INTERNET OF THINGS (IOT)

Module 1: Fundamentals of IoT Security

AN INTRODUCTION TO IOT SYSTEMS AND TECHNOLOGIES

- The Course Overview
- Case Study: Connected and Self-driving Vehicles
- Case Study: Microgrids
- Case Study: Smart City Drone Systems
- IoT Hardware and Software
- IoT Communication and Messaging Protocols
- IoT Interfaces and Services

AN INTRODUCTION TO IOT SECURITY

- Threats, Vulnerabilities and Risks
- Case Study: The Mirai Botnet Opens up Pandora's Box
- Today's Attack Vectors
- Current IoT Security Regulations
- Current IoT Privacy Regulations
- An Introduction to IoT Security Architectures

CONDUCTING AN IOT THREAT MODEL

- What is Threat Modelling
- Identifying Assets
- Creating a System Architecture
- Documenting Threats
- Rating Threats

DEEP DIVE ON PRIVACY

- IoT Privacy Concerns
- Privacy by Design (PbD)
- Conducting a Privacy Impact Assessment (PIA)
- Case Study: The Connected Barbie

Module 2: Security Engineering for the IoT

SECURELY DESIGNING IOT THINGS AND SYSTEMS

- The Course Overview
- Secure IoT System Design
- Security System Integration for the IoT
- Integrating Safety into the Design Process
- Processes and Agreements
- Technology Selection

CRYPTOGRAPHIC APPROACHES FOR THE IOT

- Fundamentals of Cryptography
- Cryptographic Modules
- Cryptographic Key Management
- Implementing Cryptography Within the IoT
- Case Study: New Approaches – Blockchain for the IoT

IDENTITY AND ACCESS MANAGEMENT FOR THE IOT

- The Device Identity Lifecycle
- In Depth: The Bootstrap Process
- Case Study: Connected Vehicles
- IAM Infrastructure
- Authorization and Access Control
- New Approaches: Applying Biometrics

SECURE CONNECTIONS TO THE CLOUD

- Introduction to Cloud Services for the IoT
- Cloud Security Architecture – Microsoft Azure
- Cloud Security Architecture – Amazon Web Services
- Cloud Security Architecture – IBM Watson IoT Platform