TAMAYOUZ CENTER
CENTRE D'EXCELLENCE
IT FSA UIZ

SMART DEVICE TRAFFIC ANALYSIS

DETECTING UNENCRYPTED MQTT COMMUNICATION & DATA LEAKAGE IN IOT NETWORKS

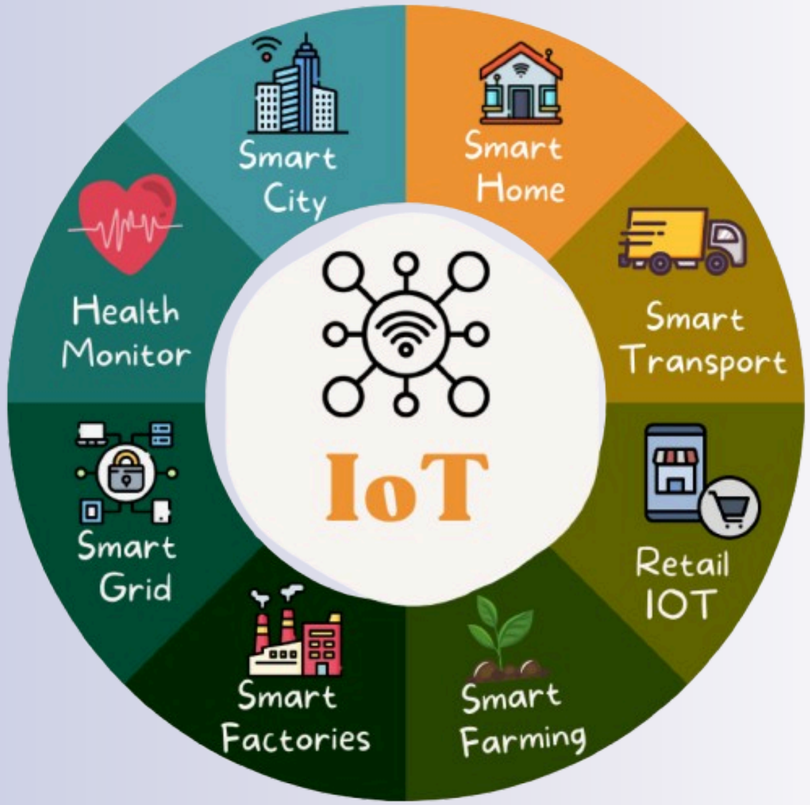
Prepared by:
Khaoula EL HARRAZ
Maryem EL-BOUCHTI
Khawla EL HASSNAOUI
Oussama GOUSSA

Supervised by:
Prof. BOUGHROUS Moncef

INTRODUCTION

IOT CONTEXT

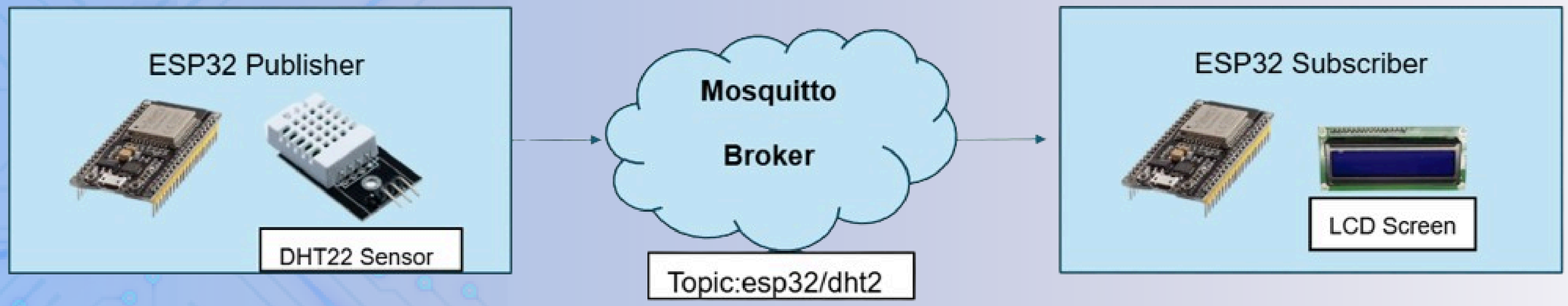
IoT devices are everywhere today-smart homes, industrial sensors, health devices, and more.
Most of them use lightweight communication protocols, especially **MQTT**.
But **MQTT** is not secure by default. When used without encryption, all the data is transmitted in plaintext. This makes IoT systems easy targets for passive sniffing or data interception.



