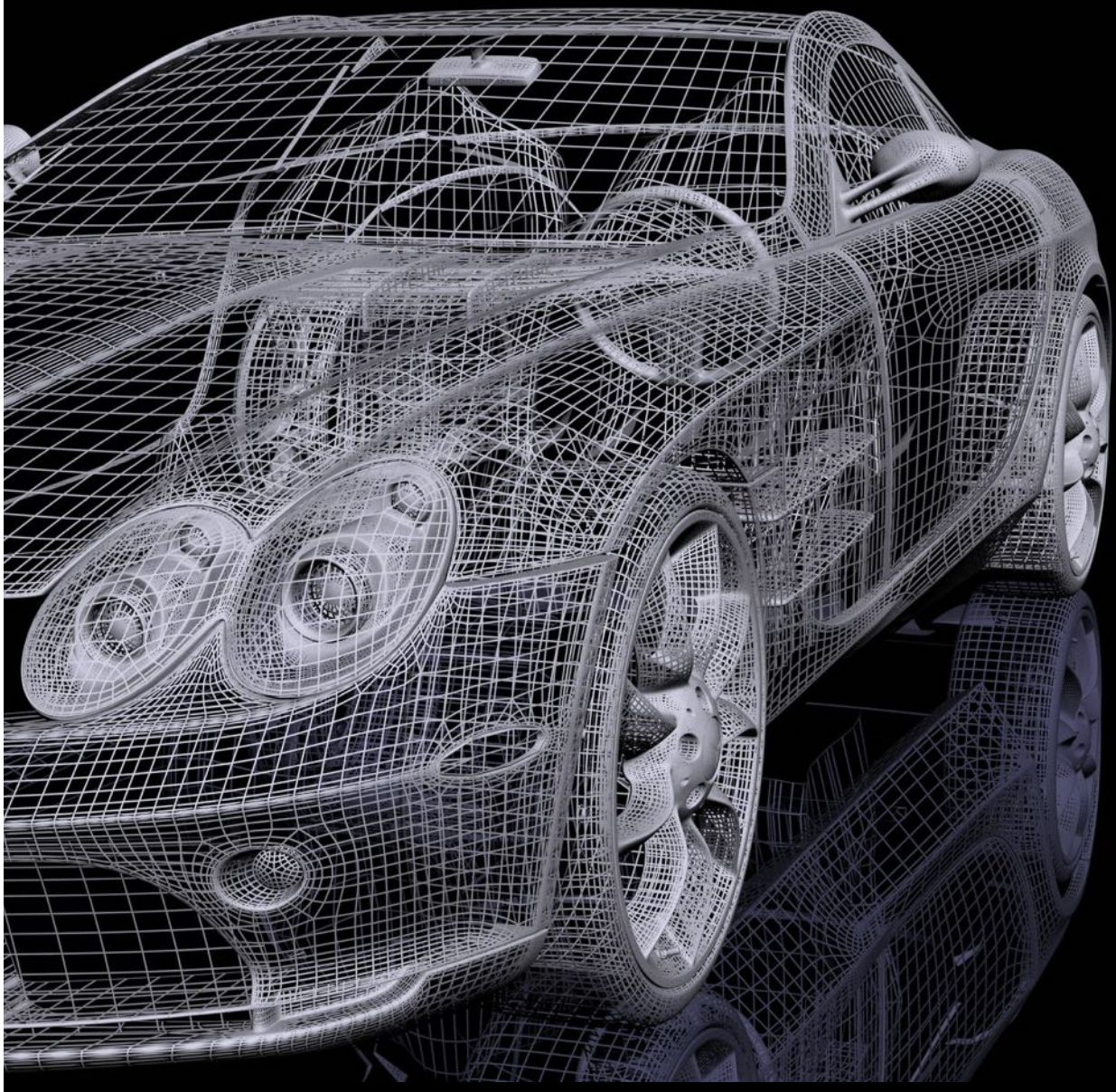
MathEmbedded

Introduction to Automotive Embedded Security Training Course



1. Introduction

1.1. Embedded Security Training

Embedded devices are often the hidden interface between the cyber world and the physical world, but connecting them to communications networks within vehicles and externally can leave them vulnerable to remote attacks that can result in brand damage, product returns, financial liabilities, and safety issues.

Understanding and addressing the risks posed by these devices is now a critical task for any OEM or automotive supplier.

This training is designed to help participants understand the technical and operational risks of embedded devices and where to start building security into organizational structure and processes.

1.2. About us

MathEmbedded is an independent, privately-owned company that provides security consultancy, specialist software development and training. We specialize in securing embedded devices and consider the end-to-end security when they are part of a complex ecosystem. MathEmbedded operates globally and has supplied consultancy and training to major OEMs and Tier 1 and 2 manufacturers.

Our trainers are active senior security consultants and can therefore add up-to-date knowledge and a wealth of experience to every training.

2. Training Scope

This course provides an introduction to understanding the risks associated with embedded systems and to ensure that security is “built in” from the start.

Securing embedded systems is difficult because:

- There is a closer connection between the software application, operating system, hardware and operating environment
- Physical security cannot be neglected – unlike servers, embedded devices aren’t safely stored at a remote location and are physically accessible to anyone
- There are often compliance requirements– especially in safety-critical situations
- There may be many identical embedded systems running the same software and all having the same security vulnerability, which opens up the potential to attack or exploit them collectively
- They have long product lifetimes and are expected to be reliable and available
- Embedded systems bridge the gap between the virtual, digital world and the physical world. Attacks on embedded systems can result in real, physical damage.

Based on many years’ real-world experience with securing embedded systems across a number of markets, this course will show you how to get started with well-established security practices that are tailored for embedded device development.

