# Embedded Security Boot Camp®
# Course Syllabus

Course Length: 4 Days
CEUs: 3.0
Format: Hands-on/Lecture

Barr Group's Embedded Security Boot Camp® is a 4-day immersion into the unique challenges of building security into embedded devices. Through lectures and hands-on exercises, this intense, fun, and information-rich program will lead engineers through the steps of architecting and implementing secure embedded systems applications, including preventing electronics, firmware, and network attacks using only the processing power and memory of resource-constrained embedded devices. This course is best suited for experienced embedded systems design engineers. All exercises are done using an ST Microelectronics target development board.

Attendees will receive a fully equipped development kit with the hardware and resources necessary to develop a secure embedded system.

- STMicroelectronics ARM Cortex-M4 STM32F417IG Processor with Crypto Accelerator (external link)
- An electronic copy of all lecture slides
- An electronic Exercise Manual with instructions for all programming exercises,
- A USB thumb drive containing:
    - Source code starting points for the exercises
    - An electronic copy of the book Programming Embedded Systems with C and GNU Development Tools (link is external) by Michael Barr and Anthony Massa
    - An electronic copy of the book Embedded C Coding Standard by Michael Barr
    - An electronic copy of the book Embedded Systems Dictionary (link is external) by Jack Ganssle and Michael Barr
    - Datasheets and User's Manuals for all of the hardware and tools
- A certificate of course completion

BARR group
The Embedded Systems Experts

**Prerequisites**

Attendees should be comfortable with writing code that interfaces with microcontroller hardware.

**Course Syllabus**

- Introduction
  - Embedded Systems Attacks
  - Uniquely Embedded Concerns
  - Reliability and Security
  - Security Arms Race
  - Role of Obscurity
- Threat Assessment
  - Attackers and Assets
  - Attack Surface
  - Attack Trees
  - Security Policy
- Random Numbers and Entropy
  - Random Numbers' Role in Security
  - Entropy
  - Random Number Generators
- Protecting Data At Rest
  - Block Ciphers
  - Cipher Modes
  - Hashes
  - Message Authentication Codes
- Common Firmware Vulnerabilities
  - Backdoors
  - Common Programming Bugs
  - C++ Techniques
  - Change of Execution Attacks
  - Denial of Service (DOS)
- Defensive Software Architectures
  - Combating Complexity
  - Secure RTOS
  - Memory Partitioning and Protection
  - CPU Time Partitioning
  - Locking Down Firmware

- Defensive Hardware Interfaces
    - Exception Handling
    - Race Conditions
    - User Interface
    - Case Study: A/D Converters
    - FPGAs and Security
- Public Key Cryptography
    - Key Exchange
    - RSA Cryptosystem
    - Elliptic Curve Cryptography
    - Digital Signatures and Certificates
    - Key Management
- Protecting Data In Motion
    - Concerns
    - Secure Protocols
    - SSL / TLS
- Secure Software Process
    - Capturing Security Requirements
    - Secure Coding Standard
    - Peer Code Reviews
    - Static Analysis