Demo: Teaching IoT with a Capture-the-Flag Challenge

Antonio Boiano, Fabio Palmese, Alessandro E. C. Redondi, Matteo Cesana
DEIB - Politecnico di Milano, Italy
{antonio.boiano,fabio.palmese,alessandroenrico.redondi,matteo.cesana}@polimi.it

Abstract

We demonstrate a Capture-the-Flag (CTF) challenge introduced within the IoT course at Politecnico di Milano to enhance student engagement and practical understanding of IoT communication technologies. Originally structured as a theory-intensive course with limited lab work, the course program has evolved over the past decade into a hands-on, lab-focused curriculum. The traditional exam-based assessment has been replaced with continuous evaluation through practical challenges and assignments. Building on this evolution, the CTF challenge we demonstrate provides an interactive, problem-solving environment that reinforces protocol knowledge, encourages active learning, and better reflects the applied nature of IoT systems.

CCS Concepts

• **Human-centered computing** → **Ubiquitous and mobile computing**; • **Social and professional topics** → *Computing education.*

Keywords

Internet of Things, Capture-the-Flag, BLE, MQTT, CoAP

1 Description of the demo

The CTF challenge presented here is one of the several practical labs in the IoT course at Politecnico di Milano, part of the M.Sc. programs in Telecommunication and Computer Science Engineering. It is designed to be completed by students during a standard 1.5-hour lecture. Given the large class size (around 400 students split into two groups), managing a hands-on hardware-based CTF for each student or group would be impractical. Therefore, the challenge is delivered online using the CTFd.io platform [1], which students can easily access via laptops or smartphones. This format also enables quick demos without specialized hardware.

The CTF consists of several challenges centered around IoT communication technologies. The version showcased in this demo includes six distinct challenges, covering both low-level technologies such as Bluetooth Low Energy (BLE) and application-layer protocols like CoAP and MQTT. Each challenge is designed to assess students' understanding of theoretical concepts covered in the course (e.g., what a BLE advertisement is) as well as their ability to use practical IoT tool covered in the lab lectures (e.g., how to connect to and subscribe to an MQTT broker).

The CTF is structured as a game consisting of six sequential quests. To enhance engagement and enjoyment, each quest is presented in the form of a rhyming poem. The CTF is designed to evolve over time, with new quests added and existing ones modified each year in order to address emerging IoT topics and continuously challenge students' skills.

In this demo, the following quests are showcased:

(1) *Let the journey begins:* Students start by scanning for Bluetooth Low Energy (BLE) devices using their laptops or smartphones. Their goal is to locate a hidden BLE device somewhere in the classroom. This device is identified by broadcasting a unique 16-bit GATT UUID within its advertising data. Students must filter the BLE advertisements to find this exact UUID and confirm the device's presence.
(2) *Book of knowledge:* After discovering the UUID, students need to understand what it means. They consult the official BLE standards or documentation to decode the description associated with that specific 16-bit GATT UUID. This step connects the raw identifier to meaningful information.
(3) *Cryptographic dance:* Students take the description retrieved from the BLE standard and apply a designated hash function (like SHA-256). This process encrypts the text, producing a secure output that will be used in the next step.
(4) *The Mosquitto realm:* The resulting encrypted hash is used as the name of an MQTT topic on a public Mosquitto broker [2]. Students subscribe to this topic and receive messages containing hints that direct them to subscribe to further MQTT topics in a particular order that simulates BLE frequency hopping.
(5) *Follow the White Rabbit:* The sequence of MQTT topics leads students to various CoAP URIs. By visiting these URIs, students gather additional clues and navigate through the challenge's final stages.
(6) *The End:* the CoAP resource value provides the key for decrypting the manufacturer data advertised by a second BLE device, providing the final answer for the CTF.

2 Educational Impact and Analysis

During the most recent CTF, we recorded 1,488 submissions, including 255 successful solves (17.1%) and 1,233 failed attempts (82.9%). This distribution aligns with our educational goal of promoting persistence and problem-solving over simple recall. BLE-focused challenges had the highest solve rates (90.5% and 87.3%), while the MQTT (54.0%) and CoAP (44.4%) challenges showed lower completion rates, reflecting their increased complexity. The CTF provided educational value by promoting learning through hands-on experimentation and offering data-driven insights for curriculum improvement. Students averaged 4.8 attempts per challenge—7.2 for the MQTT task—demonstrating active problem-solving and the development of essential debugging skills. Unlike traditional assessments, the format encouraged learning from failure. Additionally, the varying success rates across protocol-specific challenges helped educators identify concepts that may require greater emphasis in the future.

References

[1] CTFd, "CTFd: Capture The Flag Framework," https://ctfd.io/
[2] "Mosquitto broker", https://test.mosquitto.org/