conclusions 28](#_Toc197264331)

[6.3 Future Work or Countermeasures 28](#_Toc197264332)

[6.4 Call to action 28](#_Toc197264333)

[References 30](#_Toc197264334)

[Appendices 31](#_Toc197264335)

[Appendix A – Nikto Scan Result 31](#_Toc197264336)

[Appendix B – Nmap Scan Result 32](#_Toc197264337)

[Appendix C - Deliverables & requirements (Required) 33](#_Toc197264338)

[Appendix D Other settings discovered from access to Admin Account 36](#_Toc197264339)

[Appendix E Gateway Index 46](#_Toc197264340)

# Introduction

## Background

LoRaWAN stands for Long Range Wide Area Network and is used in a variety of sensors such as soil moisture sensors, animal tracking sensors, and is used in GPS- free tracking. (thethingsnetwork.org, 2024). The average data breach in the United Kingdom costs an average of £3.4 million (uk.newsroom.ibm.com, 2023) Along with the fact that LoRaWAN technology is used within vital healthcare products, the cost of a LoRaWAN hack could be immense.

There is a large given scope for this project. Not limited to but including testing physical security, security of communication in transit, web application exploits, and OS security. These were examined to identify present vulnerabilities.

Security of LoRaWAN devices is paramount, and the risk of data being compromised is decreased by the use of AES 128 encryption keys used within device communication (eetimes.com, 2020). However, vulnerabilities still exist, especially if a malicious actor can access the keys used for encryption. Other vulnerabilities in LoRaWAN have also been discovered, such as bit flipping, DOS using ABP and ACK spoofing (trendmicro.com, 2021). More vulnerabilities are being discovered in LoRaWAN, and we aim to provide a comprehensive report on the security posture of the given Dragino LoRaWAN devices.

LoRaWAN security has evolved over time, with the release of LoRaWAN 1.1 introducing new security mechanisms such as AES encrypted radio waves. However, some Dragino models will not have been automatically updated to this, leading to further vulnerabilities. As no auto-update mechanism was discovered it is possible many Dragino devices are still on an older version creating several vulnerabilities.

The LoRaWAN gateway also serves as an entry point into the broader network. All information throughout the LoRaWAN network follows a STAR topology. If the gateway device is compromised all further devices could be compromised. The devices that connect to the gateway communicate via radio waves, which the gateway sends to the cloud. This makes the gateway a prime target for any malicious actor.

This will be done through the use of the OWASP IoT Security Testing Guide, which provides a comprehensive methodology for penetration tests in the IoT field, offering flexibility to adapt innovations and developments (owasp.org, 2024) This encompasses the following elements of an IoT device

* Memory
* Firmware
* Data exchange services
* Internal interfaces
* Physical interfaces
* Wireless interfaces
* User interfaces

This allows for all in scope parts of the IoT devices to be tested.

Firmware analysis will form a key part of the testing process. A downloadable Dragino OS fo the same version of the device was found. This allowed for firmware examination of the gateway device, allowing the team to discover source code for web applications and examine further information about present services. Even though the key exchange services used AES encryption, the security of a LoRaWAN deployment is heavily dependent on the protection of the encryption keys themselves. If keys are improperly stored, exposed through firmware or recovered through another way can undermine all security in the device.

This testing will also involve tools such as Wireshark, HackRF and Burpsuite. The testing will also examine the integrity of the unique lightweight OS in order to identify methods of privilege escalation, initial access, and overall gateway security.

The client for this Project is PA Consulting. PA consulting motto is “We believe in the power of ingenuity to build a positive human future”. We aim to meet this goal by assisting to secure given LoRaWAN devices and making them more secure. PA consulting deliver a number of different services both involving technical security and not. For individuals both in the company and outside of the client it is possible that the critical vulnerabilities discovered will contribute to the client’s digital safety and uphold the CIA triad of confidentiality, integrity and availability.

The Agile methodology was used to manage the team, with meetings held biweekly. The team is allocated tasks biweekly. The Agile methodology was used, as it best fit the changing requirements and scope of a penetration test. The Agile approach lets the team change the approach as we go and can compensate for any present issues.

A RAID log will be kept for the client. This will include risks, assumptions, issues and dependencies for the project. This allows us to quickly update the client during biweekly meetings about encountered issues in all phases of the project. This is shown to the client biweekly to keep them updated about present issues.

A Gantt chart will be used to keep track of present tasks, and to discover if the team is on track. Due to the nature of this project, this may change as the team progresses across the penetration test. If we are not on track with the Gantt chart, the client will be alerted, and a team meeting will be held to decide how to proceed, how to make up lost time and what we can do to mitigate the risk in future.

Several hacks stem from compromise of IoT devices, which are held to fewer industry security standards. An example of this is the large data leak from Target in 2013. The malicious actor initially accessed the system by compromising internet connected Air Conditioners. (infosecurity-magazine.com, 2014). This is an example of the importance of IoT security to prevent large breaches. Throughout this project we aim to assist in preventing similar breaches.

The success criteria for the project include comprehensive identification and documentation of vulnerabilities along with risk ratings for each finding and actionable mitigations to continue to enhance the security of the LoRaWAN devices.

While the used scope was large, this was approached by each member given a different section that aligned with their personal experience and interests. This was done to motivate the team members in order to do align with their own interests.

Overall, LoRaWAN technology security allows us to help the client ensure security in their own use cases and contributes to the overall Dragino security.

## Aim

This project will aim to test the complete security of the LoRaWAN network. This project will test the security of:

* LoRaWAN protocol communication
* HTTP web server security
* System integrity

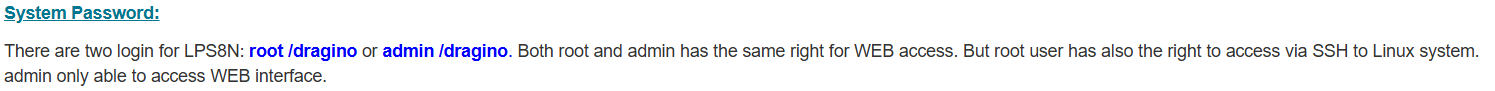
We will define success in this project, not by how many vulnerabilities are found, but by following a methodology to ensure full application coverage.

# Method

## Vulnerability Analysis

### Publicly available admin account credentials

The default credentials for the gateway are publicly available and easy to find (Figure 3.3.1.1), and are linked to the root account on the gateway, meaning that they allow for high level system access by default. These are also both very insecure, simply being the username “root” or “admin”, a common default for a high level user, and the password simply being “dragino”, the name of the company that produces this specific product, which means it is easily guessable, and likely to appear on specialised wordlists that would be used for password cracking.



*Figure 3.3.1.1: Default credentials for the gateway.*

Once logged in, the web interface provides detailed information as to the gateway’s hardware information (Figure 3.3.1.2) and provides various functionality to change options related to underlying systems on the gateway, mainly such as the password functionality and the SSH service (Figure 3.3.1.3), and requires no further authentication or authorization.

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 3.3.1.2: The gateway’s firmware and MAC address information.*

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 3.3.1.3: Password and service management options.*

### Weak cryptography through http protocol

The gateway utilises HTTP by default (Figure 3.3.2.1), which poses an issue as data sent via this protocol isn’t encrypted at all, presenting a potential issue if communications between a user and the web app are recorded by a third party, potentially using a tool such as Wireshark (Figure 3.3.2.2).

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 3.3.2.1: The HTTP service is enabled by default.*

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 3.3.2.2: The unencrypted credentials being recorded in a Wireshark session*

These credentials are also sent in every packet to/from the device, just base64 encoded. This means that even if the initial login packet wasn’t captured, it would still potentially be possible to gleam the credentials in use on the system, had they been changed from the default.

### CVE-2024-6387

The version of OpenSSH installed on the gateway, as seen in the Nmap scans, is (insert version). This is notably potential vulnerable to CVE-2024-6387, also known as regreSSHion. This utilises a race condition present in this version of OpenSSH and can lead to running unauthorised commands. An online proof of concept tool was used to test this (Karmakstylez, 2024). This code featured both scanning (Figure 3.3.3.1) and exploitation (Figure 3.3.3.2) tools.

A computer screen with text and images

AI-generated content may be incorrect.

