

# Specialized Attacks: ICS and OT

---

## Exploiting the Modbus Protocol



**Matt Lloyd Davies**

Capability Development Lead

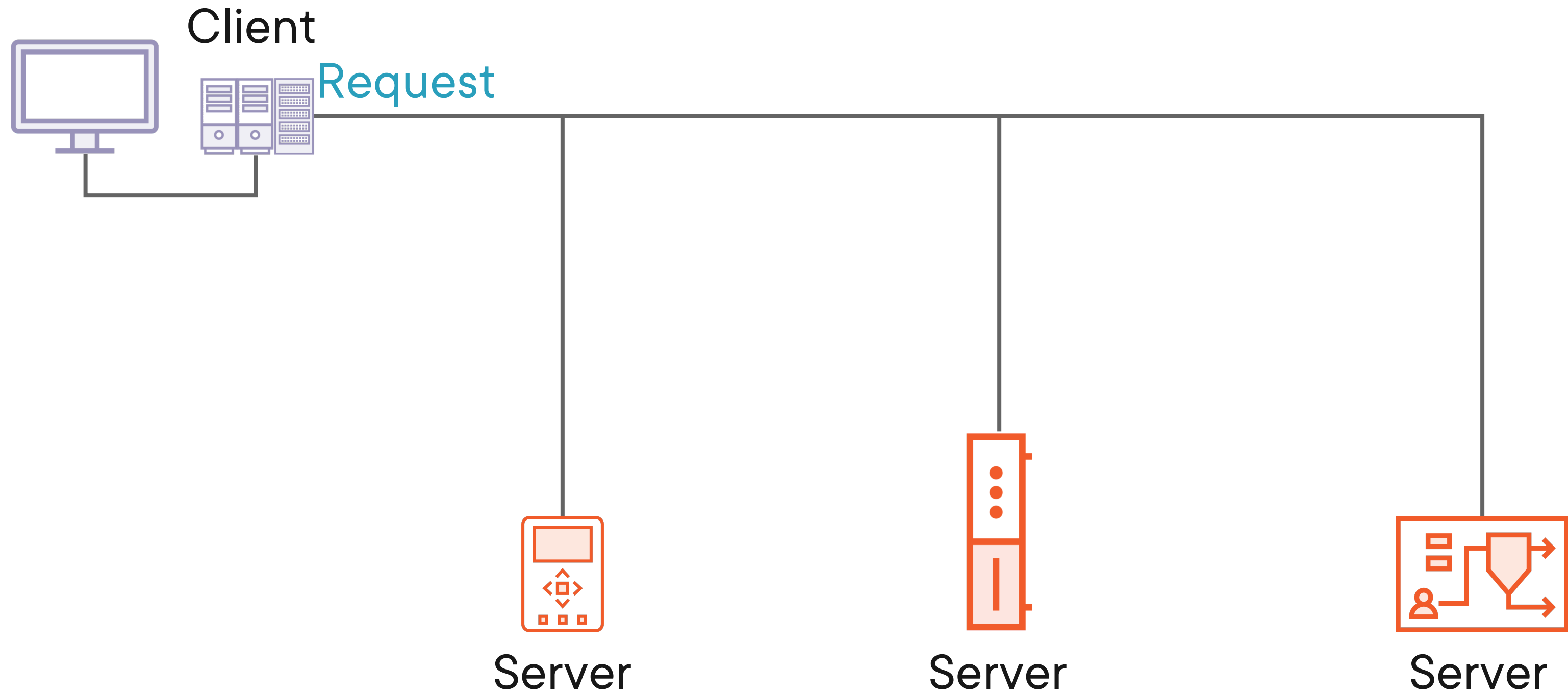


# The Modbus Protocol

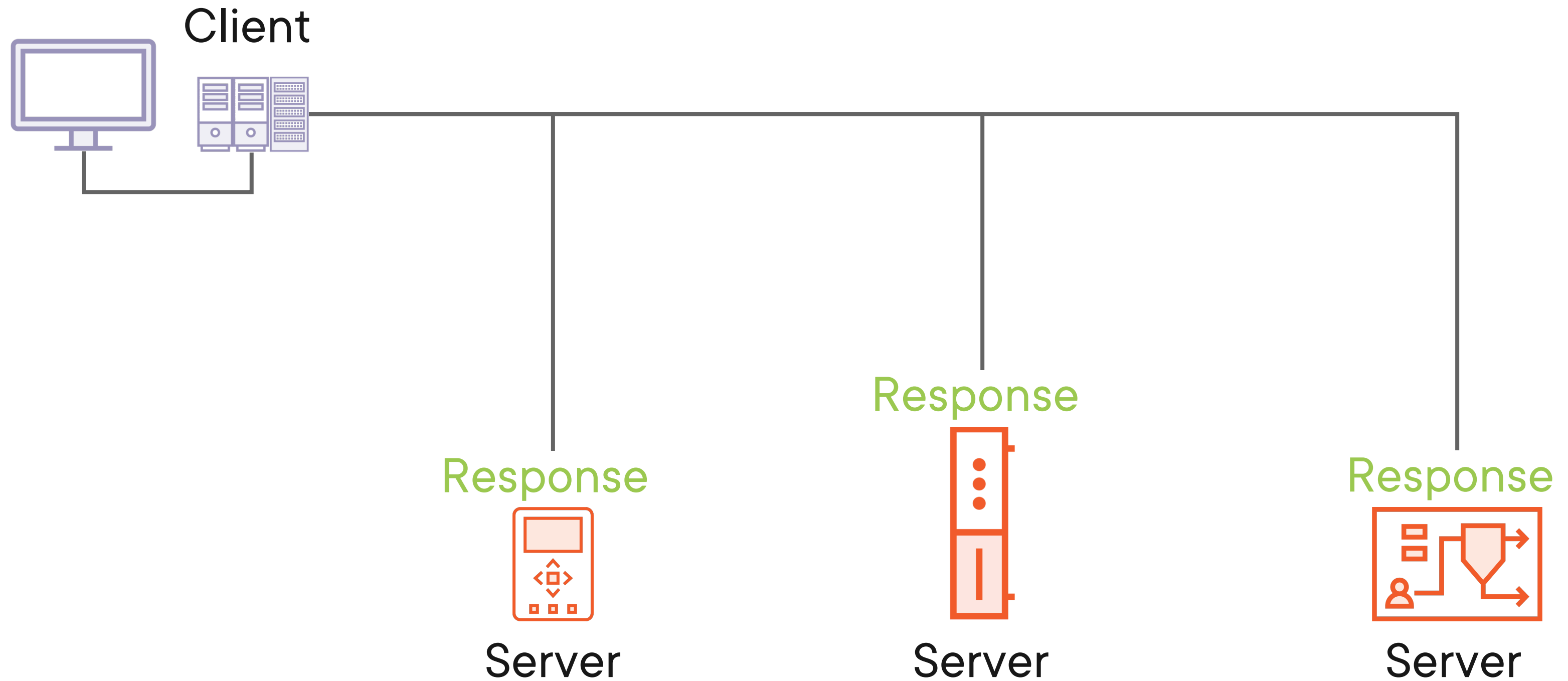
---



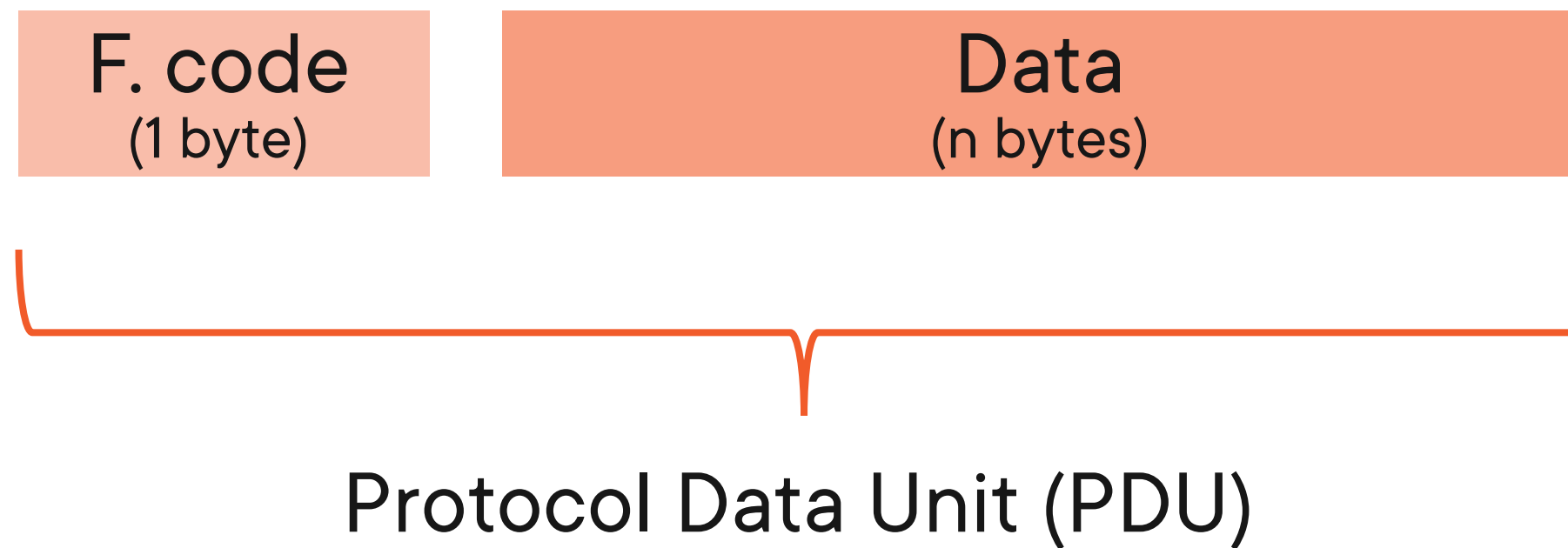
# Modbus Communication



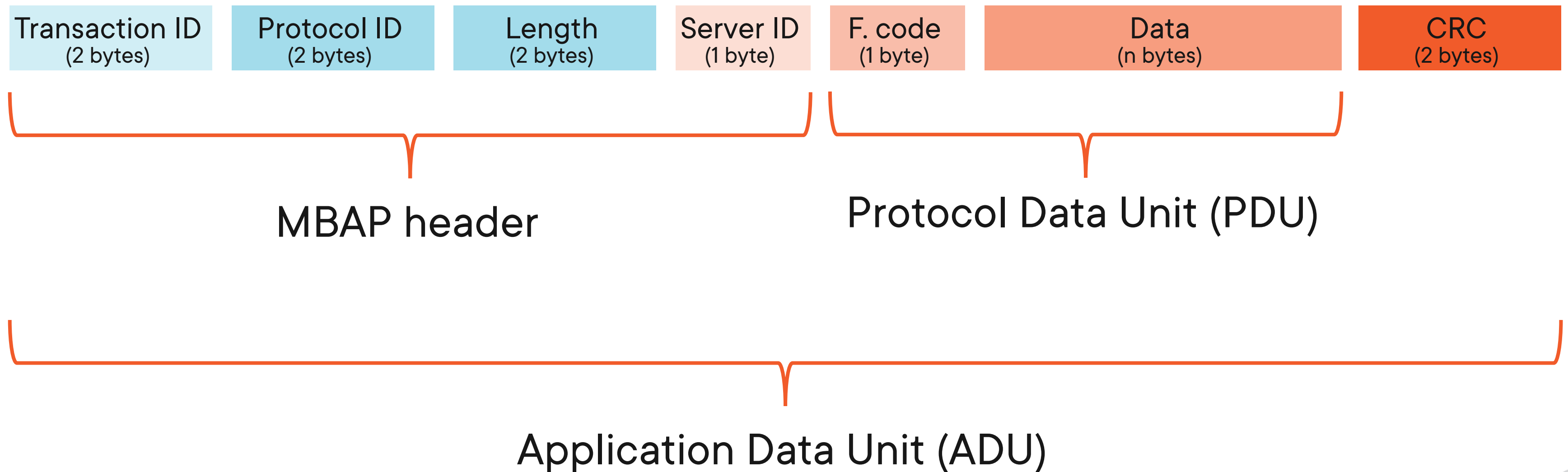
# Modbus Communication



# Modbus Communication



# Modbus Communication



# Modbus Communication

Function Code	Register Type
1	Read Coil
2	Read Discrete Input
