

# Secure coding in C++

**CYDCpp3d | 3 days | On-site or online | Hands-on**

Your application written in C and C++ works as intended, so you are done, right? But did you consider feeding in incorrect values? 16Gbs of data? A null? An apostrophe? Negative numbers, or specifically -1 or  $-2^{31}$ ? Because that's what the bad guys will do – and the list is far from complete.

Handling security needs a healthy level of paranoia, and this is what this course provides: a strong emotional engagement by lots of hands-on labs and stories from real life, all to substantially improve code hygiene. Mistakes, consequences, and best practices are our blood, sweat and tears.

All this is put in the context of C and C++, and extended by core programming issues, discussing security pitfalls of these languages.

So that you are prepared for the forces of the dark side.

So that nothing unexpected happens.

Nothing.

## Cyber security skills and drills



26 LABS



5 CASE STUDIES

### Audience

C/C++ developers

### Group size

12 participants

### Preparedness

General C++ and C development

### Outline

- Cyber security basics
- Memory management vulnerabilities
- Memory management hardening
- Common software security weaknesses
- Wrap up

### Standards and references

SEI CERT, CWE and Fortify Taxonomy

### What you'll have learned

- Getting familiar with essential cyber security concepts
- Identify vulnerabilities and their consequences
- Learn the security best practices in C and C++
- Input validation approaches and principles

# Table of contents

## Day 1

---

### › Cyber security basics

What is security?

Threat and risk

#### Cyber security threat types – the CIA triad

Cyber security threat types – the STRIDE model

Consequences of insecure software

### › Memory management vulnerabilities

#### **Assembly basics and calling conventions**

- x64 assembly essentials
- Registers and addressing
- Most common instructions
- Calling conventions on x64
  - Calling convention – what it is all about
  - Calling conventions on x64
  - The stack frame
  - Stacked function calls

#### **Buffer overflow**

- Memory management and security
- Buffer security issues
- Buffer overflow on the stack
  - Buffer overflow on the stack – stack smashing
  - Exploitation – Hijacking the control flow
  - 🔗 *Lab – Buffer overflow 101, code reuse*
  - Exploitation – Arbitrary code execution
  - Injecting shellcode
  - 🔗 *Lab – Code injection, exploitation with shellcode*
- Buffer overflow on the heap
  - Unsafe unlinking
  - 📖 *Case study – Heartbleed*

- Pointer manipulation
  - Modification of jump tables
  - Overwriting function pointers

## Best practices and some typical mistakes

- Unsafe functions
- Dealing with unsafe functions
- 🔗 *Lab – Fixing buffer overflow*
- What's the problem with `asctime()`?
- 🔗 *Lab – The problem with `asctime()`*
- Using `std::string` in C++
- Manipulating C-style strings in C++
- Malicious string termination
- 🔗 *Lab – String termination confusion*
- String length calculation mistakes
- Off-by-one errors
- Allocating nothing

## Day 2

---

### › Memory management hardening

#### Securing the toolchain

- Securing the toolchain in C and C++
- Using `FORTIFY_SOURCE`
- 🔗 *Lab – Effects of `FORTIFY`*
- AddressSanitizer (ASan)
  - Using AddressSanitizer (ASan)
- 🔗 *Lab – Using AddressSanitizer*
- Stack smashing protection
  - Detecting BoF with a stack canary
  - Argument cloning
  - Stack smashing protection on various platforms
  - SSP changes to the prologue and epilogue
- 🔗 *Lab – Effects of stack smashing protection*

#### Runtime protections

- Runtime instrumentation
- Address Space Layout Randomization (ASLR)

- ASLR on various platforms
- 🔗 *Lab – Effects of ASLR*
- Circumventing ASLR – NOP sleds
- Circumventing ASLR – memory leakage
- Non-executable memory areas
  - The NX bit
  - Write XOR Execute (W^X)
  - NX on various platforms
  - 🔗 *Lab – Effects of NX*
  - NX circumvention – Code reuse attacks
    - Return-to-libc / arc injection
  - Return Oriented Programming (ROP)
    - Protection against ROP

## › Common software security weaknesses

### Security features

- Authentication
  - Authentication basics
  - Multi-factor authentication
  - Authentication weaknesses
- Password management
  - Inbound password management
    - Storing account passwords
    - Password in transit
    - 🔗 *Lab – Is just hashing passwords enough?*
    - [Dictionary attacks and brute forcing](#)
    - Salting
    - Adaptive hash functions for password storage
    - Password policy
    - [NIST authenticator requirements for memorized secrets](#)
      - 📖 *Case study – The Ashley Madison data breach*
      - 📖 *The dictionary attack*
      - 📖 *The ultimate crack*
      - 📖 *Exploitation and the lessons learned*
  - Password database migration

### Code quality

- Code quality and security
- Data handling
  - Type mismatch
  - 🔗 *Lab – Type mismatch*
  - Initialization and cleanup

- Constructors and destructors
- Initialization of static objects
- 🔗 *Lab – Initialization cycles*
- Unreleased resource
  - Array disposal in C++
  - 🔗 *Lab – Mixing delete and delete[]*
- Object oriented programming pitfalls
  - Accessibility modifiers
    - Are accessibility modifiers a security feature?
  - Inheritance and object slicing
  - Implementing the copy operator
  - The copy operator and mutability
  - Mutability
    - Mutable predicate function objects
    - 🔗 *Lab – Mutable predicate function object*

## Day 3

---

### › Common software security weaknesses

#### Input validation

- Input validation principles
- Denylists and allowlists
- What to validate – the attack surface
- Where to validate – defense in depth
- When to validate – validation vs transformations
- Validation with regex
- Injection
  - Injection principles
  - Injection attacks
  - Code injection
    - OS command injection
    - 🔗 *Lab – Command injection*
    - OS command injection best practices
    - Avoiding command injection with the right APIs
    - 🔗 *Lab – Command injection best practices*
      - 📖 *Case study – Shellshock*
    - 🔗 *Lab – Shellshock*
- Process control – library injection
  - Library hijacking

- 🔗 *Lab – Library hijacking*
- Integer handling problems
  - Representing signed numbers
  - Integer visualization
  - Integer promotion
  - Integer overflow
- 🔗 *Lab – Integer overflow*
  - Signed / unsigned confusion
- 📖 *Case study – The Stockholm Stock Exchange*
- 🔗 *Lab – Signed / unsigned confusion*
  - Integer truncation
- 🔗 *Lab – Integer truncation*
- 📖 *Case study – WannaCry*
  - Best practices
    - Upcasting
    - Precondition testing
    - Postcondition testing
    - Best practices in C++
- 🔗 *Lab – Integer handling best practices in C++*
- Files and streams
  - Path traversal
- 🔗 *Lab – Path traversal*
  - Path traversal-related examples
  - Path traversal best practices
- 🔗 *Lab – Path canonicalization*

## Errors

- Error and exception handling principles
- Error handling
  - Returning a misleading status code
  - Error handling in C++
  - Using `std::optional` safely
  - Information exposure through error reporting
- Exception handling
  - In the catch block. And now what?
  - Empty catch block
- 🔗 *Lab – Exception handling mess*

## > Wrap up

### Secure coding principles

- Principles of robust programming by Matt Bishop

- Secure design principles of Saltzer and Schroeder

### **And now what?**

- Software security sources and further reading
- C and C++ resources