FORMATION :
SÉCURITÉ DES SYSTÈMES EMBARQUÉS ET DES OBJETS CONNECTÉS – COMPRENDRE LES ATTAQUES HARDWARE/SOFTWARE POUR SE PREMUNIR
Du 13 au 15 février à Gardanne (13)

Durée : 3 jours (21 h) **Prix : 1 500 € HT (1 200 € HT pour les adhérents Cap'Tronic)**

PUBLIC VISE ET PREREQUIS

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.

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.

LIEU

Centre de microélectronique de Provence - 880 route de Mimet - 13120 GARDANNE

INTERVENANT

M. Julien MOINARD – Société SERMA Safety Security

PROGRAMME

➢ **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 ?**

- 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

➢ **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

JESSICA FRANCE – Direction Nationale
CEA/G – Bât 51C – 17 rue des Martyrs - 38054 GRENOBLE Cedex 9
Tél. 04.38.78.37.36 - Fax : 04.38.78.50.70 - www.captronic.fr

- **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

- **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 »**

- 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)

Moyens pédagogiques : Support de cours - Exercices pratiques - Mises en situation
Moyens permettant d'apprécier les résultats de l'action : Evaluation de l'action de formation par la remise d'un questionnaire de fin de stage.
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
