SEC5 - Embedded Security for STM32-based devices

Objectives

- Understand the unique security challenges faced by embedded systems and STM32-based devices and learn how to identify potential attack vectors and threats.
- Learn about the latest security standards and best practices for embedded systems, and how to apply them to STM32-based devices.
- Learn about secure boot and firmware protection mechanisms, and how to implement them on STM32-based devices.
- Understand the principles of secure network communication and how to implement secure network protocols, such as TLS/SSL, LoRaWAN, Sigfox and WiFi security on STM32-based devices
- Learn about the best practices for IoT security and how to implement them on STM32-based devices at different layers of communication
- Understand the fundamentals of firmware update and management, and how to implement secure firmware update processes and OTA updates on STM32-based devices

Course Environment

- Theoretical course
  - PDF course material (in English) supplemented by a printed version for face-to-face courses.
  - Online courses are dispensed using the Teams video-conferencing system.
  - The trainer answers trainees' questions during the training and provide technical and pedagogical assistance.
- Practical activities
  - Practical activities represent from 40% to 50% of course duration.
  - Code examples, exercises and solutions
  - For remote trainings:
    - One Online Linux PC per trainee for the practical activities.
    - The trainer has access to trainees' Online PCs for technical and pedagogical assistance.
    - QEMU Emulated board or physical board connected to the online PC (depending on the course).
    - Some Labs may be completed between sessions and are checked by the trainer on the next session.
  - For face-to-face trainings:
    - One PC (Linux ou Windows) for the practical activities with, if appropriate, a target board.
    - One PC for two trainees when there are more than 6 trainees.
  - For onsite trainings:
    - An installation and test manual is provided to allow preinstallation of the needed software.
    - The trainer come with target boards if needed during the practical activities (and bring them back at the end of the course).
- Downloadable preconfigured virtual machine for post-course practical activities
- At the start of each session the trainer will interact with the trainees to ensure the course fits their expectations and correct if needed

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

Target Audience

- Any embedded systems engineer or technician with the above prerequisites.

Evaluation modalities

- The prerequisites indicated above are assessed before the training by the technical supervision of the traineein his company, or by the trainee himself in the exceptional case of an individual trainee.
- Trainee progress is assessed in two different ways, depending on the course:
  - For courses lending themselves to practical exercises, the results of the exercises are checked by the trainer while, if necessary, helping trainees to carry them out by providing additional details.
  - Quizzes are offered at the end of sections that do not include practical exercises to verifythat the trainees have assimilated the points presented
- At the end of the training, each trainee receives a certificate attesting that they have successfully completed the course.
  - In the event of a problem, discovered during the course, due to a lack of prerequisites by the trainee a different or additional training is offered to them, generally to reinforce their prerequisites,in agreement with their company manager if applicable.

Plan

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 toubleshooting
- Firmware protection on STM32 devices
  - Introduction to firmware protection
  - Techniques for protecting firmware on STM32 Devices
  - Implementation of firmware protection on STM32

- Haardware 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

Renseignements pratiques

Duration : 2 days
Cost : 2260 € HT