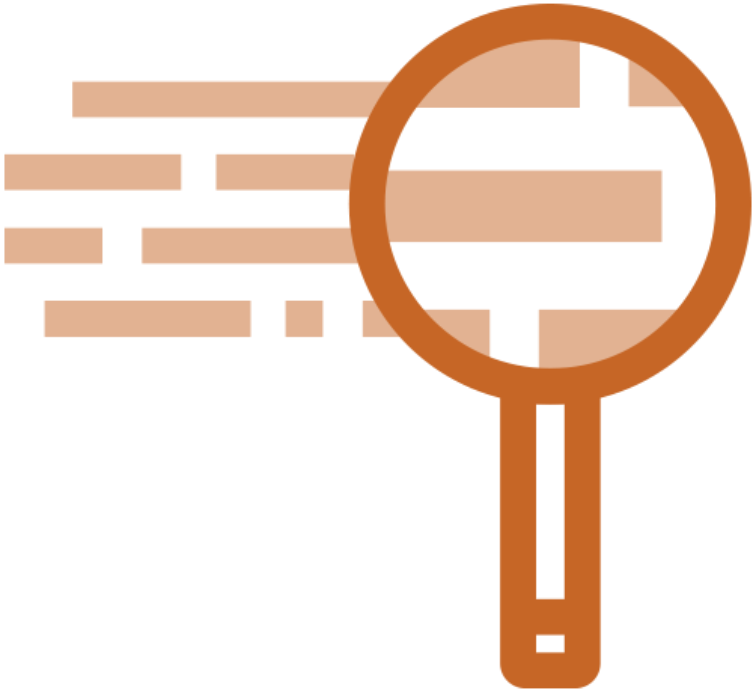
ZYBERUM

CYBER SECURITY FIRM

Secure Development Training

Introduction, C/C++ Secure Development, IoT, Embedded & Automotive Security Specialists



Feb, 2020

Table oft Content

Intro to Secure Development

Description

To create safe and secure code, it is important to understand the risks products face. This training will explain why security is important, what are vulnerabilities, and how does a hacker work when attacking a device/product.

* All contents include hands-on practice on a virtualized lab environment.
* All content can be adapted to the customer's needs, and additional focused subject can be added.
* This includes security specific fields as: Medical Devices, Automotive, Smart Home, Linux Systems and more.

Content

- What is cyber security
  - The importance of security
  - Famous attacks
  - Modern threats

- Intro to vulnerabilities
  - What are vulnerabilities
  - Vulnerabilities creation
  - Vulnerabilities types

- Workflow of an attacker
  - Mapping weak spots
  - Reverse engineering workflow
  - Exploitation process

Target Audience / For Whom?

- Software Developers
- Software Architects
- Project Manager
- Pen tester / Security Researcher
- Security Officer

Duration

- 0.5 days

Prerequisites

- None

info@zyberum.com | www.zyberum.com | Tel: +49 176 439 17074

C/C++ Secure Development

Description

This seminar provides a vast overview of security risks and vulnerabilities when developing low-level programs, by reviewing vulnerabilities developers could create, deep explanation of how hackers leverage them, and learning how to avoid them.
Hands-on practice of detecting and mitigating C/C++ vulnerabilities that are widely found in low-level programs, including the theoretical knowledge required to avoid creating vulnerabilities while writing code. As most vulnerabilities found in code are created due to missing knowledge of the developer, this is information crucial to every development team.
* All contents include hands-on practice on a virtualized lab environment.
* All content can be adapted to the customer's needs, and additional focused subject can be added.
* This includes security specific fields as: Medical Devices, Automotive, Smart Home, Linux Systems and more.

Content

- Introduction to embedded security
  - The importance of security
  - Vulnerabilities types and classification
  - Memory layout in compiled software

- Memory Vulnerabilities
  - Stack overflows
  - Heap overflows
  - DEP/ASLR
  - Double free
  - Null Dereference
  - Format string attacks
  - Integer overflows
  - Command Injections

- State machines
  - State escape
  - Global manipulation

- Summary lab exercise – C server
  - Finding security mistakes
  - Fixing badly written code

info@zyberum.com | www.zyberum.com | Tel: +49 176 439 17074

Target Audience / For Whom?

