Formation secure boot et sécurisation de Linux embarqué

L'architecture de sécurité d'un produit Linux embarqué, de la chaîne de confiance au boot jusqu'aux processus qu'exige le Cyber Resilience Act.

4 jours	Intermédiaire à avancé	Sur site ou à distance	Français ou anglais
Durée	Niveau	Format	Langue (supports en anglais)

Présentation

Cette formation décrit l'architecture de sécurité d'un produit Linux embarqué et sa mise en place, de la chaîne de confiance au démarrage jusqu'aux processus qu'exige désormais le Cyber Resilience Act. Elle couvre le secure boot et le measured boot, les stockages de clés matériels, l'intégrité et le chiffrement du stockage, le durcissement du noyau et de l'espace utilisateur, les mises à jour sécurisées, la gestion des vulnérabilités et le SBOM, et les assemble dans un produit construit avec Yocto.

La formation ne rend pas un produit conforme à elle seule, mais elle couvre les exigences techniques du CRA et les processus qui les accompagnent, pour que l'équipe sache ce que son produit doit fournir, et comment.

Objectifs

À la fin de la formation, les participants savent :

- construire le modèle de menace d'un produit connecté ;
- mettre en place une chaîne de confiance du code ROM jusqu'au rootfs ;
- stocker des clés dans un TPM, un secure element ou un TEE, et s'en servir pour le measured boot et le chiffrement du disque ;
- protéger le stockage avec dm-verity et dm-crypt, et durcir le noyau et les services ;
- mener un processus de gestion des vulnérabilités et produire un SBOM avec Yocto ;
- relier ces mesures aux exigences essentielles du CRA.

Public

Ingénieurs et architectes Linux embarqué en charge de la sécurité d'un produit connecté, et responsables techniques qui préparent un produit au CRA.

Prérequis

Bonne connaissance de Linux embarqué, de sa chaîne de boot et du Yocto Project.

Programme

La cryptographie est utilisée tout au long de la formation sans en refaire la théorie, qu'un module optionnel couvre.

Jour 1

- Menaces, actifs, attaquants et modélisation des menaces
- Le secure boot : principes, images FIT signées, secure boot dans Yocto, verrouillage du bootloader
- Les stockages de clés matériels : TPM, secure elements et environnement d'exécution de confiance (TEE)
- Le measured boot et l'attestation à distance

Jour 2

- Les attaques physiques, les ports de debug et la production sécurisée
- Le durcissement du noyau : surface d'attaque, modules de sécurité, réglages à l'exécution
- L'intégrité du stockage : rootfs en lecture seule, dm-verity, dm-integrity, fs-verity

Jour 3

- Le chiffrement au repos : dm-crypt, LUKS2, déverrouillage automatique avec un TPM ou un secure element, fscrypt
- Utilisateurs, privilèges et contrôle d'accès : capabilities, seccomp, namespaces, sandboxing systemd
- Les mises à jour sécurisées : bundles signés, slots A/B, anti-rollback

Jour 4

- La gestion des vulnérabilités : CVE, triage, VEX et l'outillage CVE de Yocto
- Le SBOM : SPDX, CycloneDX, génération dans Yocto, conformité des licences
- Le Cyber Resilience Act : périmètre, exigences essentielles, obligations de signalement et échéances
- L'assemblage dans un produit construit avec Yocto
- Pour les produits x86 : clés UEFI Secure Boot, shim et unified kernel images, détaillés dans la formation chaîne de boot x86 et secure boot

Travaux pratiques et matériel

Les travaux pratiques se font sur des machines QEMU et sur les cartes de notre laboratoire : Arm 32 bits : STM32MP157C-DK2, BeagleBone Black ; Arm 64 bits : Raspberry Pi 4 et 5, NXP i.MX8M Mini, Khadas VIM3 ; x86 : QEMU x86, Machines x86_64 génériques, Kits de développement Intel. D'autres cartes, ou le matériel du client, peuvent être utilisés sur demande.

Les sessions ont lieu sur site, en France, en Belgique, en Suisse, en Allemagne et au-delà, avec le matériel fourni par LABCSMART, ou à distance. À distance, chaque participant dispose de son propre compte SSH et de son espace de travail sur notre serveur de build, et réalise les travaux pratiques sur des machines QEMU et sur de vraies cartes. Les exercices sont tirés de nos projets clients. Les formations sont données en français ou en anglais ; les supports de cours, eux, sont en anglais.

Modules optionnels

Ces modules approfondissent des sujets que la formation ne fait qu'introduire.

- SELinux dans un produit embarqué (1 jour)
- Sécurité réseau : nftables, TLS 1.3, TLS mutuel, durcissement SSH (1 jour)
- Développement sécurisé et tests de sécurité : analyse statique, sanitizers, fuzzing (1 jour)
- Cryptographie et PKI pour ingénieurs embarqués : primitives, signatures, X.509, OpenSSL, PKCS#11 (2 jours)

Qui anime cette formation

La formation est conçue et animée par le fondateur de LABCSMART, ingénieur Linux embarqué et noyau Linux avec plus de onze ans d'expérience industrielle. Il contribue au noyau Linux en amont pour les SoC Renesas RZ, dans les sous-systèmes PCIe, audio, Ethernet, thermique, DMA et horloges, et a écrit deux livres publiés chez Packt, *Linux Device Driver Development, Second Edition* (2022) et *Mastering Linux Device Driver Development* (2021), présentés sur notre page de publications.

Organiser une session pour votre équipe. Chaque formation est composée de modules indépendants. Une équipe peut retirer les modules dont elle n'a pas besoin et en ajouter d'autres à la place, et nous construisons aussi des formations sur mesure autour d'un SoC, d'une carte ou d'un projet. Contact : contact@labcsmart.com, https://labcsmart.com/fr/contact/. Page de la formation : https://labcsmart.com/fr/formations/formation-secure-boot-securisation-linux/