



oSEC5 - Embedded Security for STM32-based devices

Objectives

- Understand embedded and STM32-specific security challenges, attack vectors, and threats.
- Apply modern security standards and best practices to STM32 devices.
- Implement secure boot and firmware protection on STM32.
- Apply secure network protocols (TLS/SSL, LoRaWAN, Sigfox, WiFi) on STM32.
- Follow IoT security best practices across communication layers.
- Implement secure firmware updates and OTA management for STM32.

Course environment

- Course will be using STM32 Tools (STM32CubeIDE, STM32CubeProgrammer, ...)
- Students will be given access to a shared filesystem to save and share their work.
- PDF course material

Prerequisites

- Familiarity with computer architecture
- Programming skills: Some programming experience, particularly in C
- Knowledge of STM32 Implementation and ARM implementations
- Basic understanding of Security Algorithms and Secure coding

Duration

- Total: 12 hours
- 2 sessions, 6 hours each
- From 40% to 50% of training time is devoted to practical activities
- Some Labs may be completed between sessions and are checked by the trainer on the next session

Environnement du cours

- Cours théorique
 - Support de cours au format PDF (en anglais).
 - Cours dispensé via le système de visioconférence Teams.
 - 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.
 - Un PC Linux en ligne par stagiaire pour les activités pratiques.
 - 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.
- Une machine virtuelle préconfigurée téléchargeable pour refaire les activités pratiques après le cours
- Au début de chaque session 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.

Plan du cours

First Day

Introduction to embedded security for STM32 devices

- Overview of embedded security and its importance
- STM32 Microcontroller overview and security features
 - STM32 MCUs and capabilities
 - Security features
 - ARM TrustZone overview
- Threads and attack vectors specific to embedded systems
 - Common attack vectors
 - Malware and exploits
 - Threat landscape for embedded systems

Exercise : Familiarizing with STM32 Security Tools

Secure Development

- Secure coding practices
 - Code reviews and audits
 - Input validation and sanitization
 - Memory management and buffer overflows
- Static and dynamic code analysis tools
 - Using static analysis tools
 - Using dynamic analysis tools
- Secure development lifecycle for STM32-based devices
 - Requirements gathering and threat modeling
 - Design and implementation
 - Testing and validation
 - Deployment and maintenance

Exercise : Using static and dynamic analysis tools to find vulnerabilities in sample STM32 Code

STM32 secure boot, firmware protection and Hardware assisted security

- Secure boot on STM32 Devices
 - Introduction to secure boot
 - Secure boot implementation
 - Secure boot verification and troubleshooting
- Firmware protection on STM32 devices
 - Introduction to firmware protection
 - Techniques for protecting firmware on STM32 Devices
 - Implementation of firmware protection on STM32
- Hardware assisted security on STM32 devices
 - Introduction to hardware assisted security
 - STM32's Cortex-M security features
 - Implementation of hardware assisted security on STM32

Exercise : Implementing secure boot on STM32 devices

Second Day

Network Security for STM32-based Devices

- Network Architecture for STM32-based Devices
 - Overview of network communication protocols for embedded systems
 - Secure communication protocols
 - Designing a secure network architecture for STM32-based devices
- Transport Layer Security (TLS)
 - Introduction to TLS and SSL
 - Implementing TLS/SSL on STM32-based devices
 - Secure communication using TLS/SSL on STM32
- WiFi security
 - Overview of WiFi security mechanisms and standards
 - Implementing secure WiFi communication on STM32
 - Best practices
- BLE security
 - Introduction to BLE
 - Overview of BLE security Mechanisms and standards
 - Implmeneting secure BLE Communications
 - Best practices for securing BLE communication
- LoRaWAN security
 - Introduction to LoRaWAN
 - Overview of LoRaWAN security mechanisms and standards
 - Implementing secure LoRaWAN communication on STM32-based devices
 - Best practices
- Sigfox Security
 - Overview of Sigfox
 - Implementing secure Sigfox communication on STM32-based devices
 - Best practices

IoT security

- Introduction to IoT Security
 - Unique security challenges faced by IoT devices
 - Overview of the common attack vectors and threats faced by IoT devices
- IoT security best practices
- Securing IoT devices at the network layer
 - IoT-specific network security protocols
- Access control and secure data transfer
 - Overview of authentication and authorization mechanisms for IoT devices
 - Discussion of secure data transfer protocols for IoT, such as MQTT and HTTPS
 - The role of application-level encryption in securing IoT devices
- Implementing secure application communication
 - Secure application communication between STM32 devices and the cloud or other systems
 - implementing secure access control, such as using JSON Web Tokens (JWT) and OAuth
- Best practices

Firmware update and management for STM32 devices

- Introduction to firmware update and management
 - Importance of firmware updates in maintaining the security of embedded systems
 - Overview of firmware update methods including manual and over-the-air (OTA) updates
- Secure firmware update processes
- OTA update mechanisms
 - Overview of OTA update mechanisms

- Implementing OTA updates, including server-side and device-side
- Best practices for OTA updates, including testing and deployment