Student : Rémi Heredero
Professor : Prof. Medard Rieder
Expert : Rico Steiner (HOOC AG, Visp)

Hes·so VALAIS WALLIS
School of Engineering

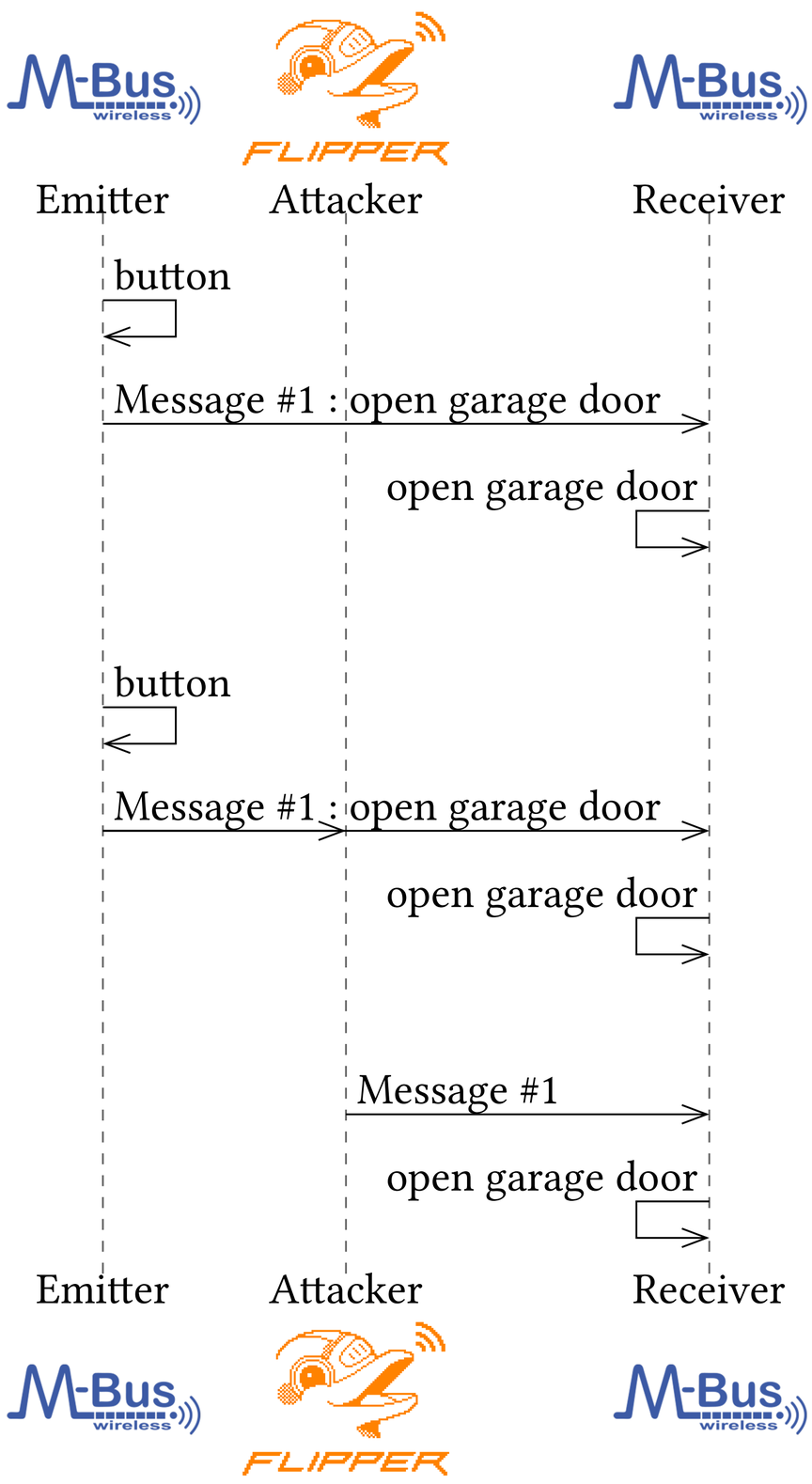
OT Security

Context

This thesis, exists in the context of the rewriting of the embedded systems security course at HEI-VS. The goal is to come up with several attack scenarios which can be used as the basis for a laboratory experience for students. These scenarios could also serve in industrial training partnerships with HEI-VS.

Replay attack scenario

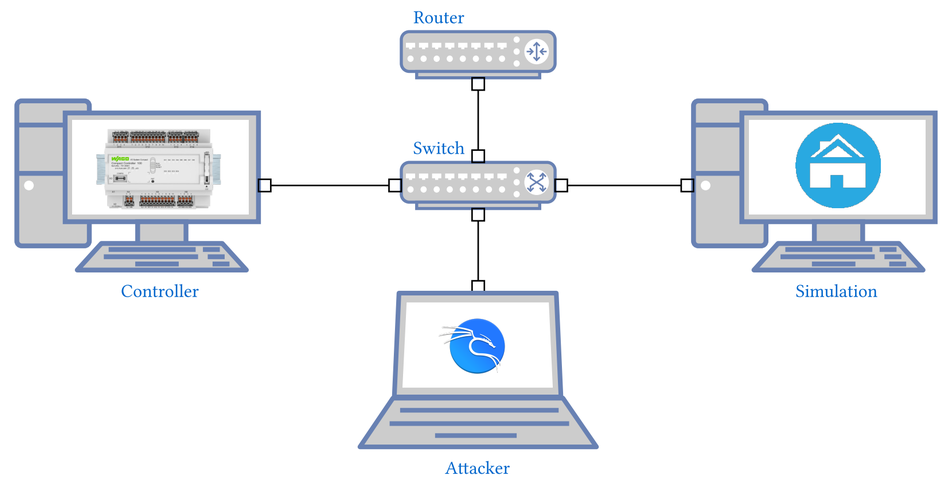
The replay scenario involves intercepting and resending a message on a wireless connection to trigger the same effect as the original message, like for example a garage door opening remote.



