Cybersécurité des systèmes embarqués et objets connectés (IoT)

Cybersécurité des systèmes embarqués et objets connectés (IoT)

Formation | 3 sessions disponibles | Attestation de présence

Formation présentielle | 21 heures

Référence de la formation: FR-CyberSys-

Version: 13.05.2024. Vous trouverez toutes les informations actuelles sur https://academie-fr.tuv.com/s/FR-CyberSys-

Automobiles, appareils ménagers, dispositifs médicaux, avions… les systèmes embarqués sont présents dans de nombreux équipements autour de nous. Des cibles à haut potentiel pour espionner ou prendre le contrôle. Comment se protéger ?

Découvrez les secrets du hardware hacking et apprenez à déjouer les cyberattaques avant qu'elles ne surviennent avec notre formation Cybersécurité des systèmes embarqués et des objets connectés. Nous partagerons avec vous comment les pirates accèdent aux hardwares et logiciels, ainsi que les outils pour vous prémunir des cyberattaques. Vous serez en mesure d'effectuer un audit complet des vulnérabilités et d'assurer la sécurité des objets connectés et des systèmes embarqués.

Les objectifs

- Appréhender les vulnérabilités et les faiblesses de sécurité des systèmes embarqués,
- Sécuriser les systèmes embarqués dès l'étape de conception,
- Assimilez les techniques de piratage informatique,
- Savoir comment se protéger d'une cyberattaque, limiter les risques et les impacts.

Le public ciblé

Amateurs et professionnels en électronique ou sécurité IT, intéressées par la sécurité des hardwares et des systèmes embarqués (développeurs, architectes, intégrateurs, concepteurs de hardware, chefs de projet…).

Les prérequis

Aucune expérience en sécurité informatique n'est requise. Cependant, des notions en électronique ou logiciel embarqué sont souhaitables.

Le contenu de la formation

JOUR 1 :

Comprendre les bases du Hardware Hacking :

- Comprendre le contexte historique des attaques sur les objets connectés
- Revoir les vulnérabilités et les aspects offensifs et défensifs
- Connaître les fondamentaux de l'électronique
- Réaliser la prise d'information sur une cible

Comment les pirates accèdent au Hardware :

- Présenter des outils et méthodes disponibles pour auditer un produit
- Extraire des données sensibles avec les outils d'audit
- Acquérir les signaux électroniques, outils et démonstration

Comment accéder au logiciel :

- Présenter les différents types d'architecture (Microcontrôleur, FPGA), et les différents accès directs au logiciel via les interfaces d'entrée et sortie (JTAG / SWD, I2C, SPI, UART, RF bande ISM, etc.)
- Accéder au firmware via différentes interfaces

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

- Réaliser un audit complet appliqué à notre système embarqué vulnérable :
  - Identifier les composants électroniques
  - Acquérir des signaux électroniques
  - Intercepter et analyser des signaux électroniques
  - Modifier et extraire un firmware via les fonctions de debug

- Réaliser un fuzzing des interfaces externes pour détecter des vulnérabilités basiques sur l'embarqué
- Exploiter des vulnérabilités (dépassement de mémoire tampon) durant un audit de sécurité hardware

JOUR 2 :

Initiation à la cryptographe :

- Présentation des différents algorithmes et protocoles cryptographiques
- La génération de nombres aléatoires
- Les algorithmes symétriques
- Les algorithmes asymétriques
- Les fonctions de hachage
- La mise à jour sécurisée
- Les mécanismes de protections matériels (HSM, TPM, secure element)

Secure Development Life Cycle

- Conception sécurisée et cycle de vie
- Analyse de risque
- 10 bonnes pratiques de sécurité
- Durcissement d'un équipement embarqué
- Comprendre les meilleures pratiques de sécurité matérielle pour limiter les risques
- Limiter les accès JTAG et les vulnérabilités logicielles au niveau de l'embarqué

Piratage avec la technologie SDR :

- Apprendre la méthodologie d'audit SDR (capture, analyse, exploitation avec des logiciels radio)
- Utiliser des outils (GQRX, GNU Radio, etc.)
- Faire de la rétro-ingénierie d'un protocole sans fil à partir des émissions radio capturées dans les airs (communication sans fil d'un panneau à LED)

JOUR 3:

CTF « Capture The Drone » :

- Audit complet appliqué à un drone miniature vulnérable :
  - Identifier les composants électroniques

- Récupérer la documentation technique
- Intercepter et analyser les signaux numériques
- Intercepter et analyser les signaux radio
- Rejouer des trames radio pour faire démarrer le drone
- Extraire et reflasher le firmware afin de modifier les clés de sécurité
- Effectuer la rétroingénierie du binaire afin de trouver des vulnérabilités
- Exploiter ces vulnérabilités via la liaison radio
- Patcher le firmware vulnérable

Méthodes pédagogiques

- Alternance d'exposés théoriques, d'illustrations par des cas concrets, d'exercices individuels ou en groupes de travail et de jeux de rôle.

Modalités d'évaluation :

- Exercices individuels, en binôme, en groupe,
- Débriefing par les groupes,
- Débriefing par le formateur.

Informations importantes

Ce cours est proposé en partenariat avec SERMA Safety & Security.

Matériel Fourni : Le matériel électronique et informatique nécessaires pour les exercices seront fournis aux participants sur place :

- Ecran Full HD avec port HDMI
- Clavier, souris
- Raspberry Pi pré-préparé
- Hardsploit avec sa carte d'entrainement
- Outils d'analyse radio...

Si vous êtes en situation de handicap, nous vous remercions de bien vouloir nous contacter avant de procéder à l'inscription en envoyant un mail à formation@fr.tuv.com. Nous mettrons tout en œuvre pour répondre à votre besoin de formation.

Aperçu des dates et réservation

Réservez dès maintenant la date de votre choix directement en ligne sur https://academie-fr.tuv.com/s/FR-CyberSys- et profitez de ces avantages :

- Processus de réservation rapide
- Compte client personnel
- Réservation simultanée pour plusieurs participant(e)s.

Vous pouvez également utiliser le formulaire de commande pour commander par e-mail.