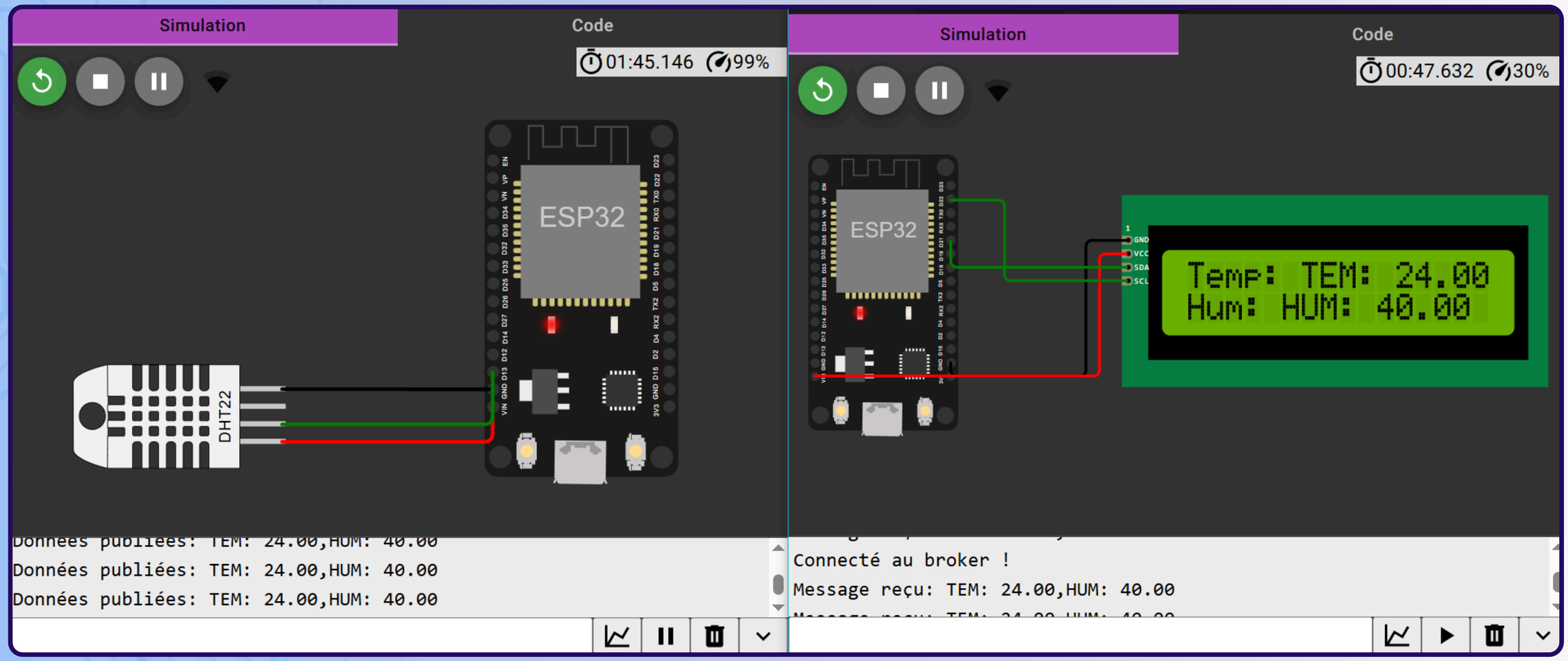
INTRODUCTION

PROBLEM STUDIED

MQTT communication between two ESP32s (**DHT22 → LCD**) tested using Wokwi, Mosquitto, and Wireshark in both unencrypted and **TLS-encrypted modes**



