FST
FACULTÉ DES SCIENCES ET TECHNIQUES
DE MOHAMMEDIA
UNIVERSITÉ HASSAN II DE CASABLANCA

ITU-MUST IPv6 and IoT
Centre of Expertise

MALAYSIA
UNIVERSITY
of SCIENCE and TECHNOLOGY

Workshop on “IoT Security”

FSTM, February 3-7, 2020

- **Preface :**

  The ability to connect, communicate with, and remotely manage an incalculable number of networked, automated devices (approximately 26 Billion by 2020) via the Internet is becoming pervasive, from the factory floor to the hospital operating room to the residential basement. The transition from closed networks to enterprise IT networks to the public Internet is accelerating at an alarming pace—and justly raising alarms about security. As we become increasingly reliant on intelligent, interconnected devices in every aspect of our lives, how do we protect potentially billions of them from intrusions and interference that could compromise personal privacy or threaten public safety?

  This training covers the basics and Intermediate levels of IoT landscape and takes you through IoT Security Challenges and vulnerabilities and teaches you the steps to hack and harden the IoT devices, applications and ecosystem.

- **Training Approach :**

  The training would involve both theory and practical led by the instructor. Easy to understand case study-based real life approach. In depth knowledge from experienced trainer.

- **Who Should Attend ?**

  This course is recommended for IoT Enthusiasts, IoT Designers, IoT Developers, IoT Implementers, IT Managers, IT Auditors and anyone who is ready to master the steps required to secure IOT Implementations.

- **Prerequisites :**

  1. Should be involved in the IT field ;
  2. Should be familiar with using Windows, Linux and VMWare ;
  3. Should understand programming concepts, but programming experience is not mandatory ;
  4. Background knowledge in reverse code engineering and vulnerability assessment will be helpful, but not required ;
  5. Enthusiasm is a must.

- **Registration :**

  - **Number of seats** : 20 ;
  - **Registration form :** https://docs.google.com/forms/d/e/1FAIpQLSf6W3XQlaNafioagUwAyEozRTHaUTQcUJRnvC6sCS6qYTUPEQ/viewform?usp=sf_link
  - **Fees** : Academics 3000 dh (300 euros), Industrials 4000 dh (400 euros) ;

- **Date :** February 3–7, 2020 ;
- **Venue :** IPv6 Moroccan Training Center, FST of Mohammedia.
- **Contact :** Pr Cherkaoui LEGHRIS (www.fstm.ac.ma)

This CIoTS course content will be certified by ITU/MUST IPv6 and IOT Centre of Expertise and the copyrights of the contents belongs to the ITU/MUST IPv6 and IOT Centre of Expertise.

Course Outline

- **Day 1. IoT Security Overview**

  - What is IoT?
  - IoT Architecture & Ecosystem
  - Hardware & Software Platforms
  - Communication Channels & Protocols
  - Cloud & IoT (Cloud & RESTful Web Services)
  - Data Streaming & IoT
  - IoT Myths
  - IoT Applications : Agriculture, Medical, Meteorology
  - Overview of IOT Security
  - IoT Threats
  - Challenges to Secure IoT Deployments
  - Types of IoT Attacks

- **Day 2. Baseline Policies for IoT Security**

  - IoT Security Controls Lifecyle
  - Authentication / Authorization
  - Logging & Audit Framework
  - Privacy by Design
  - Data Protection Policies

- **Day 3. IoT Vulnerabilities**

  - 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

- **Day 4. IoT Endpoint Security Guidelines**

  - IoT Endpoint Security Challenges
  - IoT Endpoint Security Model and Recommendations.
  - Secure the IoT Systems
  - Securing the IoT Network.
  - IPv4 Based Security Guidelines
  - IPv6 Based Security Guidelines
  - Data Link Layer Based Network Guidelines

- **Day 5 IoT Security Recommendations**

  - High Priority Security Recommendations
  - Medium Priority Recommendations
  - Low Priority Recommendations
  - 5G based IoT Endpoint Security Recommendations
  - Hacking IoT Devices (Hands On)
    - Basics of Communications (Bluetooth)
    - Hacking IoT Device (via Bluetooth Network)