HS2
Hervé Schauer Sécurité

MAJ 20/01/2021

# Formation « Sécurité des objets connectés »

**Réf : SECUOBJ**

## Objectifs

- Fournir suffisamment d'éléments techniques et de langage afin de permettre aux développeurs et aux intégrateurs de solutions communicantes de comprendre l'aspect multi vectoriel de la sécurité des systèmes embarqués avec notamment une approche de défense vis à vis d'une vision attaquante.
- Être en mesure d'évaluer une solution IoT en prenant en compte l'ensemble de la chaine de données, depuis sa production jusqu'à sa consommation. Sur l'ensemble de la formation, le profil type attaquant est un attaquant opportuniste.

## Durée & horaires

- 3 jours soit 21 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

## Nombre de participant

- Minimum 6 participants – Maximum 24 participants

## Public visé

- Le profil type ciblé est un industriel (développeur ou intégrateur)

## Pré-requis

- Avoir une bonne connaissance générale en environnement linux nécessaire, ainsi que des notions en système.

## Méthode pédagogique

- Cours magistral avec échanges interactifs
- Travaux pratiques ayant pour objectif de réaliser un audit global d'une solution IoT en mode matriochka. Plusieurs challenges sont imbriqués avec une construction en plusieurs niveaux. Chacun d'entre eux seront étudier tout au long du cours A chaque découverte d'une vulnérabilité, une fiche détail composée d'une description, d'un score (CVSSv3) et d'une recommandation sera réalisée. Les travaux pratiques seront basés sur la plateforme Microbit (https://microbit.org/) et sur les puces STM32 (STM32F103C8T6)

## Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Certificat attestant de la participation à la formation

## Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

## Certification

- Cette formation est certifiante. L'évaluation de la formation se fera sous la forme d'un Quizz.

## Programme

**Qu'est-ce que l'Iot ?**
- Au cœur de la révolution industrielle et sociétale
- L'environnement IoT
- Cadre légal
- Analyse de risque
- Référentiels (ANSSI / GSMA / GIE / norme ISO / Internationale / NIST / CIS)
- Méthodologie test d'intrusion
  - MITRE ATT&CK ICS
  - PTES
  - OSTMM
  - OWASP

**Caractéristiques spécifiques**
- Contraintes spécifiques / contraintes d'encombrement
- Microcontrôleur vs CPU
- Notion d'architecture
- Système temps-réel
- Protocoles
- Attaque

**Récupération d'information**
- Lecture de documentation technique (ex. : DataSheet et cartographie)
- Suivi des pistes physiques (ex.: Gerber)
- Voyage dans le temps (ex. : Gitlog / timemachine)
- Fiches d'identité

**Couche matérielle**
- Liaison série (Synchrone et Asynchrone)
- Accès au microcode (port débogage / lecture mémoire)
- Accès indirect / Injection de fautes (DMA/DPA)
- Introduction aux radio fréquences (SDR)

**Couche microcode**
- Rétro-ingénierie ARM (ex. : R2 et Ghidra)
- Exploitation ARM (Emulateur, Debogueur, Montage des partitions de fichiers)
- Développement sécurisé
- Simulation d'une carte “alpha” (version de développement)

**Couche concentrateurs**
- Passerelles
  - Modèle souscription/publication
  - Modèle ad-hoc
  - Gestion par événements
- Android
  - Architecture
  - Décompilation d'une archive applicative (APK)
  - Interaction avec la pile d'exécution
  - Analyse légale post-incident (Forensic)

**Couche Internet**
- Terminaison API / fonctions lambda
- Application Web
- Gestion des réseaux d'énergie / villes intelligentes

**Défense**
- Protection du matériel
- Développement sécurité par construction (Secure design)
- Sécurité périmétrique et surveillance (Parefeu, IDS/IPS, Gestion de journaux VS SIEM)

**Dates de nos prochaines sessions disponibles sur la page :**
https://www.hs2.fr/secuobj