3	Read Holding Registers
4	Read Input Registers
5	Write Single Coil
6	Write Single Holding Register
15	Write Multiple Coils
16	Write Multiple Holding Registers

Transaction ID  
(2 bytes)

Protocol ID  
(2 bytes)

Length  
(2 bytes)

Server ID  
(1 byte)

F. code  
(1 byte)

Data  
(n bytes)

CRC  
(2 bytes)



# Modbus Communication

## Typical Request Packet

Transaction ID (2 bytes)	Protocol ID (2 bytes)	Length (2 bytes)	Server ID (1 byte)	F. code (1 byte)	Data (n bytes)	CRC (2 bytes)
00AD	0000	0006	33	05	0043 FF00	8C3A

Data address — FF00 = On  
0000 = Off



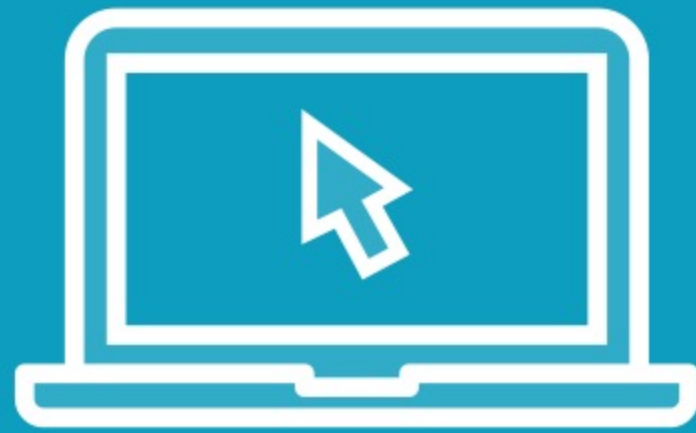
# Demo



## Capturing and analyzing Modbus traffic



# Demo



## Packet crafting with Scapy



# Planning the Attack

---



# Planning the Attack

**Injection timing**

**Sample traffic to find the right ACK**

**Create the malicious packet**

**Inject the packet**

**Monitor the effect with Wireshark**



# Demo



## Launching the attack

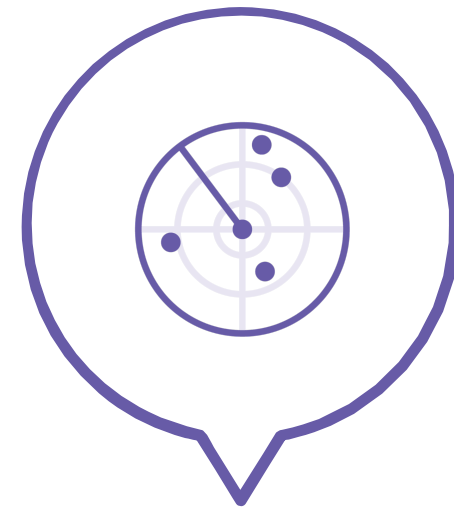


# ICS Cyber Security

---







## Identify

Understand risk  
to systems,  
assets, data and  
capabilities

## Protect

Act to ensure  
delivery of  
critical services

## Detect

Identify the  
occurrence of a  
cyber incident

## Respond

Act in response  
to a detected  
cyber incident

## Recover

Maintain plans for  
resilience and to  
restore capabilities  
and services

# ICS Cyber Security




# Drawing it All Together

---



# Specialized Attacks: OT and ICS

 Reconnaissance

 Modbus

 Packet crafting

 Plan and attack

 Cyber security

