MathEmbedded

SECURITY FOR EMBEDDED DEVICES

MathEmbedded provides software security services for connected electronics products. We specialise in helping you to get your trusted product to market faster and by providing security support throughout the lifetime of the product.

EMBEDDED LINUX SECURITY HARDENING TRAINING

THE PROBLEM

Linux is being used in an increasing number of embedded devices including set-top-boxes, automotive in-vehicle infotainment, WiFi routers and home gateways, smart meters, industrial equipment and even domestic white goods.

Increasingly these devices are being connected to networks and this can leave them vulnerable to **remote attacks** that **can result in brand damage, financial liabilities, product returns** and even **legal issues**.

"Hardening" Linux systems to make them more resistant to attack is possible and is something that should be performed for every connected embedded product.

HOW CAN WE HELP?

MathEmbedded can support you by providing hands-on **Linux system and application hardening training** for your engineering teams.

WHO ARE WE?

MathEmbedded have been working since 2010 with security vendors, silicon manufacturers, consumer electronics OEMs and operators to help them understand the security issues introduced by the use of complex software platforms.

THE SERVICE

MathEmbedded offers an intensive 3 day fixed-price training course for up to 16 people that is conducted on your premises.

The course contains a mix of theory and practical sessions. Using a practical example system, it teaches each participant to increase the security step-by-step by:

- Understanding security requirements and what needs to be protected
- Analysing the system and software architecture with respect to security
- Understanding how systems are attacked
- Hardening the boot process
- Improving the security of the Linux kernel
- Hardening the software environment to resist commonly used attacks
- Restricting access to and from the network
- Protecting sensitive data on the filesystem
- Isolating and sandboxing vulnerable software components
- Using advanced techniques such as Linux Security Modules (including SELinux) to limit the impact of a successful attack

The trainers have many years of experience working with embedded consumer electronics products and the courses are designed to provide pragmatic and real-world advice.

The course can also be tailored to suit your particular hardware and software environment.

CONTACT US

For more information on pricing and availability of this service, or other services from MathEmbedded, please contact us using the details below.

MathEmbedded

www.mathembedded.com

For more information contact us by email: security@mathembedded.com