*Figure 3.3.3.1: Utilising the scanning capabilities to confirm the OpenSSH version running.*

A screenshot of a computer screen

AI-generated content may be incorrect.

*Figure 3.3.3.2: The exploitation capabilities of the software.*

Because of the race condition behind this exploit, attempts to test this exploit is time consuming, with no method of speeding up attempts. It also has a very low success rate, with the tool making tens of thousands of attempts, and sometimes not having a single success (Figure 3.3.3.3). However, there was a single recorded successful attempt (Figure 3.3.3.4).

A computer screen with white text

AI-generated content may be incorrect.

*Figure 3.3.3.3: Twenty thousand failed attempts.*

A screen shot of a computer

AI-generated content may be incorrect.

*Figure 3.3.3.4: Successful exploitation.*

### Insecure File Upload

There is a lack of file validation on the MQTT Forwarder page (Figure 3.3.4.1), both to the file type and contents. This could potentially allow for unintended files to be uploaded to the gateway (Figure 3.3.4.2). This led to further inspection of the file handling procedure, which revealed that this is handled using a Linux copy command. This further suggests that this is vulnerability that could be exploited to uploaded user created files to unauthorized locations on the device.

A screenshot of a computer

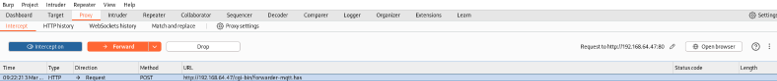
AI-generated content may be incorrect.

*Figure 3.3.4.1: The MQTT Forwarder page, allowing for specific file uploads*



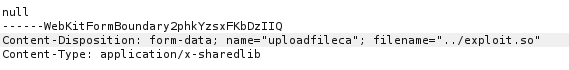
*Figure 3.3.4.2: A “py” file uploaded onto the gateway, not respecting correct file types*

This was tested by using burp suite to intercept the request used when a file is uploaded to the gateway (Figure 3.3.4.3). The uploaded file’s respective filename parameter was then changed to include a path traversal sequence (Figure 3.3.4.4), a sequence of characters that is used by the Linux file system to indicate that is should navigate up a directory level. Upon processing the request, the uploaded file can be seen in the “/usr/local/dragino/chirpstack” (Figure 3.3.4.5) folder, as opposed to the “/usr/local/dragino/chirpstack/ca” folder that was seen when file type validation was being tested.

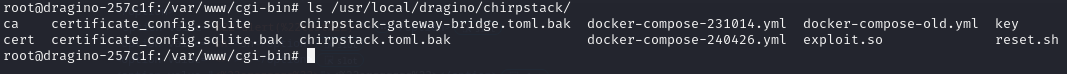
A white background with black text

AI-generated content may be incorrect.

*Figure 3.3.4.3: The upload file request caught in the proxy tool Burpsuite*



*Figure 3.3.4.4: Editing the filename parameter of the upload request.*



*Figure 3.3.4.5: Confirming this causes the file to be uploaded to a directory further up the tree*

### HackRF Radio Wave Interception

One of the major security points discussed early on by the group was the potential security of the transmissions between the sensors and the gateway. This was investigated by using a tool called HackRF, which allowed for recording and playback of the radio frequencies used by LoRaWAN.

HackRF requires several different pieces of software to work correctly. While the tool allows for recording the communications in an easy manner, decoding those communications requires specialist software that properly analyses the radio waves provided. One of these tools is called inspectrum and is used to create a spectrogram of data (Figure 3.3.5.1).

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 3.3.5.1: The inspectrum interface*

This generates a symbols table (Figure 3.3.5.2) that consists of the binary representation of the signal recorded, and allows for greater analysis of the data received. LoRaWAN is an encrypted standard, and thus requires decrypting for a large majority of the data transferred. This can be seen below (Figure 3.3.5.3).

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 3.3.5.2: The generated binary symbols table.*

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 3.3.5.3: LoRa Packet decoder, displaying some relevant information.*

The ability to record transmissions also allows for these recorded transmissions to be replayed, though this has some limitations. The transmissions that are replayed seem to need to have not initially been received by the gateway, else any repeated attempts seem to do nothing. This means that attempts to edit this data for receiving are tedious, as there is no way of seeing what varies between attempts in a decrypted form, meaning that this would have to be tested in a completely blind manner, and it is therefore unfeasible to do within a reasonable time frame.

# Procedure

## Network/Device Overview

### Overview of Network

The LoRaWAN network was setup through a multitude of provided devices. These devices were connected to a host machine on the University’s network inside a private lab meant for cyber security students. The system included a Router and Switch directly connected to the host machine via an ethernet cable as well as several sensor devices that were connected to the router. Below is a screenshot of the entire system in full as the testers analysed the devices:

A computer and electronic devices on a table

AI-generated content may be incorrect.Figure 3.1.1. LoRaWAN system setup in university laboratory.

### Router

A Dragino Model LoRaWAN kit v3 router was provided by the sponsor to connect the devices to the host machine. This router has USB-A port, an ethernet port, a power cable, and a LoRa antenna attached. These ports were all utilised for difference devices and connections. The serial number associated with the make of the router was Ips8v2130784.

A white box with a red light and a yellow cable

AI-generated content may be incorrect.

Figure 3.1.2 Dragino LoRaWAN IoT Kit v3 Router.

### Switch

A tp-link 5-port Gigabit Desktop Switch was provided to the testers for connectivity purposes. The switch contained 5 ethernet cable ports and a power cable attached. The switch was connected to the host device, the Dragino router from 3.1.1. as well as a second host device setup across from the original. The serial number for the switch was 22292X3002826.

A black box with yellow and white cables

AI-generated content may be incorrect.

3.1.3 tp-link 5-port Switch as setup in the university laboratory.

### Moisture and EC Sensor

A Dragino LoRaWAN Soil Moisture and EC sensor was provided to the testing group as a low frequency device. This device sent packets to the router that were captured and analysed through various penetration testing techniques throughout the testing process. The serial number of the device was LST25696909.

A hand holding a black antenna

AI-generated content may be incorrect.

Figure 3.1.4 Dragino LoRaWAN Soil Sensor as connected in the system.

### Liquid Level Sensor

A Dragino LoRaWAN IoT Liquid Level Sensor was provided as another LoRa frequency device connected to the router. This device sent packets that were captured and analysed by the team as with the Soil Sensor. The serial number of this device was LST25447873.

A black box with a white label on it

AI-generated content may be incorrect.

Figure 3.1.5 Dragino LoRaWAN Liquid Level Sensor connected to the system at the university.

### Temperature and Humid Sensor

A Dragino temperature and humidity sensor was provided to the team as a LoRaWAN device that connected to the router. The device transmits a LoRa frequency that the router captured packets from. The serial number of this device was HT65N698724.

A white device with a wire on a table next to a keyboard

AI-generated content may be incorrect.

Figure 3.1.6. Dragino Temperature and Humidity device connected on the LoRaWAN system.

### High Gain USB Adapter

A tp-link High Gain Wireless Dual Band USB Adapter was provided to the testers as a connective adapter potentially utilised for connecting to the devices. For the remainder of the test, the adapter was left unused as the router provided did not have enough ports attached to allow for the adapter’s connection. The serial number of this device was 222A429002014.

A wi-fi adapter and a cable

AI-generated content may be incorrect.

Figure 3.1.7. tp-link Wireless Adapter provided to the testers by the sponsor.

### Host Machine 1

There were several host devices connected either directly or through the router of the network. This first machine was an HP EliteDesk 800 G6 Small Form Factor PC. The PC utilized Ubuntu v22.04.5 LTS and connected directly to the router via an Ethernet port. This device was utilized as the main host device, responsible for the discovery of many permission-based vulnerabilities found later in the testing. The IP Addresses associated with this device were 192.168.64.1 and 192.168.2.1.

### Host Machine 2

There was a second host machine associated with this network. This machine was manufactured the same as the first, HP EliteDesk 800 G6 Small Form Factor PC. However, this PC had Kali Linux v2024.4 installed as the operating system of choice. This machine was utilized for the LoRaWAN auditing framework. The IP address associated with this machine was 192.168.64.26.

### Laptop

One of the testers brought in their very own Lenovo ThinkPad T450 for the testing process. This host was used as an extra machine for the testers to run any tests that required a machine to be on for days at a time. The machine had a kali linux virtual machine installed to conduct most examinations.

