IoT SECURITY COURSE CONTENT

Main Objectives for IoT Security:

- Be able to secure a connected IoT product from scratch
- Be able to discuss the main threats and attacks on IoT products and services
- Know how to research and assess IoT threats and risks as they arise
- Be able to implement a security reporting scheme in their organisation
- Be able to work effectively with security researchers on reported IoT security
- issues and concerns
- Have the knowledge to be able to develop a security patching strategy and
- product update life-cycle
- Have a good working understanding of the best practices laid down by the IoT

Security Foundation:

a. **Cyber security and the Internet of things**:
    - Provides the Security for internet of Things to generate 400 Zettabytes of data by 2020.
    - New Security and Privacy Challenges
    - How Organizations Address IoT
    - Security for the devices
b. **IoT Security:**
    - Security Spectrum
    - Challenges for IoT Security
c. **IoT –Identity Protection:**
        - Iot Liability
        - Device Malfunction
        - Cyber Attacks
            - Built-in Security
            - Encryption
            - Risk Analysis
            - Authorization
d. **Device Security:**
    - Application hardening
    - OS/platform hardening
    - Physical Security

Gateway Security:

Communication Protocols and network Security:

- Data link layer – Wireless communication technology security provisions
  - WiFi,Bluetooth,Zigbee and 802.15.4 Protocols
- Application layer Security
  - MQTT and HTTP Protocols
- Network hardening

IoT Cloud Platforms Security

- Creating an Active Directory
- Mapping a Custom Domain
- Creating Users
- Integrating with Azure Active Directory
- Integrating On-Premise Active Directory
- Reports
- Example platforms: AWS ,Microsoft Azure, Google Cloud Platform.

Testing challenges – mass interoperability:

a) **Many Communication protocols:**

- Mobile Z-Wave
- Wifi 6LowPAN
- Bluetooth Thread
- Zigbee NFC

b) **Simulate wide range of Networking conditions:**

- RF testing
- cell handovers
- low signal strength
- protocol analysis
- moving between 2G, 3G & LTE or wifi

c) Test scenarios to consider:

• Moving between networks

• Losing power on upgrade

• Low bandwidth

• Simulate signal loss (going through a tunnel)

• Patching the device

d) Security testing:

- Insecure web interface
- Insufficient authentication/authorization
- Insecure network services
- Lack of transport encryption
- Privacy concerns
- Insecure cloud interface
- Insecure mobile interface
- Insufficient security configurability
- Insecure software/firmware
- Poor physical security

Projects:

Connected Consumer Products

This working group is producing security best practice guidelines for various classes of consumer devices which cover important topics such as:

- Classification of Data
- Physical Security
- Device Secure Boot
- Secure Operating System
- Application Security
- Credential Management
- Encryption
- Network Connections
- Software Updates
- Logging