CAP'TRONIC JESSICA FRANCE Association Loi 1901	**FORMATION PRATIQUE de 3 jours** **Du 04 au 06 juillet 2017** **09h00 – 17h00**

FORMATION : Sécurité des systèmes embarqués et des objets connectés
Comprendre les attaques hardware/software pour se prémunir

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.

Objectif : 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.

Public concerné : 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.

Pré-requis :

- **Connaissance en électronique ou logiciel embarqué** mais aucune expérience en sécurité informatique nécessaire
- Prévoir d'apporter un PC/MAC portable avec la dernière version de VMware Player, VMware Workstation, VMware Fusion
- Disque dur : Minimum 15GB d'espace libre, RAM : 4GB Minimum, 6GB recommandé
- Minimum CPU avec deux cœurs (Intel, I3 I5 or I7), 2 ports USB libres
- Système 64 Bits avec les droits d'administration : Windows, Linux or Mac os

Intervenant : M. Julien MOINARD – Société SERMA SAFETY SECURITY
Julien MOINARD est ingénieur en électronique et consultant sécurité informatique. Au fil des années (8 ans) il s'est doté d'une solide expérience dans ces domaines au travers d'expérimentations personnelles et professionnelles. Il contribue au projet Hardsploit en qualité de chef de projet. Julien MOINARD a formé de nombreuses personnes et a présenté ses projets dans de nombreuses conférences telles que BlackHat, Chaos Computer Congress, NullCon, CanSecWest…

Date et lieu : ▶ 04 au 06 juillet 2017 - de 09h00 à 12h30 et de 13h30 à 17h00
▶ **IMS** – Bât A31 - 351 Cours de la Libération - 33405 TALENCE CEDEX

Prix : 1500 € HT
Pour les adhérents CAP'TRONIC nous consulter.
Remarque : Cette formation est éligible au financement par votre Organisme Paritaire Collecteur Agréé (OPCA).

Contact et inscription :
Réservez votre place par email au plus tôt : **cathalinat@captronic.fr** – 05 57 02 09 62 - Nombre de places limité.

Moyens pédagogiques : Support de cours - Exercices pratiques – Travaux pratiques sur matériel de prêt
Moyens permettant d'apprécier les résultats de l'action : Evaluation de l'action de formation par la remise d'un questionnaire de satisfaction.
Moyen permettant de suivre l'exécution de l'action : Feuilles de présence signées par chaque stagiaire et le formateur par journée de formation.
Sanction de la formation : Attestation de présence

CAP'TRONIC JESSICA FRANCE Association Loi 1901	**FORMATION PRATIQUE de 3 jours** **Du 04 au 06 juillet 2017** **09h00 – 17h00**

PROGRAMME sur 3 jours

MODULE 1 : 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)

MODULE 2 : Comment les pirates accèdent au Hardware ?

- Présentation des outils et méthodes disponibles pour auditer un produit
- Créer son propre plan d'audit et différences avec l'audit logiciel
- TP: Extraire des données sensibles avec les outils d'audit comme Hardsploit.
- TP : Comment acquérir les signaux électroniques, outils et démonstration

MODULE 3 : Comment accéder au logiciel ?

- Présentation des différents type d'architecture (Microcontrôleur, FPGA), accès direct au logiciel via les interfaces d'E/S (JTAG / SWD, I2C, SPI, UART, RF bande ISM, etc.)
- Présentation d'accès au logiciel via des attaques à canal latéral (analyse de puissance)
- TP: Accès au Firmware par différentes interfaces

MODULE 4 : Attaques sur un système embarqué particulier, l'objet connecté (IoT)

- Session de TP complète appliquée à notre système embarqué vulnérable :
- TP : Identification des composants électroniques
- TP : Acquisition de signaux électroniques
- TP : Interception et analyse des signaux électroniques (avec Hardsploit)
- TP : Modification et extraction de firmware via les fonctions de debug JTAG (avec Hardsploit)
- TP : Fuzzing des interfaces externes pour détecter des vulnérabilités basiques sur l'embarqué
- TP : Attaques de dépassement de tampon sur un système embarqué
- TP : Exploitation de vulnérabilités durant un audit de sécurité hardware

MODULE 5 : Comment sécuriser votre matériel

- Conception sécurisée et cycle de vie de développement (SDLC)
- Examen des meilleures pratiques de sécurité matérielle pour limiter les risques
- TP: Limiter les accès JTAG et les vulnérabilités logicielles au niveau de l'embarqué
- Examen des protections contre les attaques à canal latéral

MODULE 6 : 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)

MODULE 7 : Exercice « Capture The Drone »

- Scénario pratique Attaque / Défense d'un mini - drone
- TP : Défendez votre drone et attaquer les autres en utilisant les outils et méthodes apprises (gagne celui qui obtient le plus de points)