## Information gathering

### Nikto

The analysts first conducted a general scan of the host device connected to the network. The scan targeted 80 ports on the 192.168.64.47 IP address associated with the router. The result of this scan can be found in Appendix A as several vulnerabilities were identified. The server discovered associated with the IP address in the scan was the routers web server. The header of this web server appeared to have no anti-clickjacking imports, leaving the server susceptible to snooping from malicious threat actors. Furthermore, the device appeared to have no protections from third party manipulation, giving threat actors the ability to remotely alter permissions on the router from their own host machine.

### Nmap

After the testers conducted a thorough Nikto scan of the webserver associated with the LoRaWAN router, they proceeded onward and conducted an Nmap scan. This scan provided a more generalized and comprehensive evaluation of the network as a whole. The scan can be found in Appendix B and showed the Ubuntu machine on port 22 connected as well as the web server on post 80.

### LoRaWAN Auditing Framework

During the preliminary research of this exploitation the group was made aware of an auditing software developed specifically for LoRaWAN devices. This framework utilized docker functionality to test several known exploitations of the LoRaWAN devices. On the kali linux host device, the analysts attempted to install and run the framework against the system for several weeks of the testing process. The conclusion at the end of this rigorous setup process was that the framework was unfortunately out of date and unusable in the current year. The version of docker, go, kali, and LoRaWAN all are six years ahead of where the framework was meant for. This resulted in the testers abandoning the audit for the remainder of the testing process.

# Results

## Summary

The LoRaWAN Dragino gateway has revealed a substantial range of vulnerabilities that could compromise the networks security. These vulnerabilities include the one and only admin account credentials being unchanged and available online in the user manual for the Dragino gateway, allowing for unauthorized exposing key settings like . Usage of weak protocols for data transmission i.e. http over https allowing for unauthorized exposing key settings the firmware version, Eth0 address, and Wi-Fi Mac Address. Note that due to their only being one account for the gateway that being the exposed admin account the process of privilege escalation is not necessary for this setup. SSH regression possibly allowing for remote code execution if successful(CVE-2024-6387). There is also a weakness through insecure/unvalidated file uploads allowing for the upload of malicious files. There were other prominent areas explored which yield mixed results such as interception of radio wave packets using HackRF in which the interception was successful but the data on the packet itself used strong encryption methods meaning no valuable data could be extracted. Not only this we attempted to use a tool known as LoRaWAN Auditing Framework which proved unsuccessful as the dependencies for its usage were outdated making it hard to find the specific dependencies and being incompatible with our setup.

## Exploits and Vulnerabilities

### Publicly available admin account credentials

The Default credentials for the Dragino LoRaWAN gateway are available online through the user manual as seen in the related [procedure](#_Publicly_available_admin) section. Said credentials are for the only gateway account that being the admin account. As a result, privilege escalation is unnecessary for this security test. Once logged an attacker can see settings which are also seen in [Appendix D](#_Appendix_D_Other) . These setting expose vital System information which reveals the firmware version, Eth0 address, and Wi-Fi Mac Address. Meaning attackers can exploit known vulnerabilities on this firmware and have Mac addresses used for attacks with related tools. The lack of unique credentials significantly reduces the security of the system, making it highly susceptible to unauthorized access. The results from this can be seen in figures 4.1 and 4.2.

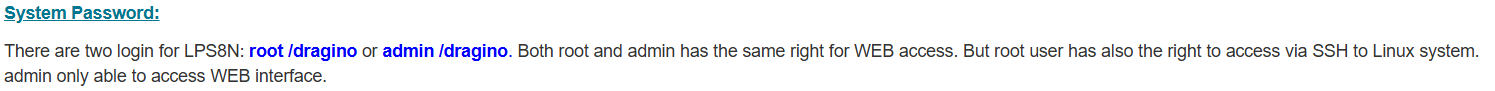


Figure **Error! No text of specified style in document.**‑1 The default credentials as seen in the gateway manual

A screenshot of a computer

AI-generated content may be incorrect.

Figure **Error! No text of specified style in document.**‑2 Settings which can be seen and modified after accessing the admin account

### Weak cryptography through http protocol

Through the weak cryptography of the LoRaWAN Dragino Gateway webpage with the HTTP protocol an attacker could perform a man-in-the-middle attack using Wireshark or a similar tool manual like burpsuite as seen in the related [procedure](#_Weak_cryptography_through) section. Discovering the admin account credentials. Similar to the previous vulnerability once logged an attacker can see are also seen in [Appendix D](#_Appendix_D_Other) . These setting expose vital System information which reveals the firmware version, Eth0 address, and Wi-Fi Mac Address. Meaning attackers can exploit known vulnerabilities on this firmware and have Mac addresses used for attacks with related tools this vulnerability highlights the importance of implementing secure communication protocols. The results from this can be seen in figure 4.3.



Figure 4.3 The default credentials intercepted through a man-in-the-middle-attack with Wireshark

### CVE-2024-6387

This vulnerability is related to the OpenSSH service and allows for remote code execution on the host system in this case the LoRaWAN network. Our attempt to exploit this vulnerability failed however as seen in our related [procedure](#_CVE-2024-6387) section. This could be due to a limited setup or other unknown reasons so further investigation into this CVE and different setups for the LoRaWAN network is recommended as it could potentially allow attackers to compromise the LoRaWAN network remotely. The results from this can be seen in figure 4.4.

A screen shot of a computer

AI-generated content may be incorrect.

Figure 4.4 The process of attempting to exploit CVE-2024-6387

### Insecure File Upload

Due to a lack of file upload verification on the LoRaWAN gateway it is possible to upload files of any kind onto the network. As seen in the related [procedure](#_Insecure_File_Upload) section using Haserl its possible to use the copy command to move a foreign file onto the system in this case “test.py”. It is also possible to do this using a proxy-based tool such as burpsuite. As seen in the related procedure section there has been an interception of a packet which is related to the file upload on the LoRaWAN gateway which has then been intercepted and changed the sent file to our foreign file “exploit.so”. This vulnerability is significant because it allows attackers to execute/upload malicious code/files potentially compromising the entire network. The results from this can be seen in figures 4.5 and 4.6.



Figure 4.5 The uploaded and unverified test.py file

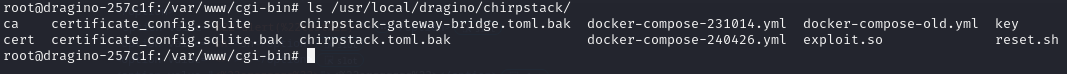


Figure 4.6 The uploaded and unverified exploit.so file

### LoRaWAN Auditing Framework

As a group we discovered a tool which at the time we believed could be of wonderful use. To use the tool in question that being the LoRaWAN Auditing Framework. This framework utilizes functions and tools like docker and python to test exploitations relating to LoRaWAN networks. However, upon attempting to use this framework on the testing environment many issues occurred mainly relating to the framework relying on outdated versions of its tools and functionality stalling overall progress for the project. Due to this as a team we decided to stop our attempts at using this framework tool therefore yielding no results to note.

## Communications Analysis

### HackRF and Radio Waves

We intercepted radio wave packets related to the Dragino LoRaWAN gateway and sensors as seen in the related [procedure](#_HackRF_Radio_Wave) section. A successful attempt was conducted to intercept an uplink from the sensors and subsequently replay that to the gateway, This was then accepted as a valid packet not previously received. However, the packets proved to be heavily encrypted meaning attempts to decrypt the contents of the uplinks were unsuccessful. This indicates that while the gateway is vulnerable to replay attacks, the encryption of the packets themselves is robust and effectively protects the data from being accessed. The results from this can be seen in figure 4.7.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4.7 The captured packet from the replay attack seen to be encrypted

# Discussion

*(around 900-1100 words, 1 student to write the Discussion)*

## General Discussion

Our engagement comprised the objective of conducting a full-scope penetration test on LoRaWAN IOT infrastructure run by the Company, with the goal to identify vulnerabilities, assess risks and where necessary posit solutions, related in particular to network communication, device security and backend configuration.