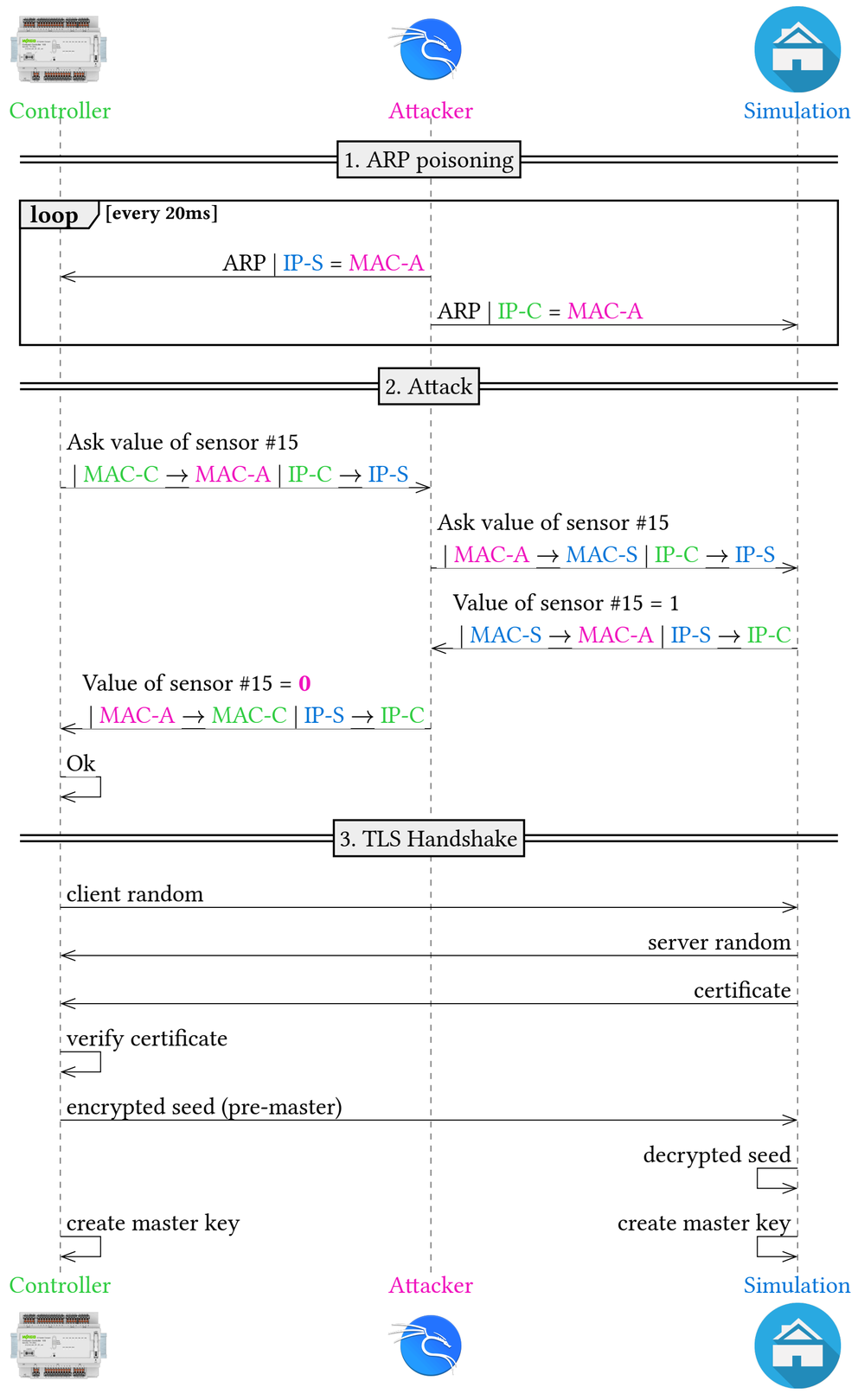
To protect against such an attack, the system should integrate a security mechanism as part of the message, like for example a rolling code or an encrypted counter signed with a private key.

Man in the middle

The Man in the Middle scenario involves intercepting, modifying and sending packets to take over the control of a Modbus/TCP installation.



The first step of the attack is to intercept the communication between the controller and the installation. To achieve this, the attacker has to conduct an ARP poisoning attack (1). Once the attacker has intercepted all packets, it is possible to modify those (2). To protect against such an attack, the system must use Modbus over TLS (3).



Stack

Kali — OS
Wireshark — Packets sniffer
Ettercap — MitM tool
Iptables — Firewall
Python — Programming language
Scapy — Packet manipulation
Golang — Programming language
Flipper Zero — Pen testing toy
Wireless M-Bus — Wireless protocol

HES-SO Valais-Wallis • rue de l'Industrie 23 • 1950 Sion
+41 58 606 85 11 • info@hevs.ch • www.hevs.ch

swissuniversities

EQUAL SALARY

Valais excellence CERTIFIED