Formation Protocole Sécurité SSL/TLS sur MCU (STM32)

+ 1 jour

Objectif pédagogique :

Accélérer la prise en main des nouveaux concepts de programmation liés à l'utilisation de connectivité TCP/IP et sécurité SSL/TLS sur microcontrôleur.

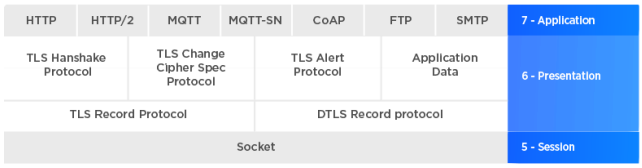
Prérequis :

La pratique du langage C et de sa mise en œuvre dans des applications à base de microcontrôleur est indispensable. De bonnes connaissances des protocoles TCP/UDP sont requises (formation réf. TCP-1J).

Méthode :

Manipulation sur PC avec des outils de développement (IDE, Compilateur GCC, Débogueur), une sonde JTAG/SWD sur carte d'évaluation à base de STM32 à cœur ARM Cortex-M4.

Durée : 1 jour (1 x 8 = 8 heures)



CycloneSSL

1) Introduction à la Sécurité sur Ethernet
Bases théoriques

Durée : 2h

- Historique de SSL 3.0 à TLS 1.2 & TLS 1.3
- Pile de protocoles de sécurisation SSL/TLS
- Encryption / Intégrité / Authentification
- Suites cryptographiques TLS • Algorithme d'échange de clés
- Cryptographie symétrique
- Cryptographie asymétrique
- Fonctionnement du handshake TLS
- Chaîne de certificats
- Format X.509
- Les certificats avec OpenSSL

2) Travaux pratiques TLS

Durée : 6h

Les travaux pratiques sont réalisés autour d'une pile de communication TCP/IP et SSL/TLS embarquée open source (ORYX CycloneTCP + CycloneSSL) sur carte à base de STM32. Les participants pourront choisir leurs TPs d'un commun accord et selon le temps disponible.

Exercices généraux :

- Configuration et utilisation de Wireshark
- Authentification par Identifiant et Password
- Création de certificats OpenSSL au format X.509

Mise en place d'un serveur HTTPS sur STM32

- Installation d'une pile TLS sur une cible embarquée du type ARM Cortex-M
- Authentification du certificat serveur par un client PC (Navigateur Windows)
- Contrôle sur votre PC par un organisme de confiance
- Etude des échanges Full TLS Handshake entre client et serveur

Mise en place Socket TLS pour un Client embarqué

- Rappel sur une connexion non-sécurisée d'un client à un serveur
- Installation de la couche de sécurité TLS sur le client embarqué
- Interrogation d'un serveur pour obtention d'une page HTML en mode sécurisé
- Contrôle d'authentification du serveur par le client
- Authentification du client en cas de demande de contrôle par le serveur
- Sauvegarde et restauration de session

Mise en place Socket TLS pour un Serveur embarqué

- Rappel sur une connexion non-sécurisée d'un serveur à un client
- Installation de la couche de sécurité TLS sur le serveur embarqué
- Contrôle des certificats serveur par un client
- Contrôles du client PC par le serveur embarqué

Références pour Formation SSL/TLS :

- **SSL-1JP** : formation inter-entreprises (1 jour)
- **SSL-1JS** : formation intra-entreprise (1 jour)

Références pour Formation TCP/IP + SSL/TLS :

- **TCP-SSL-2JP** : formation inter-entreprises (2 jours)
- **TCP-SSL-2JS** : formation intra-entreprise (2 jours)

Numéro de déclaration d'activité de formation n° 11 75 53750
(Cet enregistrement ne vaut pas agrément de l'Etat, en application de l'article L6352-12 du code du travail)

cynetis embedded

CYNETIS EMBEDDED • SARL au capital de 20 000 €
RCS PARIS 809 147 283 • N° TVA : FR80 809147283 • APE : 4651Z
Siège social : 76 rue des Grands Champs, 75020 Paris, FRANCE
Tél. : 01 85 08 70 69 • Email : info@cynetis-embedded.com
www.cynetis-embedded.com