**So how did the Team do** – was the project and the Team successful in achieving its aim? Broadly speaking, yes. It identified two serious, high-risk vulnerabilities in (i) publicly available administration account details; and (ii) a lack of file upload verification; together with (iii) a medium risk of a configuration panel using unencrypted http traffic. These identified vulnerabilities that could allow hackers to significantly disrupt services, steal sensitive data, or deploy malware into the Company’s IOT environment. In testing, the Team was also able to intercept radio wave packets related to the Dragino LORAWAN gateway and sensors although the encryption of the packets themselves was robust and so effectively protected the data from being assessed.

While the Team did identify significant vulnerabilities, it did also fail in its attempts to exploit two other areas of potential vulnerability.  Testing for the CVE-2024-6387 vulnerability (otherwise known as *RegreSSHion*) is related to the Open SSH service and allows for remote code execution on the host system (ie the LORAWAN network). The failure in testing could be due to a limited setup or outdated software however frankly it was not entirely clear to the Team. Similarly, the Team attempted to use a LORAWAN Audit Framework tool to utilize functions like docker and python to test exploitation relating to the LORAWAN network however were unsuccessful in using such tool.

Consequently, while the Team has produced a relatively comprehensive report which identified and documented significant vulnerabilities along with risk ratings, it is recognized it did struggle with its testing in two areas. Nevertheless, it did identify actionable, specific and effective mitigations and solutions for such vulnerabilities, including for Firmware updates, secure file handling and credential management, to enhance the security of the LoRaWAN devices.

## Conclusions

The vulnerabilities identified by the Team could all have a serious impact on the Client’s business if left unremedied. They could potentially lead to system downtime and consequent business discontinuity as thevulnerabilitiesneed to be identified and remedied/mitigated; reputational damage and loss of customer trust leading to reduced sales; compliance issues with possible fines; financial loss and exposure through breach of contract claims in litigation; higher insurance premiums; and talent and customer retention issues if the vulnerabilities continue unmitigated.

Fortunately, we have been able to identify and recommend effective and relatively simple solutions for the vulnerabilities identified:

1. The default credentials for the Dragino LORAWAN gateway are available online through the user manual allowing hackers to log-in as admins. Once logged in an attacker can see and modify settings such as the firmware version, EthO address, Wi-Fi Mac address and SSH/HTTP ports.

The lack of unique credentials significantly reduces the security of the system, making it highly susceptible to unauthorised access. This can be resolved by simply adding users and randomising credentials given out.

1. The lack of file upload verification on the LORAWAN gateway is significant because it allows attackers to execute/upload malicious code and/or files potentially compromising the whole network, i.e., a file could be uploaded with no validations as to the type or contents of the file. In addition to randomising credentials, mitigation requires the use of proper file validation, and especially to ensure the files are not used with a cp. The Company should use character input validation ensuring  “../” or variations of it do not appear anywhere. Further the Company simply utilising proper file handling within haserl would also help since the vulnerability itself simply comes from some very insecure code.
2. The configuration panel using unencrypted HTTP traffic makes it vulnerable to credential theft and man-in-the-middle attacks using tools such as Wireshark or  Burpsuite.

The solution to this vulnerability requires the implementation of secure communication protocols. The Company could use something like openssl to generate certificates, and use HSTS cookie to ensure HTTPS is used.

1. The testing for CVE-2024-6387 vulnerability (otherwise known as RegreSSHion) related to the Open SSH service and could allow hackers to compromise the LORAWAN network remotely. The test failed, however for completeness we recommend this risk nevertheless be mitigated simply by the Company obtaining and installing an updated version of Open SSHsince this vulnerability has been patched in all recent versions.

1. Similarly, the attempt to use the LORAWAN Auditing Framework tool which could utilize functions like docker and python to test exploitations relating to LORAWAN networks failed, largely because the framework relied on outdated versions of its tools and functionality and was incompatible with modern OS versions and dependencies. While the auditing framework tool could have revealed several vulnerabilities that we couldn’t test, on reflection the Team felt most of them we were able to test for using  HackRF. While an updated version of the framework tool doesn’t really exist, we could create for the Company a simple version of this framework. This would allow us to test the communications using captured keys potentially allowing us to decrypt communications.

## Future Work or Countermeasures

The dangers and exposure of the Company to serious financial, reputational and operational loss through not addressing the vulnerabilities exposed are outlined above. We have identified the need for the Company to randomise credentials, implement proper file handling and validation, and secure communication protocols, and in some cases to update tools. We could assist the Company in designing and implementing these fixes. However, we would also suggest that we be engaged by the Client to go deeper into hardware exploitation, to develop or update an auditing framework tailored to modern LORAWAN deployments by the Company, and to investigate long-term fixes, such as firmware patching strategies or building tools to better automate testing for the Client’s IOT devices.

## Call to action

Finally, we would also suggest consideration be given to the Team being engaged to investigate long-term fixes, such as firmware patching strategies or building tools to better automate testing for Client’s IOT devices.

We would welcome the opportunity to discuss this Report, and to explain and quote for any and all of the suggested further work identified above, at your convenience.  We can be contacted at the address below:

burgerjoint64WOWwhatAdeal@gmail.com

# References

The Things Network. (n.d.). Message Types. [online] Available at: https://www.thethingsnetwork.org/docs/lorawan/message-types/.

‌IBM (2023). IBM Security Report: Cost of a Data Breach for UK Businesses Averages £3.4m. [online] IBM UK Newsroom. Available at: https://uk.newsroom.ibm.com/24-07-2023-IBM-Security-Report-Cost-of-a-Data-Breach-for-UK-Businesses-Averages-3-4m.

‌Trend Micro. (2021). Low Powered and High Risk: Possible Attacks on LoRaWAN Devices. [online] Available at: https://www.trendmicro.com/en\_gb/research/21/a/Low-Powered-but-High-Risk-Evaluating-Possible-Attacks-on-LoRaWAN-Devices.html.

Cerrudo, C., Cto, I., Esteban, M. and Fayo (2020). LoRaWAN Networks Susceptible to Hacking: Common Cyber Security Problems, How to Detect and Prevent Them. [online] Available at: https://act-on.ioactive.com/acton/attachment/34793/f-87b45f5f-f181-44fc-82a8-8e53c501dc4e/1/-/-/-/-/LoRaWAN%20Networks%20Susceptible%20to%20Hacking.pdf.

Infosecurity Magazine. (2014). Target Hackers May Have Gotten In Through the Air Conditioner. [online] Available at: https://www.infosecurity-magazine.com/news/target-hackers-may-have-gotten-in-through-the-air/.

‌

# Appendices

## Appendix A – Nikto Scan Result

Nikto -h 192.168.64.47

- Nikto v2.5.0

---------------------------------------------------------------------------

+ Target IP: 192.168.64.47

+ Target Hostname: 192.168.64.47

+ Target Port: 80

+ Start Time: 2025-01-27 08:42:21 (GMT-5)

---------------------------------------------------------------------------

+ Server: lighttpd/1.4.65

+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .

+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.

+ 9868 requests: 0 error(s) and 4 item(s) reported on remote host

+ End Time: 2025-01-27 08:46:22 (GMT-5) (241 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested

## Appendix B – Nmap Scan Result

Sudo Nmap -p- -sC -sV -oN full\_scan.txt 192.168.64.47

[Sudo] password for kali:

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-27 08:41 EST

Stats: 0:02:49 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 66.67% done; ETC: 08:44 (0:00:21 remaining)

Stats: 0:04:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 66.67% done; ETC: 08:47 (0:01:07 remaining)

Nmap scan report for 192.168.64.47

Host is up (0.00096s latency).

Not shown: 65532 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 256 2c:19:3d:f2:ed:a4:c4:ed:c9:15:ce:4e:ca:0d:11:f8 (ECDSA)

|\_ 256 0d:2b:aa:45:f4:1c:15:f9:38:8f:59:c7:37:e6:40:3e (ED25519)

80/tcp open http lighttpd 1.4.65

|\_http-server-header: lighttpd/1.4.65

|\_http-title: Site doesn't have a title (text/html).