- Software Developers
- Software Architects
- Project Manager
- Pen tester / Security Researcher
- Security Officer

What?

- Live Hacking
- Exercises
- C/C++ Secure Coding

Duration

- 2 days

Prerequisites

- Knowledge in C/C++

info@zyberum.com | www.zyberum.com | Tel: +49 176 439 17074

Embedded & IoT Secure Development

Description

This seminar provides the must-known information when designing and developing embedded & IoT devices – by learning how to avoid creation of vulnerabilities, usage of encryption and embedded security systems.

Hands-on practice of detecting and mitigating C/C++ vulnerabilities that are common in embedded devices, including the theoretical knowledge required to avoid creating vulnerabilities while writing code. As most security issues found in devices are created due to missing knowledge of the developer, this is information crucial to every development team. Overview of cryptographic mechanisms that are commonly misused when implementing security systems for devices, learning how to correctly use them and avoid common mistakes. Examination of widely used security features and analysing design vulnerabilities found in them.

* All contents include hands-on practice on a virtualized lab environment.
* All content can be adapted to the customer's needs, and additional focused subject can be added.
* This includes security specific fields as: Medical Devices, Automotive, Smart Home, Linux Systems and more.

Content

- Introduction to embedded security
  - The importance of security
  - Vulnerabilities types and classification
  - Memory layout in compiled software

- Memory Vulnerabilities
  - Stack overflows
  - Heap overflows
  - DEP/ASLR
  - Double free
  - Null Dereference
  - Format string attacks
  - Integer overflows
  - Command Injections

- State machines
  - State escape
  - Global manipulation

- Cryptographic mechanisms & How to use them
  - Passwords & Privileges
  - Secure password storing
  - Password cracking
  - Hashes
  - Encryption & Decryption
  - PKI & Signatures
  - SSL/TLS

- Physical attacks
  - TOCTOU attacks
  - SPI manipulation
  - Memory replacement
  - JTAG & Debug ports
  - Glitching

- Security based features implementation
  - Secure boot
  - Disk encryption
  - Software updates
  - Server communication

- Integrating security into the development process
  - Risks in external libraries
  - External libraries management
  - Automatic security analysis

- Summary lab exercise – Bootloader vulnerabilities mitigations
  - Finding security mistakes
  - Fixing badly written code

Target Audience / For Whom?

- Software Developers
- Software Architects
- Project Manager
- Pen tester / Security Researcher
- Security Officer

What?

- Live Hacking
- Embedded
- Hands-On Exercises
- C/C++ Secure Coding

Duration

- 3-4 days

Prerequisites

- Knowledge in C/C++
- Basic Linux command line
- Embedded development experience is recoomended

Automotive ECUs Unique Security Threats

Automotive Security Specialist/Developer

Description

One of the most fast-growing embedded market is the automotive industry, and like other embedded devices – ECUs could be vulnerable to cyber threats. This training was built by world class automotive security experts to teach automotive developers the dangers ECUs face and how to protect them. It will go over unique protocols and threats relevant for the automotive industry and how to handle and protect them.

* All contents include hands-on practice on a virtualized lab environment.
* All content can be adapted to the customer's needs, and additional focused subject can be added.

Content

- Automotive Attack Surface
  - History of automotive threats
  - Modern attack surface
- DoIP
  - The DoIP state machine
  - Route Escapes
- Unified Diagnostic Services
  - Secure session control
  - DID handling
  - Safe routine handlers
  - Flashing verification
- ISOTP Parsers
  - ISOTP fuzzing
  - State confusions
  - CANFD threats
- Summary lab exercise
  - Writing an ISOTP parser for fuzzing

info@zyberum.com | www.zyberum.com | Tel: +49 176 439 17074

Target Audience / For Whom?

- Automotive Software Developers
- Automotive Software Architects
- Automotive Project Manager
- Automotive Pen tester / Security Researcher
- Automotive Security Officer

What?

- Live Hacking
- Embedded
- Hands-On Exercises
- C/C++ Secure Coding

Duration

- 1 days

Prerequisites

- Knowledge in C/C++
- Linux
- Embedded development
- Automotive protocols

info@zyberum.com | www.zyberum.com | Tel: +49 176 439 17074