Aims of the course

1. To raise awareness of the need for security in the automotive industry
2. To identify specific security requirements participants might need to meet
3. To improve understanding of how security can be become part of the design/development/test process

Expected outcomes. Participants should be able to…

- Identify the security issues for automotive embedded devices
- Give examples of the consequences of embedded security failure
- Identify security technologies that are available to help
- Explain the security terminology commonly used in security requirements
- Identify specific security requirements that are directly applicable to their business
- Explain the connection between security, safety and functional requirements
- Use a high-level threat model to identify possible security vulnerabilities and their mitigations
- Create an action plan for meeting the security needs of their current processes

No previous knowledge of security is expected.

3. Course Description

Day 1

Security and the SSDL

In this session we describe the current automotive embedded system security landscape, identifying the risks and the threats and the reasons why embedded systems need different security measures to other computer systems. We also explain the need in embedded systems for system hardening as well as the targeted measures required for normal application security. We discuss how existing standards for safety and security address these requirements. Recent, high profile, attacks on automotive systems will be discussed.

Adopting a Secure Software Development Lifecycle (SSDL) can help to build security into your products, so this session explains what that involves as well as introduce some useful security terminology.

Hardware security

In this session, we explain how security lessons learned in other markets can be applied to embedded products in general. We look at the security features of modern embedded processors: hardware encryption engines, secure boot, key storage and management and provisioning.

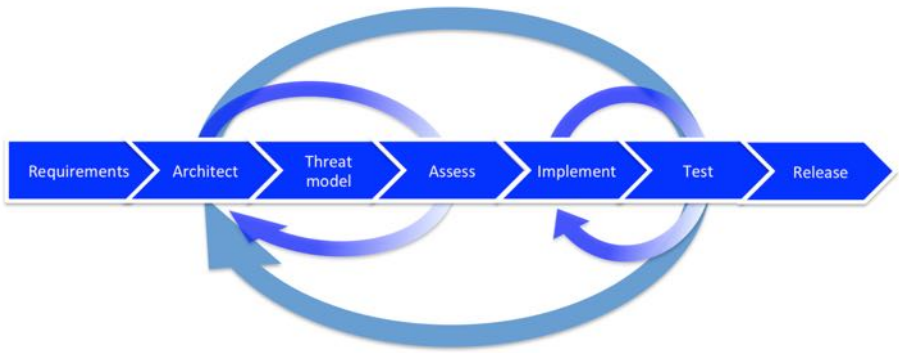
Common software attacks and mitigations

Two common vulnerabilities account for more than half the attacks on real-world systems. We will discuss the mechanisms behind these and other common attacks on embedded systems.

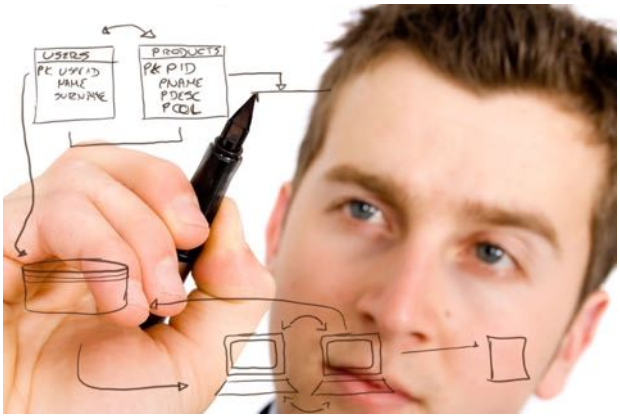
We will identify practical steps to mitigate against these attacks with best-practice rules for software design and implementation.

Common attacks – practical examples

In this session, participants can try their skills as the attacker of a vulnerable system. Working through increasingly complex levels of vulnerability, each successful exploit is followed by a practical exercise showing the techniques that could have been used to protect the system.



Day 2



Threat modelling and implementation

This session introduces threat modelling using data flow diagrams and STRIDE analysis to identify potential vulnerabilities in a design and covers how to design mitigations for these vulnerabilities using standard control measures.

It covers the deficiencies of STRIDE for embedded systems and some alternatives and enhancements that can be used.

It describes approaches for risk assessment once threats have been identified and mitigations have been produced. Strategies for prioritization of risk and getting the maximum benefit from limited resources are then explored and how system hardening measures can be used to address multiple risks.

Threat modelling example

In this session participants produce their own threat model of a typical consumer electronics product. Using the techniques from the previous session, possible threats and mitigations will be identified.

Using a simulation of the product, we demonstrate how to exploit some expected vulnerabilities. We will discuss how the mitigations from the threat analysis could be applied and test the result to make sure that the product is better protected.

Security architecture and design

In this session we explain how to identify your security goals and what you need to protect in your product and how to use these along with functional, safety and other compliance requirements to create your security requirements. We cover some guiding security principles to help build these requirements into the architecture and design of your project, with examples given from automotive systems.

The consequence of tight integration between the operating system and the application in embedded systems is also explored, as well as the tighter integration between software and hardware.

Testing, deployment and maintenance

In this final session we take a look at security testing practices such as threat model driven tests, automated tests and vulnerability assessment and penetration testing. We also discuss deploying and maintaining your secure products.

We conclude with a practical exercise in testing with a fuzzing tool.

4. Further information

For further information and pricing, please contact:

E-mail:	**info@mathembedded.com**
Telephone:	+44 117 911 9570
Website:	https://www.mathembedded.com

Upon request, MathEmbedded can also create completely customized training material. We have a large range of training material and so customization may not result in additional cost.

MathEmbedded

Smart Security