9517/tcp open unknown

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 303.08 seconds

## Appendix C - Deliverables & requirements (Required)

**Agreement Form: Project Deliverables**

|  |  |
| --- | --- |
| **Group Name, Names of Team Members, and Programme** | **Ryan Petrie, Issac Potts, Ben Poulton, Annie Place, Mattia Pulvirenti, Joey Hall** |
| **Subject specialist’s Name (Client)** | **Peter Bennet** |
| **The deliverables listed below will be submitted by the team by the due date.** | |
| **Part A deliverables** | Compromise device level security  Compromise network level security  Compromise gateway security  vulnerability disclosure reports |
|  | Client presentation at end of term  Client presentations for each meeting  Presentation for university  White paper report on findings |
| **Subject specialist’s (Client) signature** | **A blue line drawn on a white surface  AI-generated content may be incorrect.** |
| **Team members’ signatures** | **Ryan Petrie**  **Issac Potts**  **Ben Poulton**  **Annie Place**  **Mattia Pulvirenti**  **Joey Hall** |

**Agreement Form: Requirements**

Group Name: EH8

Team members: Ryan Petrie, Issac Potts, Ben Poulton, Annie Place, Mattia Pulvirenti, Joey Hall

Project Title: LoRaWAN Network IoT Devices Security Test

Please refer to the attached documentation for full details of the project. The requirements are listed in Table 1. The signatures below indicate that the requirements for this project have been agreed by the project stakeholders.

Any changes to the project documentation should be made using the correct change authorization procedure agreed with the programme specialist.

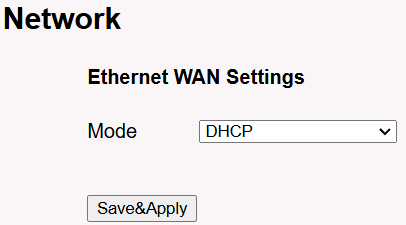
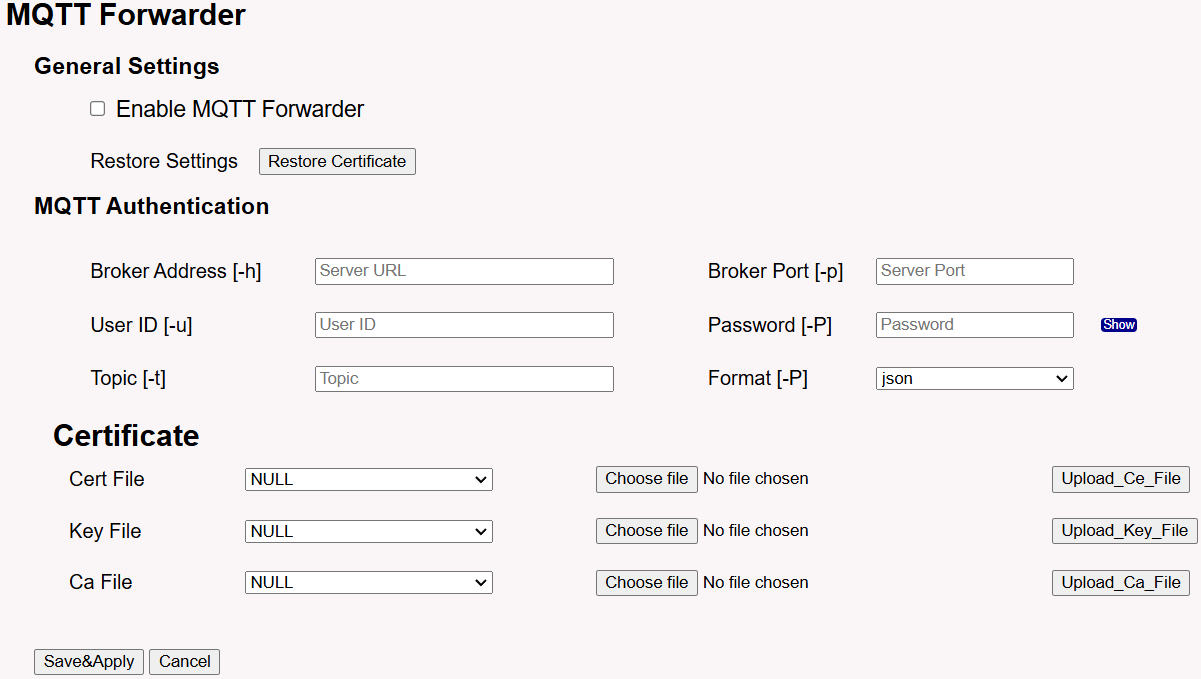
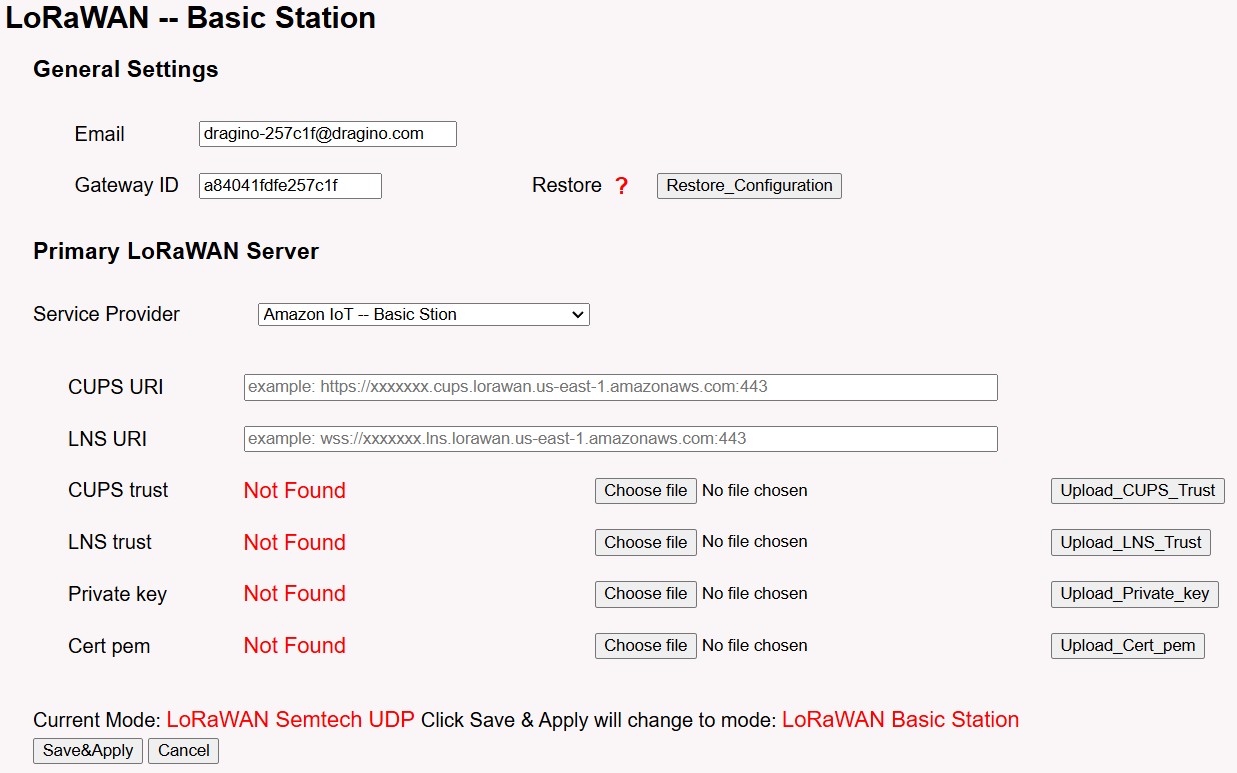
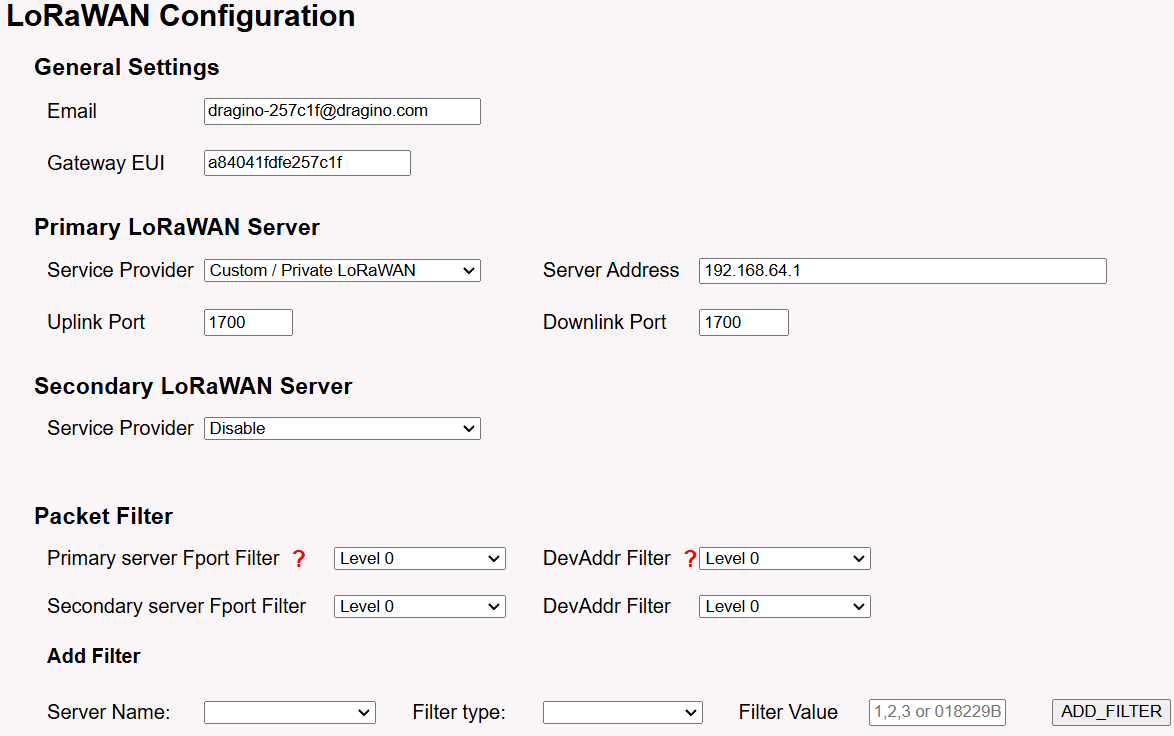
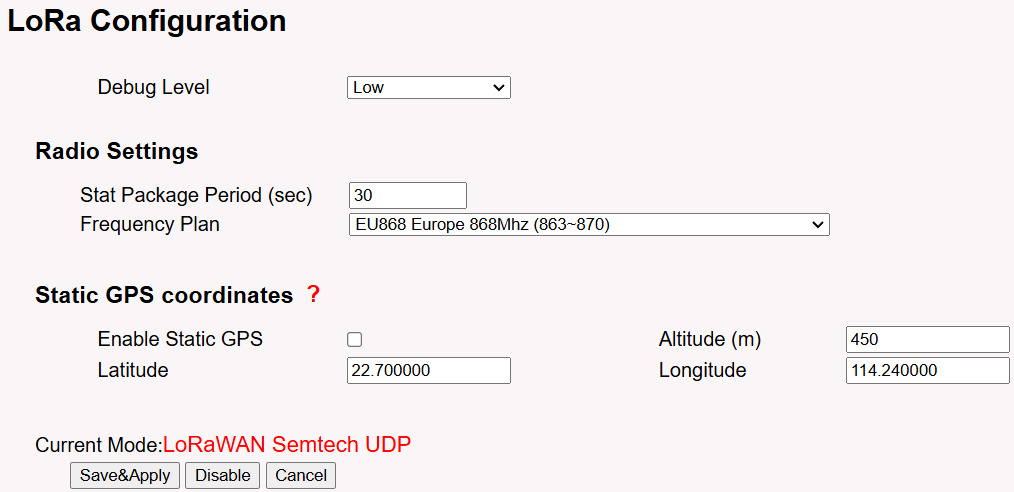
Table 1

