CSP103 - SECURE SOFTWARE DESIGN

Course Learning Objectives

In this course, we'll examine how to design software securely from the ground up, integrating core principles of secure software architecture throughout the development lifecycle. Key areas include leveraging principles like least privilege, modular programming, and separation of duties to build resilient systems, establishing security layers (defense in depth), and implementing secure failover mechanisms. We'll explore threat modeling, attack surface analysis, and strategies to manage risks. Additional topics include securing data through proper handling, cryptography, privacy techniques, access controls, and designing for confidentiality, integrity, and availability. We'll also cover cloud, container, and virtual environments and review security standards (NIST, OWASP, ISO/IEC 27001, PCI DSS) as frameworks for a robust security strategy.

Description

Secure Software Design was made for Developers and Software Architects interested in learning about the foundational and advanced practices for building secure systems as part of their CSSLP certification. It is recommended that you complete AppSec Fundamentals and Secure Software Requirements before taking this course.

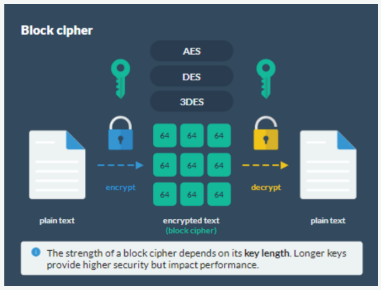
Audience

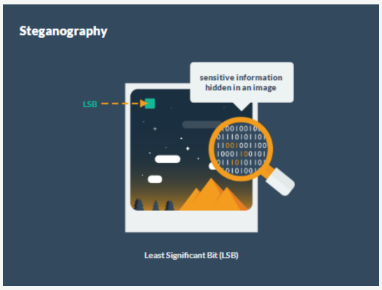
Developers

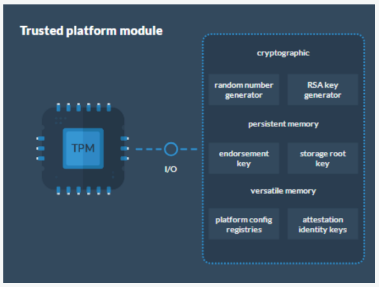
Architects

Time Required

Tailored learning - 115 minutes total (approx.)







CSP103 - SECURE SOFTWARE DESIGN

Course Outline

1. Security Design Principles

- About
- Least privilege
- Modular programming
- Benefits to modular programming
- Separation of duties
- Defense in depth
- Fail secure
- Generic errors
- Economy of mechanisms
- Complete mediation
- Open design
- Least common mechanism
- Psychological acceptability
- Leverage existing components
- Pervasive computing
- Security considerations for pervasive computing

2. The Design Process

- Threat modeling
- Importance of threat modeling
- What can be threat modeled
- What we will threat model
- Threat modeling overview
- STRIDE categories
- Attack surface
- Defining the attack surface
- Identifying and mapping the attack surface
- Measuring and assessing the attack surface
- Managing the attack surface
- Comparison between threat modeling and attack surface
- Review
- Data security and privacy
- Secure data handling
- Communication protocols
- Content delivery network
- Cloud environment
- Server resources
- Payment processing

3. Design Considerations

- Confidentiality design
- Overt cryptography
- Symmetric key encryption
- Common algorithms
- Block cipher
- Stream cipher
- Asymmetric key encryption
- Hash functions
- Covert cryptography
- Covert cryptography uses
- Steganography
- Traffic padding
- Integrity design
- Input validation
- Syntax validity
- Semantic validity
- Client-side and server-side validation
- File upload validation
- Data validation
- Access controls
- Data consistency mechanisms
- Audit trail
- Availability design
- Redundancy
- Failover mechanisms
- Data replication
- Data backup
- Disaster recovery planning
- Scalability
- Vertical scaling
- Horizontal scaling
- Health monitoring
- Security standards
- NIST Cybersecurity Framework
- OWASP
- ISO/IEC 27001
- PCI DSS
- Security strategy

SecurityCompass

CSP103 - SECURE SOFTWARE DESIGN

Course Outline

4. Securing Common Technologies

- Server virtualization
- Hypervisors
- Application containers
- VMs vs containers
- Newsflash: MITRE breach
- Security concerns
- Hypervisor vulnerabilities
- VM image integrity
- VM escape
- Misconfigured security settings
- Network security risks
- DoS and DDoS
- Container breakout
- Weak or outdated container dependencies
- Container security
- Develop stage
- Deploy stage
- Run stage
- Components of container runtime policies
- The Trusted Computing Base
- TCB system security
- Hardware security
- Operating system security
- Security policies and procedures
- Cryptographic techniques
- Network security
- Trusted platform module
- Secure boot, attestation, and platform integrity verification
- Hardware based security
- Secure cryptographic key storage
- Enhanced authentication
- Data protection
- Protection against firmware attacks
- Databases
- Inference attacks
- Polyinstantiation
- Normalization
- Views for databases

SecurityCompass