

IOT DEVICE SECURITY

“Secure the Edge — Build Resilience Against Evolving Threats in the Internet of Things Ecosystem.”

Schedule

Venue	Fees
In-House	ASK FOR THE QUOTATION

► Available delivery methods: In-House Training

Introduction

As IoT devices proliferate across industries, security has become a top priority. This course provides a deep dive into the threats, vulnerabilities, and countermeasures related to IoT device security. Participants will explore hardware, firmware, network, and cloud-based vulnerabilities, and gain hands-on experience with security assessment, threat modeling, and secure development practices to protect IoT infrastructures from end to end.

Objectives

By the end of this training, participants will be able to:

- Identify common vulnerabilities in IoT device ecosystems
- Understand the security architecture of IoT hardware and firmware
- Apply best practices in securing communication, storage, and access
- Implement secure device lifecycle management (from provisioning to decommissioning)
- Conduct threat modeling and perform basic penetration testing on IoT systems

Why Attend

IoT security failures can result in major breaches, service outages, and regulatory fines. This course equips professionals to proactively secure devices and networks, comply with standards, and mitigate risk in IoT deployments across industries.

Target Audience

- IoT Developers and Embedded Engineers
- Cybersecurity Professionals and Penetration Testers
- Network Engineers and System Integrators
- IT Risk and Compliance Officers
- Product Managers and Architects in IoT Solutions

Individual Benefits

- Gain specialized IoT security expertise for career advancement
- Learn practical tools and frameworks for securing devices and platforms
- Develop the ability to assess and test real-world vulnerabilities
- Earn recognition with a professional security training certificate

Organizational Benefits

- Mitigate risks of data breaches, downtime, and non-compliance
- Strengthen defenses across distributed IoT environments
- Enhance customer trust and reputation through security-by-design
- Reduce costs associated with incident response and remediation

Instructional Methodology

- Hands-on labs and real-world simulations
- Vulnerability analysis and live demos
- Industry case studies and security incident reviews
- Group threat modeling and risk assessment exercises

Course Outline

DETAILED 5-DAY COURSE OUTLINE (CUSTOMIZABLE)

- Training Hours:** 7:30 AM – 3:30 PM
- Daily Format:** 3–4 Learning Modules | Coffee Breaks: 09:30 & 11:15 | Lunch Buffet: 01:00 – 02:00
- Day 1: Introduction to IoT Security Landscape**
- Module 1:** IoT Ecosystem Overview & Attack Surfaces (07:30 – 09:30)
 - Module 2:** Common Threats & Vulnerabilities in IoT Devices (09:45 – 11:15)
 - Module 3:** IoT Security Standards (NIST, ETSI, ISO/IEC) (11:30 – 01:00)
 - Module 4:** Case Study: Famous IoT Breaches & Lessons Learned (02:00 – 03:30)
- Day 2: Device Architecture & Secure Firmware**
- Module 1:** Hardware Components and Trusted Execution Environments (07:30 – 09:30)
 - Module 2:** Secure Boot, Firmware Signing & Updates (09:45 – 11:15)
 - Module 3:** Device Identity & Cryptographic Storage (11:30 – 01:00)
 - Module 4:** Hands-On Lab: Firmware Analysis Basics (02:00 – 03:30)
- Day 3: Network & Communication Security**
- Module 1:** Securing IoT Communication Protocols (MQTT, CoAP, BLE) (07:30 – 09:30)
 - Module 2:** TLS/SSL, VPN, and Encryption Best Practices (09:45 – 11:15)
 - Module 3:** Authentication & Access Control for IoT Devices (11:30 – 01:00)
 - Module 4:** Lab: Simulating Network Attacks on IoT Devices (02:00 – 03:30)
- Day 4: Threat Modeling & Testing IoT Devices**
- Module 1:** STRIDE & PASTA for IoT Threat Modeling (07:30 – 09:30)
 - Module 2:** Static and Dynamic Analysis Tools for IoT (09:45 – 11:15)
 - Module 3:** IoT Penetration Testing Methodologies (11:30 – 01:00)
 - Module 4:** Hands-On Lab: Basic IoT Exploitation (02:00 – 03:30)
- Day 5: Device Lifecycle & Security Governance**
- Module 1:** Secure Provisioning, Maintenance & Decommissioning (07:30 – 09:30)
 - Module 2:** Incident Response & Recovery for IoT Breaches (09:45 – 11:15)
 - Module 3:** Compliance, Privacy & Risk Management (11:30 – 01:00)
 - Module 4:** Final Practical Challenge & Certification Wrap-Up (02:00 – 03:30)

Certification

Participants will receive a **Certificate in IoT Device Security** upon successful completion of the training and final challenge assessment. This credential validates the ability to secure IoT devices and environments following global cybersecurity best practices.

Why Choose MAWA Events

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation’s unique goals.

In-House / Customized Training Interested in running this course for your team? Please contact us:	TEL: +601116373203	EMAIL: info@mawaevents.net
--	---	---

© Material published by MAWA Events shown here is copyrighted. All rights reserved. Any unauthorized copying, distribution, use, dissemination, downloading, storing (in any medium), transmission, reproduction or reliance in whole or any part of this course outline is prohibited and will constitute an infringement of copyright.