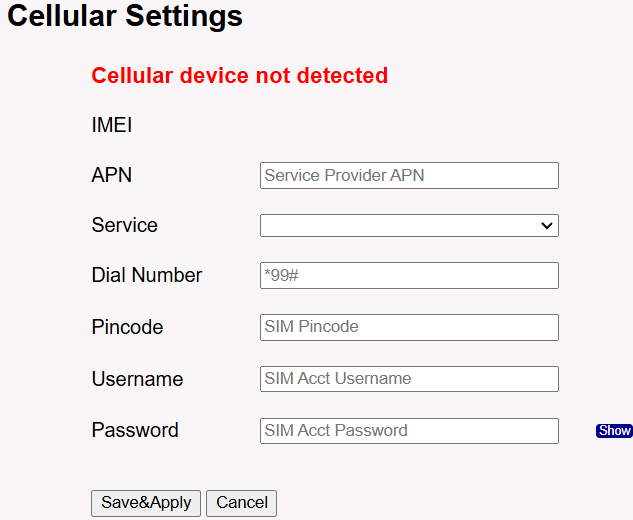
|  |  |
| --- | --- |
| **ID** | **List of Agreed Requirements** |
|  | Compromise device level security  Compromise network level security  Compromise gateway security  Vulnerability disclosure reports  Client presentation at end of term  Client presentation for each meeting  University presentation for coursework  White paper report on findings |

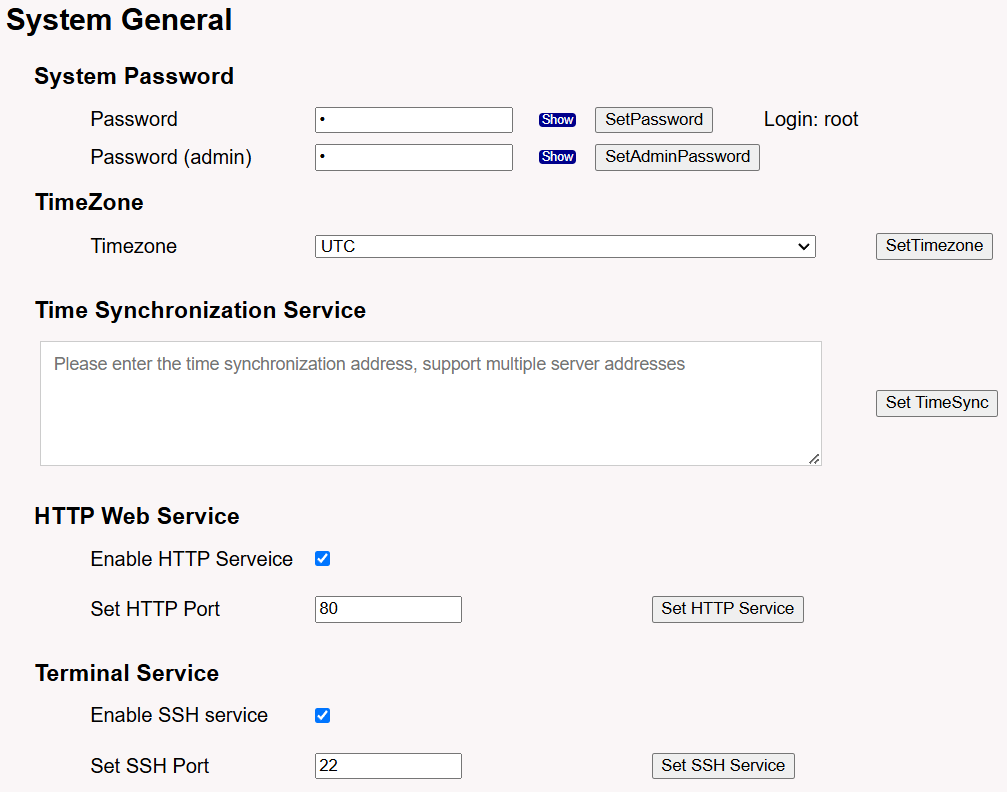
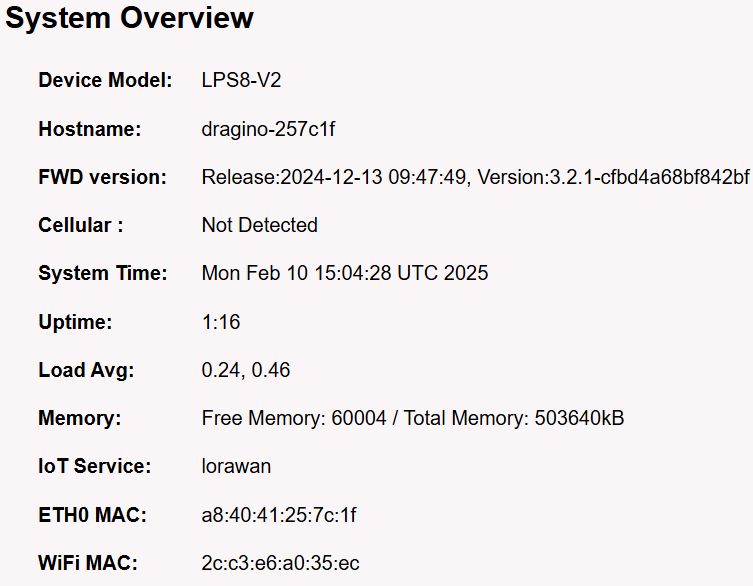
|  |  |  |
| --- | --- | --- |
| **Stakeholders** | **Signatures** | **Date** |
| Team members | Ryan Petrie  Issac Potts  Ben Poulton  Annie Place  Mattia Pulvirenti  Joey Hall | 14/04/2025 |

|  |  |  |
| --- | --- | --- |
| Subject Specialist | **A blue line drawn on a white surface  AI-generated content may be incorrect.** | 14/04/2025 |
| Client (if applicable) | **A blue line drawn on a white surface  AI-generated content may be incorrect.** | 14/04/2025 |

