# TEST DE CYBERSECURITE DES SYSTEMES EMBARQUES

Formation

3 jours
2 250€ HT

*Kereval propose des formations Inter et en Intra-entreprise dispensées par des formateurs certifiés et experts en test logiciel. Selon les besoins spécifiques, Kereval est en mesure de dispenser des formations sur-mesure, dont le contenu et la durée sont adaptés à votre contexte.*

L'électronique et les logiciels embarqués des dispositifs médicaux gagnent en complexité. Les normes cybersécurité applicables permettent de garantir la qualité et la sécurité de ces dispositifs. Cette formation vous permet de comprendre la spécificité du risque cyber des systèmes embarqués dans les applications médicales, et de l'environnement avec lequel ils interagissent.

## Objectifs pédagogiques

- Comprendre les fondamentaux de la sécurité dans un dispositif embarqué
- Acquérir une compréhension des compétences d'un attaquant dans un environnement embarqué
- Appliquer de manière concrète les compétences acquises en manipulant un système embarqué, afin de renforcer la maîtrise des techniques présentées
- Se familiariser avec les protocoles radio et la radio logicielle
- Comprendre les risques associés à l'écosystème IoT

## Pré-requis

Il est recommandé d'avoir des compétences de base en informatique et électronique et de connaître les normes applicables à la cybersécurité des dispositifs médicaux.

## Public formé

Fabricants de dispositifs électroniques

## Contenu

La formation est composée de 3 modules :

**Module 1** : Sécurité dans les systèmes embarqués

**Les fondamentaux de la cybersécurité**

- Définitions et termes techniques (risque, vulnérabilité, exploit, etc.)
  - Relations entre risques, menaces et vulnérabilités (ISO 27000)
  - Qu'est-ce qu'un exploit ? Exemple pratiques

**Tour d'horizon de la menace dans le contexte d'un système embarquée**

- La sécurité embarquée
  - Pourquoi la sécurité de l'IoT est-elle importante ?
  - Comment diffère-t-elle de la sécurité IT traditionnelle ?
  - Frameworks, standard et guide

- La modélisation de la menace dans l'embarqué
  - Framework pour la modélisation de la menace (STRIDE)
  - Utilisation d'« attack tree » pour préciser la menace
  - Comment classer vos menaces à l'aide du système DREAD ?
  - Autres types de modélisation
  - Menaces communes dans l'IoT
- La méthode de test pour la sécurité embarquée
  - Reconnaissance passive (OSINT)
  - Couche matérielle (périphérique, interface de debug, attaques par canaux auxiliaires…)
  - Couche réseau (scan, détection de service, écoute réseau)
  - Analyse des protocoles et attaques des services
  - Test de pénétration des applications (web, mobiles)

**Hardware hacking**

- Analyse des composants d'un circuit imprimé
- Exploitation UART, JTAG et SWD
  - Présentation de l'UART, outils pour communiquer en UART, identification des ports UART et la vitesse de transmission
  - Présentation du JTAG et SWD, identification des pins, matériels utilisés
  - Démonstration
- Exploitation des bus de communications (SPI, I²C)
  - Matériels nécessaires
  - Fonctionnement du SPI
  - Lecture de mémoire à l'aide du SPI
  - Fonctionnement de l'I²C
  - Attaques pratiques sur l'I²C (sniffing)
- Firmware Hacking
  - Comment obtenir un firmware ?
  - Analyse statique d'un firmware (extraction des fichiers, analyse automatique)
  - Analyse dynamique (émulation de firmware)
- Les attaques par canaux auxiliaires
  - Définition et concept
  - Exemple d'attaque : DPA
  - Exemple d'attaque : Injection de fautes
- Mise en pratique sur système réel
  - Fingerprinting
  - Dump mémoire
  - Analyse de firmware

**Module 2** : Fonctionnement et vulnérabilités des transmissions sans fil

- Présentation d'un protocole radio « sécurisé » et des vulnérabilités associées
  - Protocole constructeur RKE
  - Bluetooth Low Energy
  - Zigbee
- Démonstration d'outils open source de manipulation de protocoles radio
  - Mirage toolkit : attaque "Man in the middle" sur du protocole BLE
  - De Gnuradio à wireshark : démonstration utilisant une LimeSDR pour "sniffer" du Zigbee

- Gnuradio en "Man In The Middle": paramétrage AES, CRC, CTR...

**Module 3** : Attaque de l'écosystème IoT

- Présentation des référentiels de sécurité (ISO 62443) et des différentes menaces spécifiques à l'IoT
  - Exemple de la prise en compte des tests de sécurité dans le mécanisme de mise à jour d'un équipement IoT : Packaging / Transport / Réception / Installation
  - Comment mettre en place des tests de sécurité et comment les inclure dans une chaine d'intégration continue ?
  - Exemple d'intégration de tests sur TLS
- Principes de base de cryptographie
  - La cryptographie symétrique : exemple avec DES et AES
  - La cryptographie asymétrique : exemple de RSA
  - La bonne utilisation des certificats
  - Les fonctions de hachage
- Méthodologie d'attaque sur un serveur distant
  - Reconnaissance des services en écoute
  - Découverte et exploitation de vulnérabilités
  - Exécution de code distant (RCE)
  - Maintien de l'attaque (backdoor) ou pivoting

## Méthodes pédagogiques

- Formation en présentielle
- Support ppt
- Démonstrations / Exercices pratiques

## Modalités d'accès et délais

Modalités d'inscription : nous contacter

Délais d'accès : de 1 à 6 mois

Les délais d'accès sont dépendants de la disponibilité de nos formateurs.

Accessible aux personnes en situation de handicap. Nous contacter pour tout aménagement spécifique.

## Modalités d'évaluation

Le participant complète un test de positionnement en amont et en aval pour valider les compétences acquises.

## Durée

21h sur 3 jours

| Prix intra – entreprise | Prix inter – entreprise |
|---|---|
| Nous contacter pour obtenir un devis | 2 250€ HT / stagiaire |

## Chiffres clés

Nous ne possédons pas encore d'indicateurs sur cette formation.