Code responsibly with generative AI in C++

CYDCpp3dGenAI | 3 days | On-site or online | Hands-on

Generative AI is transforming the software industry, with tools like Claude Code, GitHub Copilot or others, enabling developers to achieve unprecedented levels of efficiency. While this is exciting progress, it also raises important concerns, encouraging stakeholders to approach these technologies with care. Current AI tools often lack the nuanced understanding necessary to address subtle, yet critical aspects of software development, particularly in the domain of security.

This course provides a comprehensive insight into the responsible use of generative AI in coding. Participants delve into topics in software development that are most likely to be impacted by careless use of generative AI, including authentication, authorization, and cryptography. The curriculum also includes an analysis of how Claude Code, GitHub Copilot or others handle secure coding practices related to key vulnerabilities outlined in the OWASP Top Ten, such as path traversal, SQL injection, or cross-site scripting.

Through hands-on learning and experimenting, participants will get a solid understanding of both the strengths and limitations of AI-assisted development. In addition, case studies of real-world incidents showcase the consequences of insecure code and demonstrate the dual nature of generative AI as both a resource and a potential risk.

By the end of the course, developers will be equipped with the knowledge and skills to integrate AI tools into the software development lifecycle responsibly, enhancing efficiency without compromising security or product quality.

Skills and drills

29 LABS

9 CASE STUDIES

Audience

C and C++ developers using GenAI tools

Group size

12 participants

Preparedness

General C++ and C development

Outline

- Coding responsibly with GenAI
- Memory management vulnerabilities
- Memory management hardening
- Common software security weaknesses
- Using vulnerable components
- Wrap up

Standards and references

SEI CERT, CWE and Fortify Taxonomy

What you'll have learned

- Understanding the essentials of responsible AI
- Getting familiar with essential cyber security concepts
- Correctly implementing various security features
- Identify vulnerabilities and their consequences
- Learn the security best practices in C++
- Managing vulnerabilities in third party components
- Input validation approaches and principles

Table of contents

Day 1

› Coding responsibly with GenAI

What is security?
Threat and risk
Cyber security threat types – the CIA triad
Cyber security threat types – the STRIDE model
Consequences of insecure software
What is responsible AI?
Security and responsible AI in software development

› 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 convention 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
Case study – Stack BOF in FriendlyName handling of the Wemo Smart Plug

- 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

- Using std::string in C++
- Unterminated strings
- readlink() and string termination
- Manipulating C-style strings in C++
- Malicious string termination

Lab – String termination confusion

- String length calculation mistakes

Day 2

› Memory management hardening

Securing the toolchain

- Securing the toolchain in 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
- 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
    - *Case study – Systematic exploitation of a MediaTek buffer overflow*

› Common software security weaknesses

Security features

- Authentication
- 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
  - 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
  - Inheritance and object slicing
  - Implementing the copy operator

- The copy operator and mutability
- Mutability
  - Mutable predicate function objects
  - *Lab – Mutable predicate function object*

› Using vulnerable components

Security of AI generated code

- Practical attacks against code generation tools
- Dependency hallucination via generative AI
- *Case study – A history of GitHub Copilot weaknesses (up to mid-2025)*
- *Case study – Agentic coding and code security (mid-2025 onward)*

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
- Injection
  - 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*
    - *Lab – Experimenting with command injection in GenAI*
    - *Case study – Command injection in Zyxel IKE packet decoder*
- Integer handling problems
  - Representing signed numbers
  - Integer visualization
  - Integer promotion
  - Integer overflow
  - *Lab – Integer overflow*
  - *Lab – Experimenting with integer overflow in GenAI*
  - *Case study – Integer underflows in IPv6 handling of tcpip.sys*

- Signed / unsigned confusion
- *Case study – Signed/unsigned confusion DoS in DrayTek Vigor routers*
- *Lab – Signed / unsigned confusion*
- *Lab – Experimenting with signed / unsigned confusion in GenAI*
- Integer truncation
- *Lab – Integer truncation*
- *Lab – Experimenting with integer truncation in GenAI*
- Best practices
  - Upcasting
  - Precondition testing
  - Postcondition testing
  - Using big integer libraries
  - Best practices in C
  - UBSan changes to arithmetics
  - *Lab – Handling integer overflow on the toolchain level in C++*
  - Best practices in C++
  - *Lab – Integer handling best practices in C++*
  - *Case study – Integer check failure in Skia*
- Files and streams
  - Path traversal
  - *Lab – Path traversal*
  - Path traversal-related examples
  - *Case study – File spoofing in WinRAR*
  - Virtual resources
  - Path traversal best practices
  - *Lab – Path canonicalization*
  - *Lab – Experimenting with path traversal in GenAI*
- Format string issues
  - The problem with printf()
  - *Lab – Exploiting format string*

› 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
- Generative AI – Resources and additional guidance