Connectivité TCP/IP & Sécurité SSL/TLS sur MCU STM32 ARM Cortex-M

Application
TLS
TCP
IP

1 jour sur TCP/IP + 1 jour sur SSL/TLS

OBJECTIF

L'utilisation de microcontrôleurs 32 bit ne cesse de croître dans la réalisation d'applications électroniques embarquées. Lorsque des critères tels que la vitesse d'exécution, le besoin de connectivité, une taille mémoire limitée ou encore une consommation optimisée sont déterminants, l'utilisation de ces composants semble particulièrement adaptée. A cela s'ajoute une complexité logicielle croissante (multitâches, tâches prioritaires ou temps réel, utilisation de piles de communication et de sécurité). Notre formation vise à accélérer la prise en main de de les nouveaux concepts de programmation liés à l'utilisation d'une pile de communication TCP/IP et de protocoles de sécurité SSL/TLS qui sont probablement parmi les briques de middleware les plus complexes que l'on retrouve sur de petits microcontrôleurs.

VOUS APPRENDREZ COMMENT

- Mettre en place une pile de communication TCP/IP, utiliser les sockets UDP et TCP et configurer un serveur Web dynamique avec les contraintes propre à l'embarqué sur une cible microcontrôleur 32 bit.
- Comprendre les concepts de sécurité du protocole TLS pour vous permettre d'échanger efficacement avec le service informatique de votre entreprise.
- Mettre en place des protocoles sécurisés comme HTTPS sur microcontrôleur en comprenant les contraintes d'usage RAM.
- Utiliser un environnement de développement et de débogue JTAG / SWD (une démonstration des possibilités débogue via la Trace ETM est possible sur demande)

A QUI S'ADRESSE CE STAGE

Ce stage s'adresse aux ingénieurs et techniciens de développement qui souhaitent mettre en œuvre concrètement du middleware de connectivité et de sécurité sur microcontrôleur. La pratique du langage C et de sa mise en œuvre dans des applications à base de microcontrôleur du type ARM Cortex-M est indispensable.

EXERCICES PRATIQUES

Chaque participant sera doté pendant toute la durée du stage d'un PC muni d'un environnement de développement, d'une sonde de débogue USB - JTAG/SWD et d'une plate-forme d'évaluation à base de composant à cœur ARM Cortex-M. Notre formation est essentiellement basée sur des exercices pratiques. Les exercices consisteront en la mise en œuvre d'une pile TCP/IP + TLS 1.3, cette révision du protocole étant recommandée par les organismes officiels depuis fin 2018.

DOCUMENTS

L'ensemble des documents, comprenant les supports de cours, les notes d'application, les manuels d'utilisation, les articles techniques et les programmes étudiés pendant le stage vous sera remis au cours de la formation. Ce support vous apportera une aide précieuse pour exploiter avec succès une connectivité TCP/IP sécurisée par TLS dans vos applications futures.

INSCRIPTIONS

Email : info@cynetis-embedded.com

Téléphone : 01 85 08 70 69

Lieu de la formation :

Paris

ou sur site client

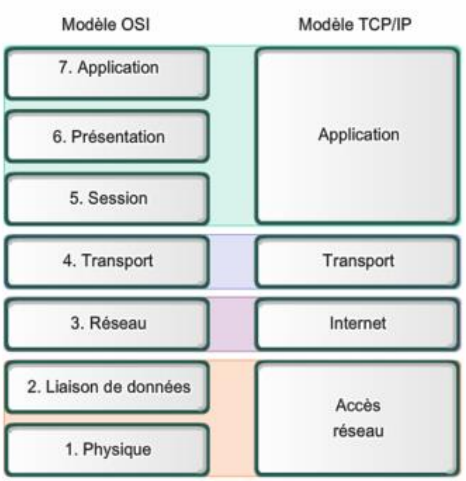
Connectivité TCP/IP & Sécurité SSL/TLS sur MCU STM32 ARM Cortex-M

Application
TLS
TCP
IP

1 jour sur TCP/IP + 1 jour sur SSL/TLS

CONTENU DU COURS : Connectivité TCP/IP (1 jour)

1) Bases théoriques (durée : 2h)

