oSEC4 - wolfSSL avancé pour la sécurité embarquée

Objectifs

- Établir des connaissances fondamentales sur la cryptographie, les algorithmes et les protocoles.
- Découvrir le fonctionnement du cryptage et la gestion des clés secrètes
- Comprendre et mettre en Œuvre la cryptographie
- Apprendre à mettre en Œuvre l'authentification sécurisée avec wolfSSL
- Développer en utilisant la bibliothèque de cryptographie de wolfSSL (wolfCrypt)
- Comprendre comment construire wolfMQTT sur des plateformes standards et l'utiliser dans une application IoT
- Compiler wolfSSH sur des plates-formes standard
- Démarrage sécurisé en utilisant wolfBoot (avec wolfCrypt et WolfSSL)

Pré-requis

- Programmation en C
- Expérience du développement des systèmes embarqués
- oSEC3 Sécurité embarquée avec wolfSSL

Environnement du cours

- Cours théorique
  - Support de cours au format PDF (en anglais) et une version imprimée lors des sessions en présentiel
  - Cours dispensé via le système de visioconférence Teams (si à distance)
  - Le formateur répond aux questions des stagiaires en direct pendant la formation et fournit une assistance technique et pédagogique
- Activités pratiques
  - Les activités pratiques représentent de 40% à 50% de la durée du cours
  - Elles permettent de valider ou compléter les connaissances acquises pendant le cours théorique.
  - Exemples de code, exercices et solutions
  - Pour les formations à distance:
    - Un PC Linux en ligne par stagiaire pour les activités pratiques, avec tous les logiciels nécessaires préinstallés.
    - Le formateur a accès aux PC en ligne des stagiaires pour l'assistance technique et pédagogique
    - Certains travaux pratiques peuvent être réalisés entre les sessions et sont vérifiés par le formateur lors de la session suivante.
  - Pour les formations en présentiel::
    - Un PC (Linux ou Windows) pour les activités pratiques avec, si approprié, une carte cible embarquée.
    - Un PC par binôme de stagiaires s'il y a plus de 6 stagiaires.
  - Pour les formations sur site:
    - Un manuel d'installation est fourni pour permettre de préinstaller les logiciels nécessaires.
    - Le formateur vient avec les cartes cible nécessaires (et les remporte à la fin de la formation).
- Une machine virtuelle préconfigurée téléchargeable pour refaire les activités pratiques après le cours
- Au début de chaque session (demi-journée en présentiel) une période est réservée à une interaction avec les stagiaires pour s'assurer que le cours répond à leurs attentes et l'adapter si nécessaire

Audience visée

- Tout ingénieur ou technicien en systèmes embarqués possédant les prérequis ci-dessus

Durée

- Totale : 12 heures
- 2 sessions de 6 heures

Modalités d'évaluation

- Les prérequis indiqués ci-dessus sont évalués avant la formation par l'encadrement technique du stagiaire dans son entreprise, ou par le stagiaire lui-même dans le cas exceptionnel d'un stagiaire individuel.
- Les progrès des stagiaires sont évalués de deux façons différentes, suivant le cours:
  - Pour les cours se prêtant à des exercices pratiques, les résultats des exercices sont vérifiés par le formateur, qui aide si nécessaire les stagiaires à les réaliser en apportant des précisions supplémentaires.
  - Des quizz sont proposés en fin des sections ne comportant pas d'exercices pratiques pour vérifier que les stagiaires ont assimilé les points présentés
- En fin de formation, chaque stagiaire reçoit une attestation et un certificat attestant qu'il a suivi le cours avec succès.
  - En cas de problème dû à un manque de prérequis de la part du stagiaire, constaté lors de la formation, une formation différente ou complémentaire lui est proposée, en général pour conforter ses prérequis, en accord avec son responsable en entreprise le cas échéant.

Plan

Première session

Advanced WolfCrypt usage

- Public Key Cryptography
  - RSA
  - DH (Diffie-Hellman)
  - EDH (Ephemeral Diffie-Hellman)
  - DSA (Digital Signature Algorithm)
- PKCS Public Key Cryptography Standards
  - PKCS#1 RSA Cryptography Standard
  - PKCS#3 Diffie-Hellman Key agreement Standard
  - PKCS#5 Password Based Cryptography Standard
  - PKCS#6 Extended-Certificate Syntax Standard Historic
  - PKCS#7 and RFC 3369 : Cryptographic Message Syntax (CMS)
  - PKCS#8 Private Key Information Syntax Standard
  - PKCS#9 Selected Object Classes and Attribute Types
  - PKCS#10 Certification Request Syntax Standard
  - PKCS#11 Cryptographic Token Interface Standard
  - PKCS#12 Personal Information Exchange Syntax Standard
  - PKCS#15 Cryptographic Token Information Syntax Standard
- Cryptographic Certification
  - FIPS 140-2 Certification
  - NSA Certification
- Progressive Cryptography
- Hardware Accelerated Cryptography
- X.509 Certificates
- Key and Certificate genration
- WolfCrypt CertManager API

Exercise : *Sign and Verify data with RSA*
Exercise : *Sign and Verify data with ECC*
Exercise : *Sign and Verify data with Ed25519*
Exercise : *Key Agreement with ECDH and Curve25519*
Exercise : *PKCS#7 and CMS bundle Generation and Verification*
Exercise : *wolfCrypt “FIPS Readyâ€Â•*
Exercise : *Progressive Cryptography*
Exercise : *Creating Keys and Certificates*
Exercise : *Generate RSA/ECC Key and Certificates via API*
Exercise : *WolfCrypt Certificate Manager*

Deuxième session

wolfBoot

- • Introduction
- Features
- Components
- Wolfboot bootloader
- Integrating wolfBoot
- Upgrading the firmware

Exercise : *Upgrading the firmware using wolfBoot*

wolfSSH

- Overview
- Building wolfSSH
- wolfSSH User authentication Callback
- wolfSSH SFTP
- wolfSSH SCP

Exercise : *wolfSSH examples with passwords and Keys*
Exercise : *SFTP with wolfSSH*
Exercise : *SCP with wolfSSH*

wolfMQTT

- MQTT and MQTT-SN Overview
- MQTT client
- MQTT packet
- MQTT socket
- API reference

Exercise : *MQTT Broker*

Renseignements pratiques

Renseignements : 12 heures