Formation chaîne de boot x86 et secure boot : UEFI, UKI

UEFI, boot loaders et unified kernel images : la chaîne de boot d'un produit x86, du firmware jusqu'à un Linux signé, mesuré et mis à jour sans risque.

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

Présentation

Cette formation couvre la chaîne de boot d'un produit Linux embarqué basé sur x86, et sa sécurisation. Le firmware UEFI vient du fabricant de la carte et ne se porte pas : le travail porte sur l'EFI System Partition et les variables EFI, le choix entre GRUB, systemd-boot ou une unified kernel image lancée directement par le firmware, les clés Secure Boot et le TPM, et les mises à jour qui doivent garder l'ensemble démarrable.

La formation s'appuie sur nos travaux sur des PC industriels x86. Pour les plateformes Arm, la formation chaîne de boot Arm et secure boot couvre le code ROM, TF-A, OP-TEE et U-Boot.

Objectifs

À la fin de la formation, les participants savent :

- expliquer comment UEFI trouve et lance Linux, et ce que contrôlent les variables EFI ;
- choisir entre GRUB, systemd-boot et une unified kernel image lancée directement ;
- fournir tôt dans le boot les surcharges ACPI et le microcode CPU ;
- générer, enrôler et protéger les clés UEFI Secure Boot, et utiliser shim et MOK si besoin ;
- lier des secrets à l'état du boot avec le TPM et le PCR 11 ;
- mettre à jour la chaîne de boot sans risque avec des slots A/B et BootNext.

Public

Ingénieurs qui construisent des produits Linux embarqués sur des cartes x86, des PC industriels ou des kits Intel, et doivent les démarrer et les sécuriser.

Prérequis

Bonne connaissance de Linux embarqué. Des bases du Yocto Project aident pour les parties intégration.

Programme

Le premier jour explique comment une carte x86 démarre Linux, le second comment sécuriser et mettre à jour cette chaîne.

Jour 1

- Le firmware dans la chaîne de boot : BIOS legacy et UEFI
- L'EFI System Partition, les variables EFI et efivarfs
- Démarrer Linux : l'EFI stub, systemd-boot, GRUB, et les unified kernel images avec ou sans systemd-stub
- Les tables ACPI et leurs surcharges, le microcode CPU
- Les formats d'image et l'intégration dans un build Yocto

Jour 2

- UEFI Secure Boot : la hiérarchie de clés PK, KEK et db, la génération et l'enrôlement des clés
- shim, les machine owner keys et la révocation SBAT
- Unified kernel images et TPM : le PCR 11 et les secrets scellés
- Les mises à jour A/B avec RAUC et BootNext
- Les pièges rencontrés en production : une CA trop large dans db, des clés sur le serveur de build, une révocation jamais prévue

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.

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-chaine-de-boot-x86-uefi/