
# Sécurité des systèmes embarqués et IoT

## LE PUBLIC

Cette formation cible les personnes intéressées par les aspects de sécurité liés au hardware ou à l'embarqué.

Les amateurs ou professionnels en électronique ainsi que les professionnels de la sécurité IT.

## LES OBJECTIFS

Cette formation mélange méthodes et outils pour vous donner les connaissances nécessaires afin d'effectuer des audits de sécurité hardware par vous-même. La dernière partie de cette formation, propose un exercice complet « Capture The Drone » pour mettre en pratique ce qui aura été appris dans un scénario d'attaque défense en présence de nos petits objets volants préférés.

## VOTRE FORMATION

**DURÉE** : 5 JOURS

35 heures

**PROCHAINE SESSION** :

8, 9, 10, 17 et 18 juin 2020

**LIEU** : En distanciel

**PRIX** : 1 495 €

net de taxes

## PRÉ-REQUIS

Administration Windows/ Linux

Maitrise de Linux en ligne de commande est un plus

## RESSOURCES

- Support de cours
- 80 % d'exercices pratiques
- PC avec OS 64bits, avec VMware Player / Workstation 15Go de DD; 8 Go RAM

## MODALITES

Formation 100 % à distance

De 4 à 16 participants

9h –17h30

Financement éligible au FNE Formation pour tout salarié d'entreprise en activité partielle

Matériel requis : cartes et composants électroniques. A défaut, prévoir un coût supplémentaire pour des logiiciels de simulation en ligne.

## VOTRE CONTACT :

**Andrea FALLOURD**
Conseillère en formation
06 74 51 44 97
afallourd@itescia.fr

**ITESCIA** - Campus de Pontoise
8 rue Pierre de Coubertin
95300 PONTOISE

www.itescia.fr

# VOTRE PROGRAMME

**Cette formation vous présente les différentes attaques possibles lors des tentatives de piratage du hardware et du software de votre produit et les contremesures à déployer pour se protéger. La méthodologie est basée sur des exercices pratiques avec des scénarii d'attaque/défense. L'objectif est de vous apprendre les techniques indispensables pour mesurer le niveau de sécurité de vos architectures embarquées. À la suite de ces attaques, vous apprendrez à déclencher la riposte appropriée et à en élever le niveau de sécurité.**

### Rappel sur les architectures embarquées

Système informatique ordinaire et système embarqué.

Les différents types d'architectures embarquées.

Les différentes contraintes liées à la solution embarquée.

### Le hacking et la sécurité

Formes d'attaques, modes opératoires, acteurs, enjeux.

Audits et tests d'intrusion.

### L'environnement de l'embarqué et IoT

Réseau : 4G, LTE, LoRA, WiFi, MQTT, ZigBee, Z-Wave,…

Firmware et OS embarqués : Win, Linux ou Raspbian.

Cryptographie: communication et stockage

Matériel : puce, Storage, JTAG, UART, capteurs, caméra,…

Architecture : ARM, MIPS, SuperH, PowerPC.

TP: Découverte des cartes Arduino et Raspberry

### Vulnérabilités des architectures embarquées

OWASP TOP 10, SANS TOP 25 et CWE et CVE

Recherche de vulnérabilités et mécanismes d'authentification.

Connectivité : réseau, capteur et périphérique.

Applications/programmes hébergé sur un système embarqué.

La méthodologie des tests d'intrusion.

Les outils : analyseurs, débog., désass. et décompil.

TP: Niveau de sécurité d'une architecture embarquée.

### Les bases du Hardware Hacking

Revue historique des attaques sur les objets connectés

Revue des vulnérabilités et des aspects offensifs et défensifs

Rappel des connaissances fondamentales en électronique

TP : Prise d'information sur la cible (fingerprint des composants)

### Comment les pirates accèdent au Hardware ?

Outils et méthodes pour auditer un produit

Plan d'audit et différences avec l'audit logiciel

TP : Extraire des données sensibles avec Hardsploit.

TP : Acquérir les signaux électroniques, outils et démonstration

### Comment accéder au logiciel ?

Architecture Microcontrôleur, FPGA)

Interfaces E/S (JTAG / SWD, I2C, SPI, UART, RF etc.)

Accès au logiciel via attaques à canal latéral

TP : Accès au Firmware par différentes interfaces

### Attaques système embarqué particulier, l'objet connecté (IoT)

### Comment sécuriser votre matériel

Cycle SDLC et Best practice

Limiter les accès JTAG et les vuln. au niveau de l'embarqué

Examen des protections contre les attaques à canal latéral

### SDR Hacking

Méthodologie d'audit SDR (capture / analyse / exploitation avec radio logiciel)

Présentation des outils (GNURadio, etc.)

TP : Ingénierie inverse d'un protocole sans fil à partir de zéro (communication sans fil d'un panneau à LED semblable à ceux que l'on peut trouver dans la rue)

### Exercice « Capture The Drone or the Car»

Scénario pratique Attaque / Défense d'un mini–drone ou d'une voiture connectée

…