Shadow RTU

Innovative system developed by :

UNIVERSIDADE DE COIMBRA
FACULDADE DE CIÊNCIAS E TECNOLOGIA

Type: *ICS Security System*

Packaging: *Ready to use system embedded in Raspberry PI hardware*

Main Functionalities

- Modbus TCP / IEC104 packet decoding
- Continuous monitoring
- Message integrity checking (cmd tampering)
- Modbus traffic modification detection
- Abnormal behavior detection from the monitored device
- RTU reprogramming and MITM attacks detection
- Zero-day attacks Detection
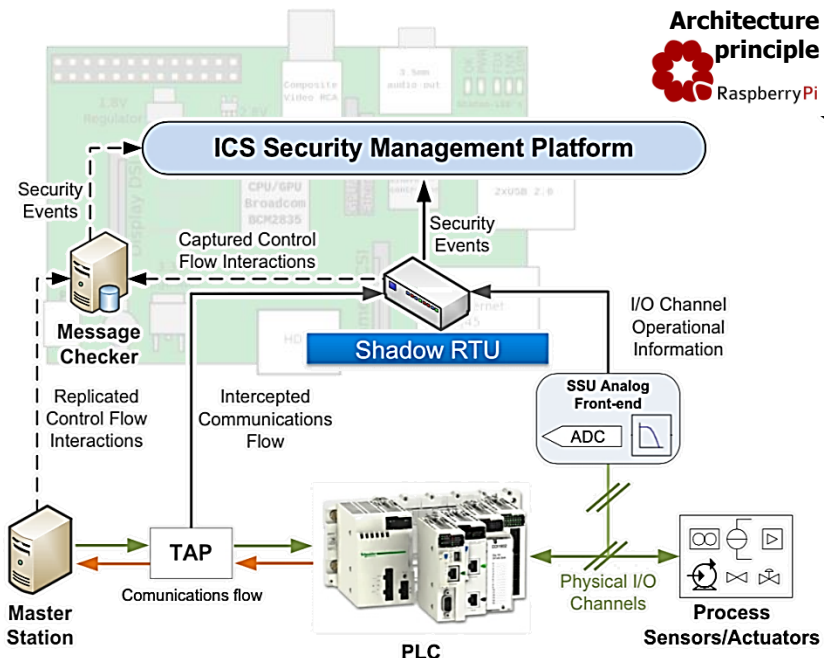- HMI exploitations detection (HMI modification)

Modus Operandi

- Shadow mode operation (the system have no IP address and still remains undetectable)
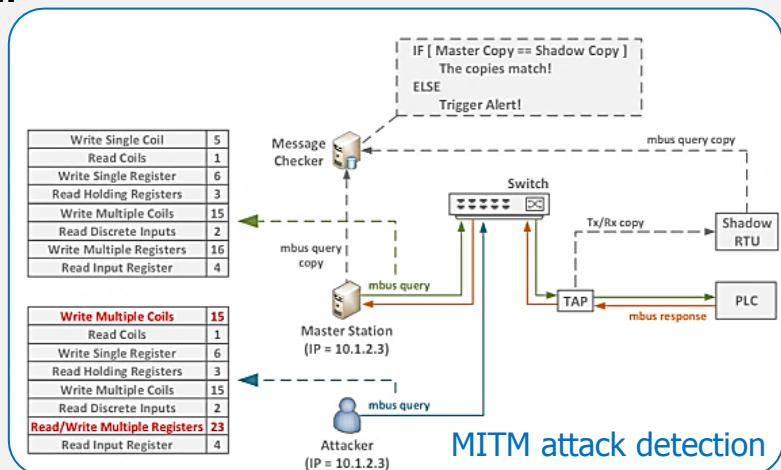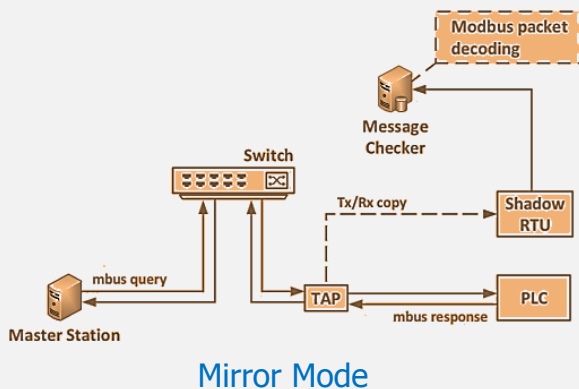- Mirror mode
- Very unexpansive

Architecture principle

Raspberry Pi

Examples of monitoring and attack prevention

Mirror Mode

MITM attack detection