Safety and security

Embedded security

Embedded security is the practice of protecting embedded systems from cyber threats. These systems are found in a wide range of devices, including smartphones, automobiles, and medical equipment, and they are often used in critical applications. Ensuring the security of embedded systems is important to prevent unauthorized access or manipulation of the system and to protect the confidentiality, integrity, and availability of the system and its data. There are various approaches to securing embedded systems, including the use of secure processors and specialized security hardware, the implementation of security protocols, and the use of secure coding practices. It is also important to have a system in place for distributing updates and patches to address newly discovered vulnerabilities. At AC6 Training, we offer a range of courses on embedded security, including courses on secure coding practices, hardware security, and the use of secure processors. Our courses are designed to provide professionals with the knowledge and skills they need to design and implement secure embedded systems.

Main Courses

SEC1 - Developing C/C++ Secure Embedded Systems This course provides an introduction to embedded security and covers industry standards such as ISO/SAE 21434, IEC 62443, NIST SP 800-53, Common Criteria, and OWASP. It covers secure coding practices for C/C++ and introduces the RUST programming language with its built-in security features. Students will learn about secure software development methodologies, security testing, and cryptography in embedded systems. The course covers the design and implementation of secure embedded system hardware architecture and communication protocols. Additionally, it provides an overview of security best practices for IoT devices and systems.

SEC2 - Advanced Embedded Systems Security Create secure connected embedded systems Discover how to protect your programs from malicious user input, Secure System Software and Consideration, Apprehend the context and the use of Hypervisors and System Virtualization and Discover Security checks and Tools

SEC12 - Comprehensive Secure Systems Programming The oSEC12 course is designed for software engineers that need to design and program secure systems. This course is a combination of oSEC1 - Secure C/C++ Development for Embedded Systems course and oSEC2 - Advanced Embedded Systems Security course, with a special price when both consecutive sessions are booked at once.

SEC3 - wolfSSL for Embedded Security The oSEC3 course is designed for software/ Hardware engineers to understand how SSL/TLS Works , establish fundamental knowledge about cryptographic, algorithms, and protocols and Learn how to implement secure authentication with wolfSSL

SEC4 - Advanced wolfSSL for Embedded Security The oSEC4 course is designed for software/ Hardware engineers. The aim of this course is to discover how encryption works and how to manage secret keys, learn how to implement secure authentication with wolfSSL, building wolfSSH on standard Platforms, secure boot using wolfBoot (with wolfCrypt and WolfSSL)and understand how to build wolfMQTT on standard platforms and use it in an IoT application

SEC34 - Comprehensive Security with WolfSSL The oSEC34 course is designed for software/Hardware engineers that need to fully understand how SSL/TLS works, establish detailed knowledge about cryptographic algorithms and protocols and how to implement a full secured environment, integrated in a Public Key Infrastructure, with wolfSSL. This course is a combination of oSEC3 - wolfSSL for Embedded Security course and oSEC4 - Advanced wolfSSL for Embedded Security course, with a special price when both consecutive sessions are booked at once.

SEC5 - Embedded Security for STM32-based devices This course is designed to teach you about the security challenges faced by embedded systems and STM32-based devices. You will learn how to identify potential attack vectors and threats and understand the latest security standards and best practices for embedded systems. You will also learn about secure boot and firmware protection mechanisms and how to implement them on STM32-based devices.

Additionally, the course will cover 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. The course will also cover best practices for IoT security and how to implement them on STM32-based devices at different layers of communication. Finally, you will understand the fundamentals of firmware update and management and how to implement secure firmware update processes and OTA updates on STM32-based devices.

SEC6 - Embedded Security for NXP i.MX-based processors This course teaches the security challenges of embedded systems and NXP-based devices, covers latest security standards and best practices, and explains how to implement secure boot, network protocols, IoT security, and firmware updates.

SEC7 - ARM TrustZone for Cortex-M based devices This course aims to provide an in-depth understanding of the ARM v8-M architecture and its security features. It covers topics such as the Memory Protection mechanism, Security Attribution unit configuration, management of Security access faults, and building and debugging secure and non-secure software. The objective is to equip attendees with the necessary knowledge and skills to develop secure applications for ARM v8-M based systems.

SEC8 - Secured Embedded Linux Platform Build

Additional Courses

C8 - Critical Systems Safety Embedded systems are more and more critical and subject to safety constraints. This training introduces the main concepts and standards applicable to safety-critical systems.

oSEC3 - wolfSSL for Embedded Security The oSEC3 course is designed for software/ Hardware engineers to understand how SSL/TLS Works , establish fundamental knowledge about cryptographic, algorithms, and protocols and Learn how to implement secure authentication with wolfSSL

oSEC4 - Advanced wolfSSL for Embedded Security The oSEC4 course is designed for software/ Hardware engineers. The aim of this course is to discover how encryption works and how to manage secret keys, learn how to implement secure authentication with wolfSSL, building wolfSSH on standard Platforms, secure boot using wolfBoot (with wolfCrypt and WolfSSL)and understand how to build wolfMQTT on standard platforms and use it in an IoT application