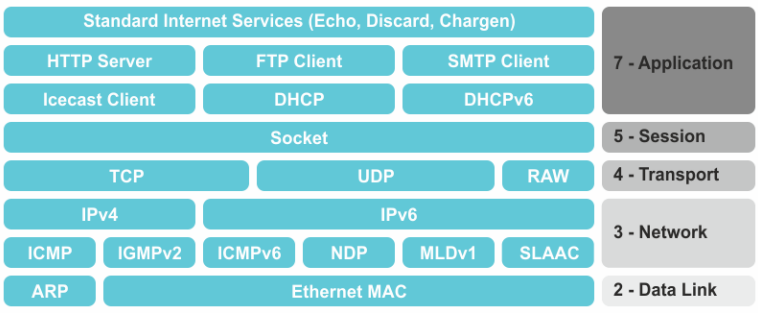


- Présentation du modèle OSI
- Présentation des couches protocolaires TCP/IP
- Ethernet et la gestion de collisions
- Adresse MAC et adresse IP
- Notion de routage
- Protocole ARP
- Utilisation des sockets en mode connecté (TCP)
- Utilisation des sockets en mode non connecté (UDP)
- Notions de Ports et notions de Sockets
- Connexion Client – Serveur

2) Travaux pratiques (durée : 6h)

Les travaux pratiques sont réalisés autour d'une pile de communication TCP/IP embarquée open source (CycloneTCP) sur carte à base de composant STM32 à cœur ARM Cortex-M4

- Prise en main d'une pile de communication TCP/IP sur STM32
- Fonctions de base d'un contrôleur Ethernet
- Mise en place d'un DHCP
- Interaction de la stack TCP/IP avec le RTOS FreeRTOS
- Découverte des sockets UDP et TCP au travers d'une application de tchat
- Mise en place d'un serveur Web avec contenu dynamique (CGI et Ajax)
- Mise en place de sockets et établissement d'une communication avec une application PC



Connectivité TCP/IP & Sécurité SSL/TLS sur MCU STM32 ARM Cortex-M

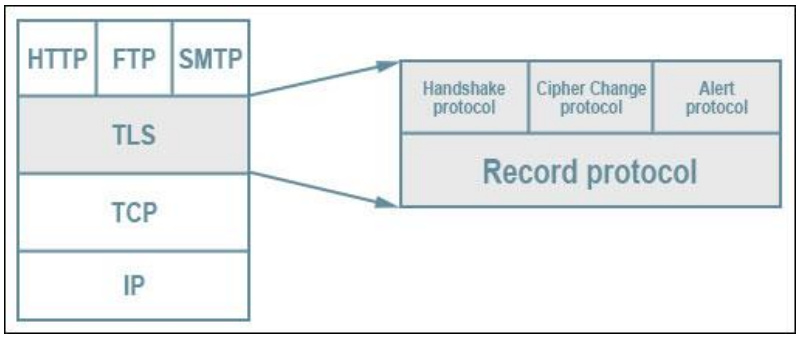
Application
TLS
TCP
IP

1 jour sur TCP/IP + 1 jour sur SSL/TLS

CONTENU DU COURS : Sécurité SSL/TLS (1 jour)

Cette formation a pour but de vous donner les bases théoriques sur les protocoles de sécurité et mettre en œuvre une communication TCP/IP sécurisée par le protocole TLS sur microcontrôleur.

3) 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 W.509
- Les certificats avec OpenSSL

Connectivité TCP/IP & Sécurité SSL/TLS sur MCU STM32 ARM Cortex-M

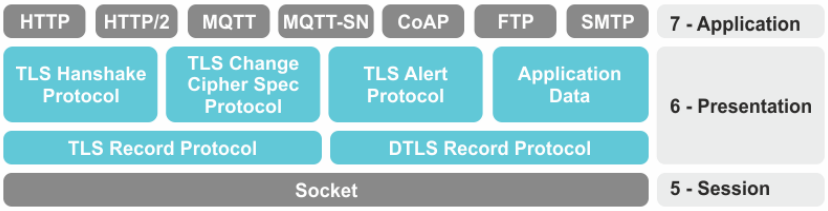
Application
TLS
TCP
IP

1 jour sur TCP/IP + 1 jour sur SSL/TLS

4) Travaux pratiques sur TLS (durée : 6h)

Les travaux pratiques sont réalisés autour d'une pile de communication TCP/IP et SSL/TLS embarquée open source (CycloneTCP + CycloneSSL) sur carte à base de composant STM32 à cœur ARM Cortex-M4.

Les participants pourront choisir leurs TPs d'un commun accord 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 de 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 de 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