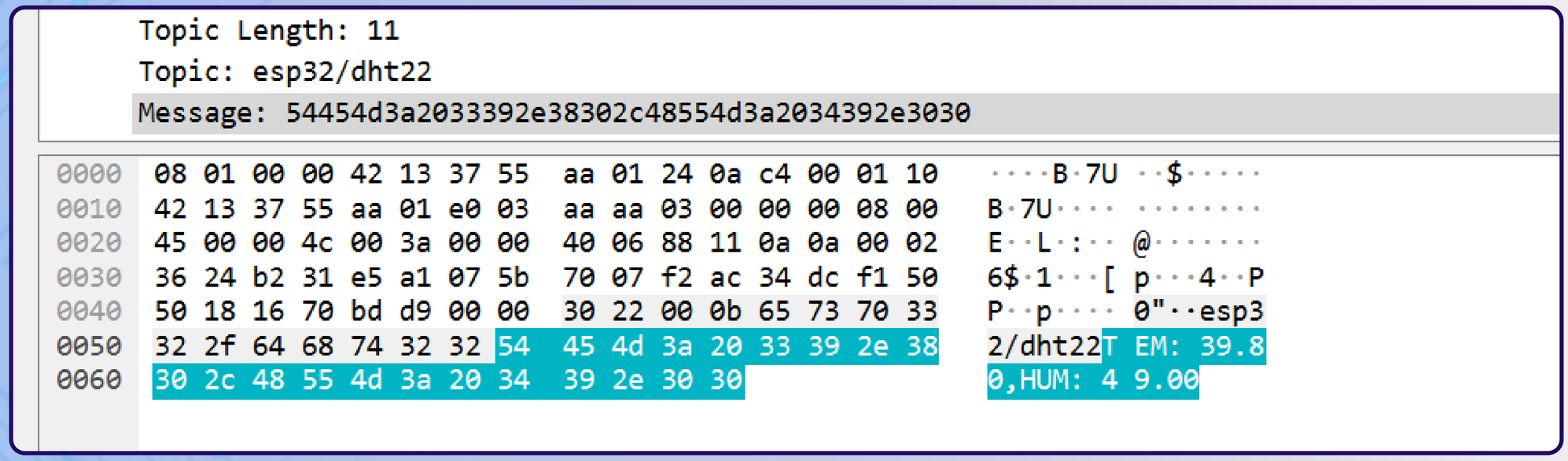
METHODOLOGY



DEMONSTRATION

UNENCRYPTED MQTT

Wireshark capture of unencrypted **MQTT** traffic. Both the **JSON** payload (temperature and humidity) and the topic are fully visible, showing that all data is transmitted in plaintext and easily readable by anyone on the network.



SECURITY RISKS OF UNENCRYPTED MQTT

01

Confidentiality

Data is sent in plaintext, so anyone on the network can read sensor values and topics.

02

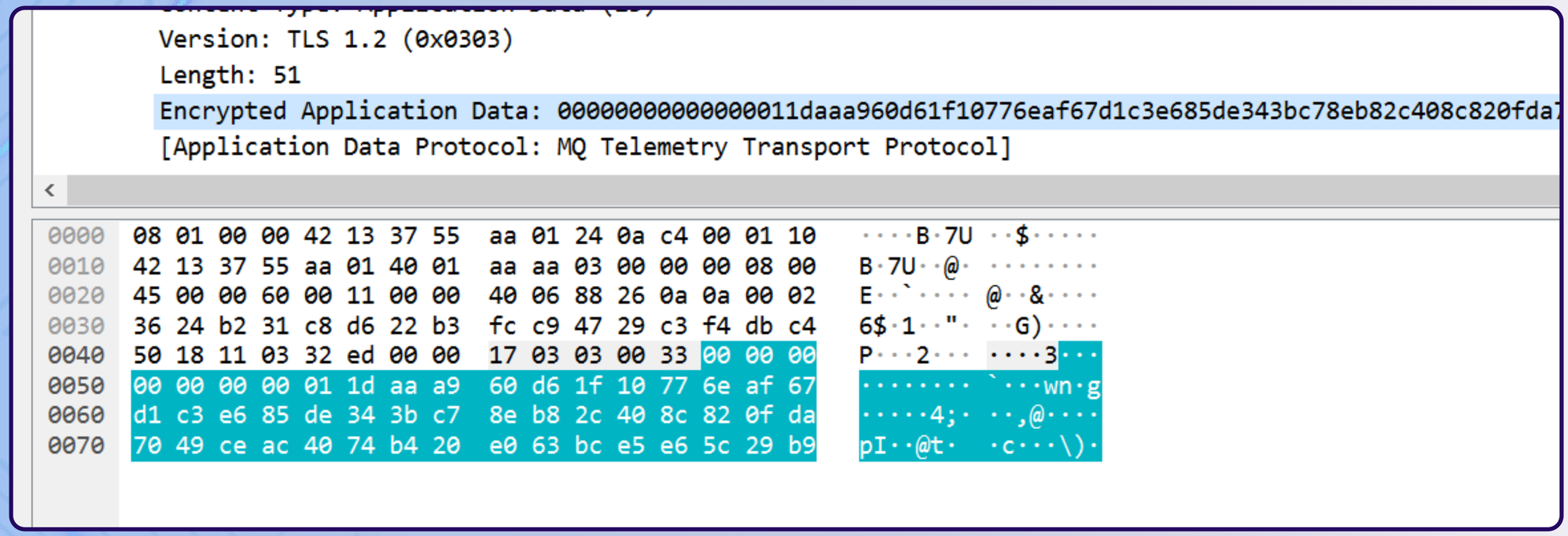
Integrity (Message Injection)

Since topics are visible and there's no authentication, attackers can publish fake messages to the same topic.

DEMONSTRATION

SECURING MQTT WITH TLS (MQTTS)

Wireshark capture of **MQTT** over **TLS**. The payload and topics are fully encrypted, preventing any readable data from being intercepted on the network.



MQTT VS. MQTTS - BEFORE AND AFTER

Aspect	MQTT (Unencrypted)	MQTTS (TLS)
Payload	Readable in plaintext	Encrypted
Topic	Visible	Hidden
Sniffing	Easy to intercept	Not readable
Authentication	No authentication	TLS authentication
Confidentiality	Compromised	Restored

CONCLUSION

Communication is the most important aspect of any **IoT** system, but using **MQTT** alone puts the data at risk. Without encryption, all messages and topics can be intercepted or modified by attackers.
This is why securing **MQTT** with **TLS** is essential, as it encrypts the communication and protects both payloads and topics, greatly improving the security of **IoT** systems.

THANK YOU!