MathEmbedded Security Training

Summary of Courses

About MathEmbedded

MathEmbedded is an active design and development consultancy helping our customers to build secure embedded systems for broadcast systems, consumer electronics, IoT and automotive markets. We feed all our design experience and up-to-date security knowledge into our security courses:

- Hardening Embedded Linux
- Defensive Embedded C Programming
- Secure Software Development Lifecycle

Our Security Courses

We believe that security should not be an expensive add-on. Security is something you can build into all stages of your existing product development cycle:

- Requirements capture
- Hardware specification
- Ecosystem design
- Software architecture
- Software development and integration
- Verification and Test
- Support and incident response

Our courses help your team to adopt a security mindset and provide them with the technical knowledge to make your products secure.

This blend of organisational and technical skills is reinforced with hands-on practical examples and case studies and backed up with comprehensive written material for future reference.

Hardening Embedded Linux

Linux is often chosen as an embedded operating system for its flexibility and for the huge base of open source software that can support almost any peripheral and application. Linux has many configuration options and security features that are often underused and not well understood.

This 5-day course covers all aspects of creating a secure embedded system with Linux:

- Security fundamentals and guiding principles
- The secure software development lifecycle
- Common attacks and how to protect against them
- Threat Modelling and mitigation design
- Introduction to Cryptography
- Linux boot, bootloaders and the chain of trust
- Hardening the Linux kernel
- Isolating applications and processes, sandboxes and Linux Security Modules
- Network and peripheral communications security
- Developing, building and maintaining secure software
- Securing the run-time environment
- Secure information storage and file systems
- Security testing
- Secure software update
- Using Open Source software

The course raises awareness of security vulnerabilities with a fun Wargame. Presentations are reinforced with hands-on investigations of the tools and techniques discussed.

Defensive Embedded C Programming

Software written in C is at the heart of most embedded systems. It is a powerful and versatile language but Its inherent flexibility is often also the cause of security weaknesses.

This 3-day course shows developers how to look beyond the function of their software and code securely in C.

Topics include:

- Programming in a secure software development lifecycle
- Common software attacks and how to protect against them
    - Command injection
    - Buffer overflow on the stack and heap, ROP gadgets
    - Null pointer dereference
    - Memory allocation vulnerabilities, use-after-free, double free
    - Integer overflow
    - Format string vulnerabilities
    - Race conditions, File I/O, signal handlers
    - Side channel attacks
- Securing multi-threaded applications and IPC mechanisms
- Security guidelines to add to your favourite software design methodology
- Use of cryptography, code signing
- Testing for security, code review, static and dynamic analysis

The course is not specific to any platform or operating system, although interaction with Posix-type operating systems is discussed.

IoT Software Security

Consumer, automotive, medical and industrial ‘things’ connected to the Internet are creating security concerns for the companies that operate those devices and also for the rest of us that become vulnerable to attack from botnets of compromised devices.

This 4-day course covers all aspects of creating embedded software architectures that secure the end-to-end operating environment for your sensors, actuators, gateways, networks and servers.

The course looks at components of a typical IoT ecosystem, but is not specific to any particular platform.

Topics include:

- Security fundamentals and guiding principles
- The secure software development lifecycle
- Common attacks and how to protect against them
- Threat Modelling and mitigation design
- Introduction to Cryptography
- Device identity and provisioning
- Secure boot and the Chain of Trust
- Network and peripheral communications security
- Typical IoT ecosystems
- Industry-standard protocols and data formats
- Security hardware options
- Security testing
- Secure software update
- Using Open Source software

Secure Software Development Lifecycle

This one-day course provides foundation knowledge for an organisation that wishes to design, develop and maintain secure embedded software products by considering security and privacy at all stages of the software development lifecycle (SDL).

The course can help you adopt an industry standard SSDL (Microsoft SDL, BSIMM, SAMM, etc.) or incorporate security into your existing lifecycle stages, whether formally defined (e.g. ISO 26262) or ad hoc.

Topics include:

- Understanding current threats and evaluating the risk
- Identifying your exposed attack surface
- Threat Modelling
- Specifying cost-effective security measures at each lifecycle stage: requirements, design, development, verification, test, release and support
- Adopting appropriate industry standards and guidelines

The course is applicable to software systems on all platforms, for all operating systems and coding languages.

The Wargame

As well as learning how to protect a system, trainees on most courses gain awareness of how attackers view a system and execute attacks through a series of practical challenges in the Wargame, our capture-the-flag server that is vulnerable to a number of typical attacks.

Personalisation

We discuss the detailed contents of each course with you to make sure we meet the needs of your team. We are always open to adapting or adding new material for a better fit with your target market.

Half day/One day

A shorter version of each course, covering the main organisational issues, is suitable as an information primer for senior managers and board members.

Extra Days

With an extra day or more MathEmbedded consultants present the course content with workshop sessions to apply the course objectives to the customer's products and processes. Workshops can include:

- Identifying potential threat actors and threats to the customer's products using abuse cases
- Identifying security and privacy goals and assets to protect
- Applying SSDL templates and techniques to the customer's current development lifecycle process
- Develop a threat model of a product or system, perform a risk analysis and specify standard mitigations
- Add steps to ensure security and privacy to the customer's current software development methodology
- Create a checklist for verifying software security and privacy

Technical workshops can also initiate security assessment and design for a specific product:

- Software architecture security evaluation
- Secure device provisioning
- Securing the software update mechanism
- Securing network connections and communications

Pricing and terms

Courses are offered under MathEmbedded's standard terms and conditions, as detailed on our Booking Form.

This document is subject to revision without notice. It does not constitute a contract or commitment to provide any products or services.

Mathembedded Ltd.
Park House
10 Park Street
Bristol BS1 5HX

+44 117 911 9570
security@mathembedded.com