Introduction to IoT & OT Security Day 1

Understanding IoT & OT Ecosystems

- What is the internet of things:
- Consumer
- Commercial
- Industrial
- Infrastructure

IoT Breakdown

- The Internet

Practical – Finding Devices with Shodan

- The Thing

Edge Devices

- Microcontrollers
- CPU
- Memory
- Input/Output
- Single Board Computers

Practical – Interfacing with GPIO

- Breakdown Sensors
- Breakdown Digital Conversion
- Breakdown Digital Sensors
- Breakdown Actuators
- MQTT

MQTT Practical – Attacking MQTT

Legal and ethical considerations In IoT

- CMA
- Informed Consent
- Responsible Disclosure
- Data Privacy
- Legal Compliance
- Minimizing Harm
- Transparency
- Vulnerability Handling
- Consider Impact on Critical Infrastructure:
- Continuous Learning and Collaboration
- Responsible Disclosure.

Hacking Fundamentals of IoT & OT Technologies Day 2

Morning Session:

The Cyber Kill Chain

Common Vulnerabilities in IoT and OT Technologies

- Default Credentials
- Lack of encryption
- Insecure firmware
- Legacy Systems
- Insecure protocols

In depth discussion of CAN Protocol

- Voltage Signalling
- Transmission Rate
- CAN Frame Structure
- Error Monitoring
- Common Issues

Afternoon Session:

Car Hacking Practical (Virtualised)

- Can Injection
- CAN Reversing

Operational Technologies Day 3

Morning Session:

Assessing OT Environments & Special Considerations
The Devices Found Within ICS Environments
SCADA & MODBUS
Passive Analysis Of ICS Environments

Afternoon Session:

Assessment Of TCS Virtualised Factory

Practical – Exploitation of virtualised factory.

Hardware Hacking Day 4

Morning Session:

Hardware Overview

Definitions of:

- Uses WRT54GL
- Meet your router
- Device
- Software
- Hardware
- Firmware
- Processors
- Volatile memory
- Non-volatile memory
- Analog components
- GPIO/External Interfaces

Afternoon Session:

UART

- What is UART?
- Identifying UART
- Determining BAUD Rate

Practical - Determining Pins

- Identify UART

Practical - Obtaining a shell

JTAG

- What is JTAG?
- Identifying JTAG
- Plug Into WRT54G
- Practical Interface with JTAG using bus pirate.
- Debugging Via JTAG

Practical - Dumping the firmware via JTAG

Introduction to Reverse Engineering Firmware

Q&A and Close