## Appendix D Other settings discovered from access to Admin Account

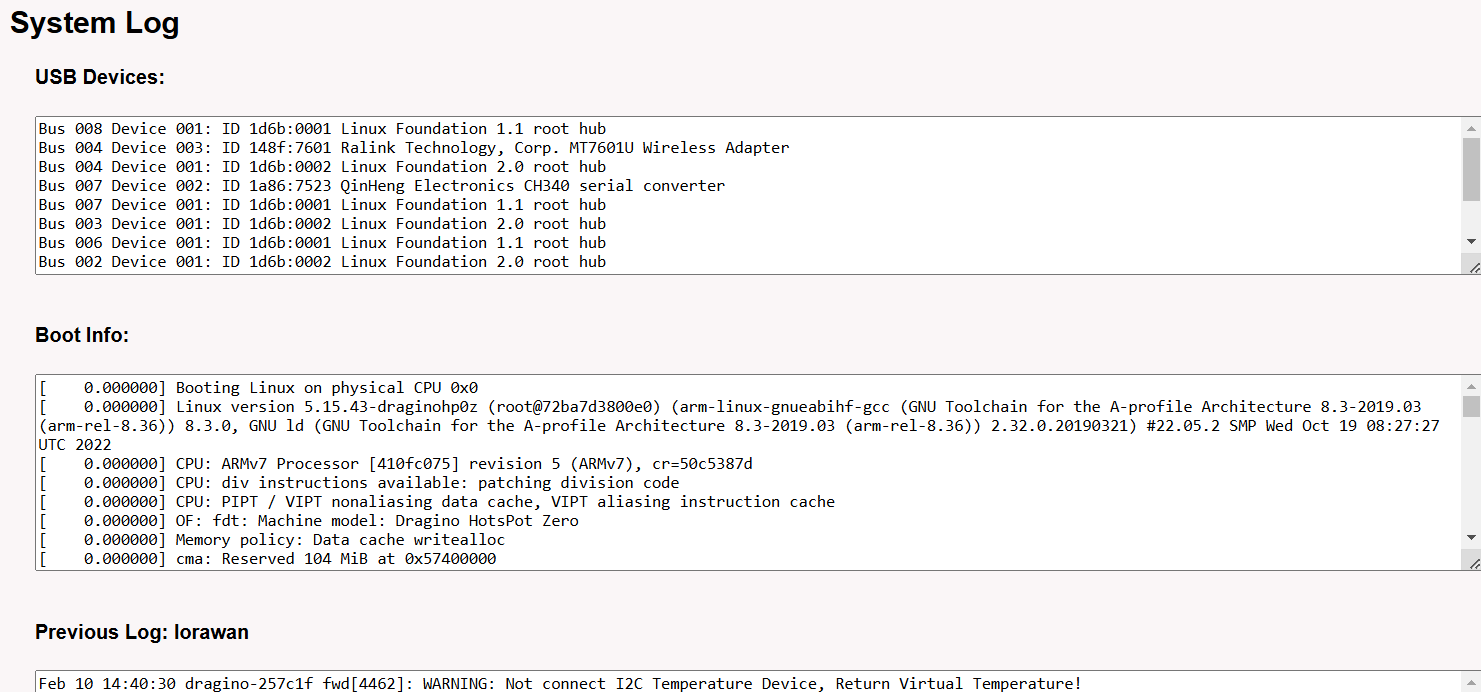
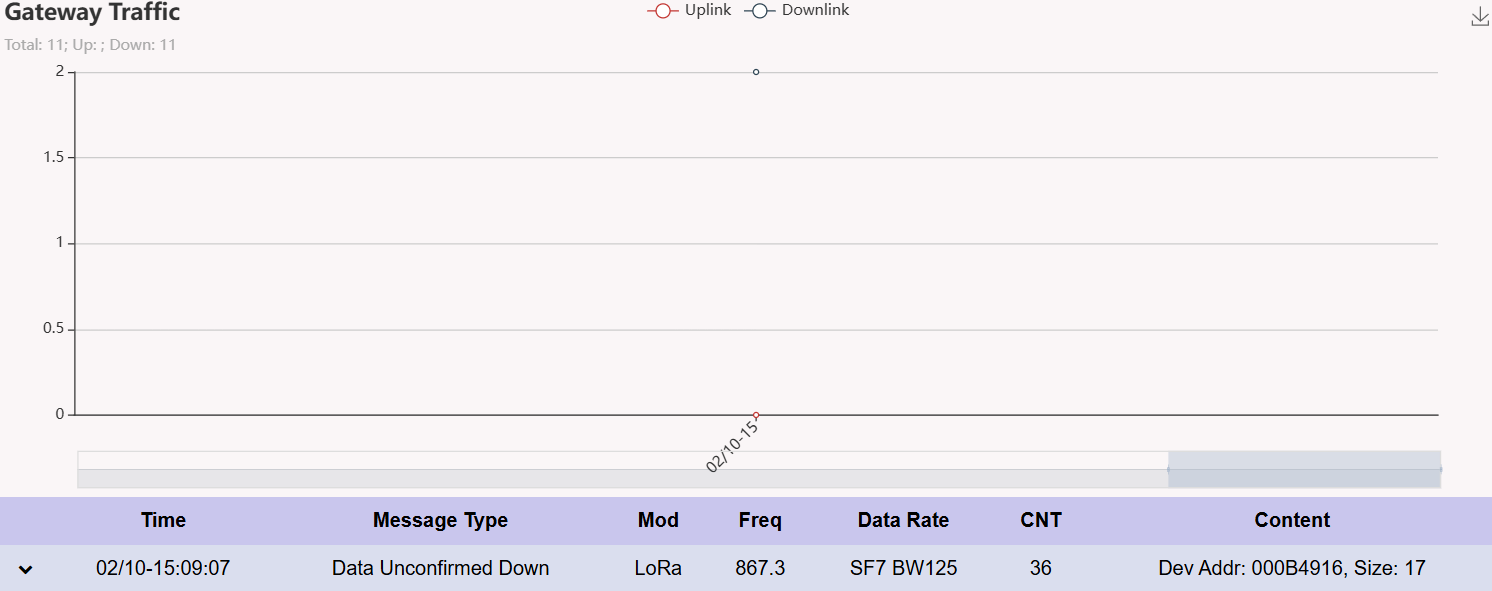
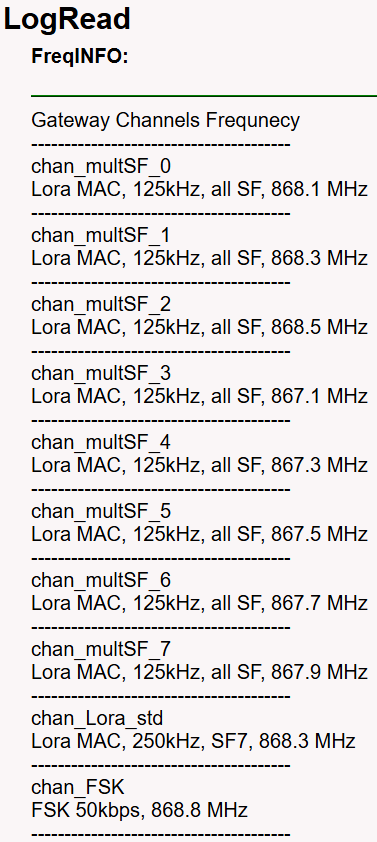
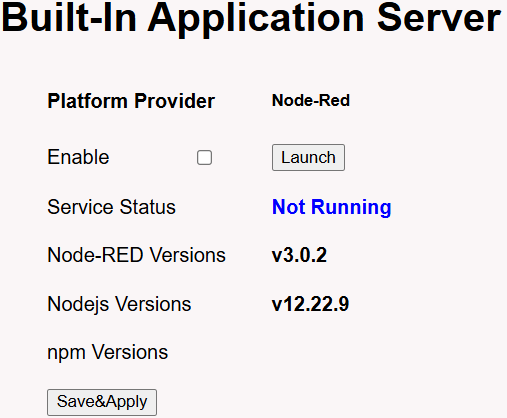
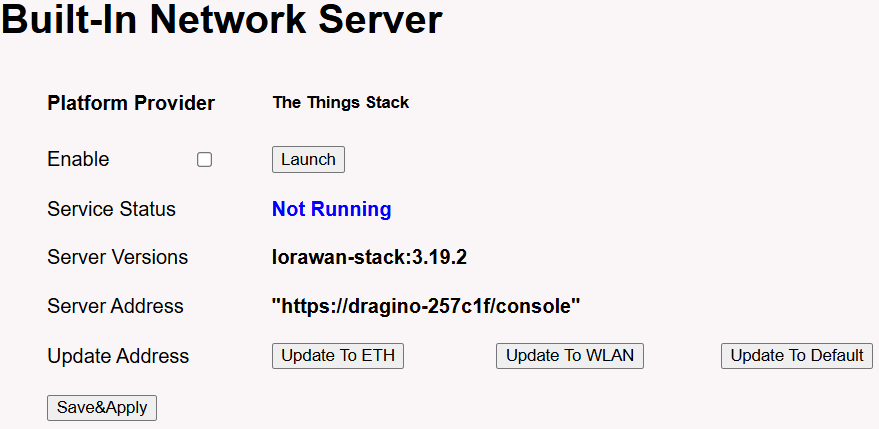
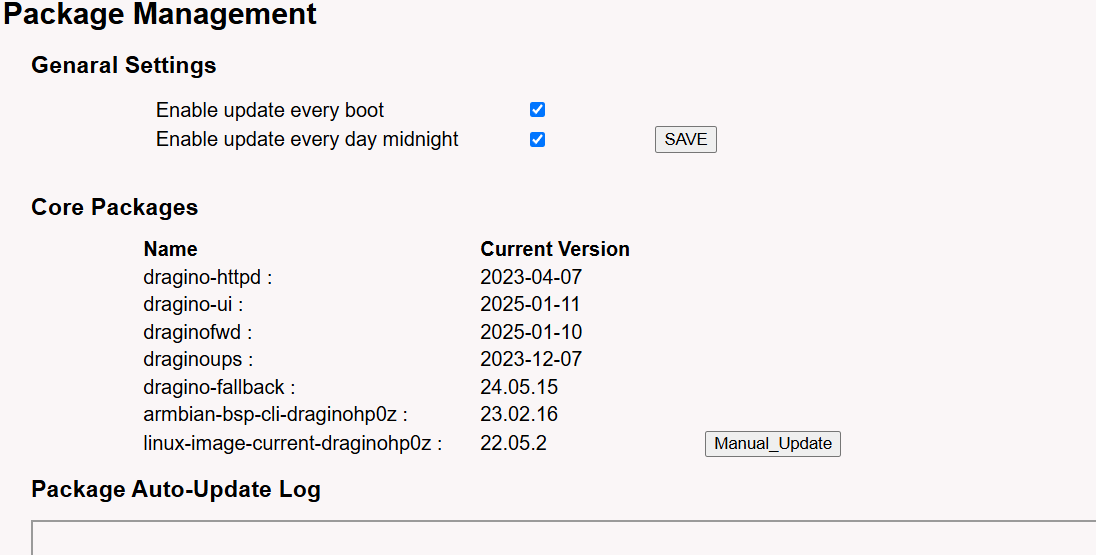
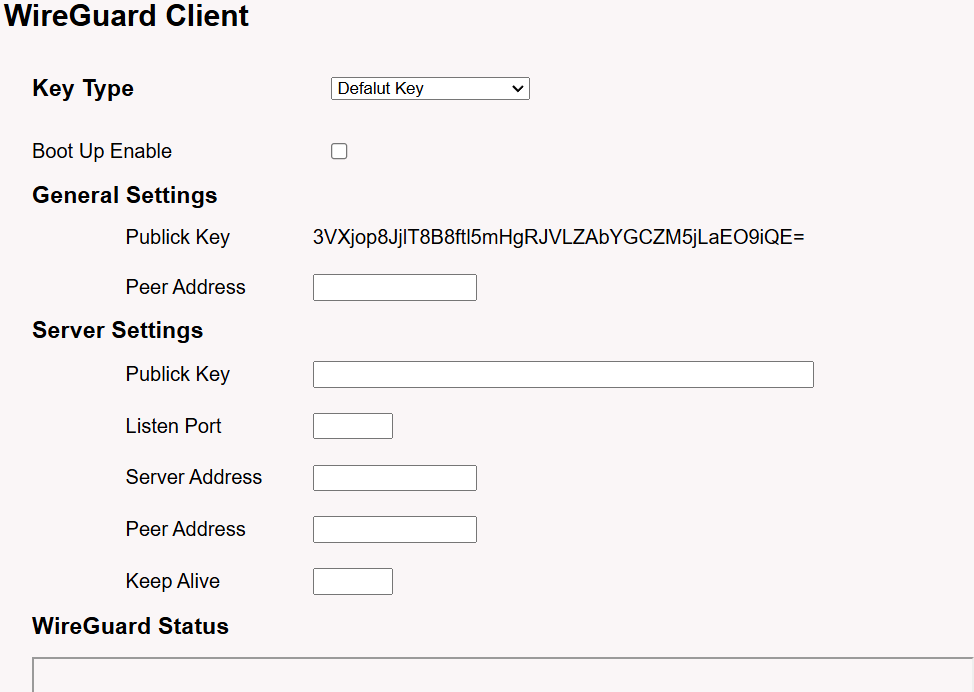
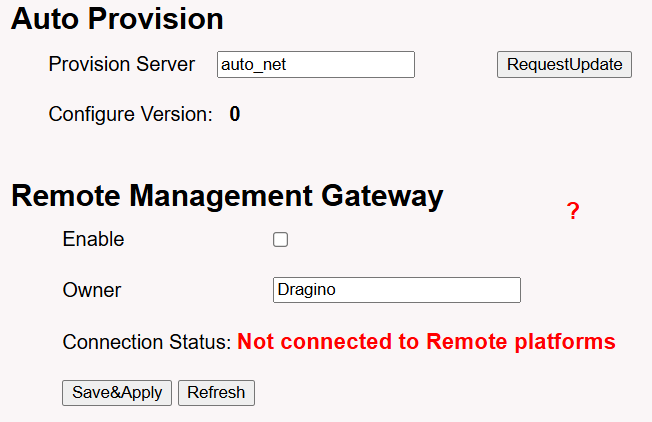
A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer program

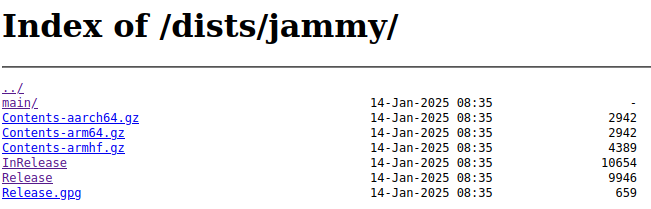
AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

## Appendix E Gateway Index

A close-up of a calendar

AI-generated content may be incorrect.A close-up of a calendar

AI-generated content may be incorrect.A close-up of a black text

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A close-up of a calendar

AI-generated content may be incorrect.A close-up of a computer screen

AI-generated content may be incorrect.