Paul Romer

CSD370

Module 4.2 Assignment

Secure Design Principles

Requirements: There are many sets of secure design principles available to you. In addition to your text, find at least two (2) other sets of principles. What is common to all sets? What only appears in one set? After reading through all three, come up with your own list of what you consider to be key principles. At the end of the list, explain why you chose the items you did. Make sure you include a list of resources used.

Common Principles Across All 3 Resources

1. **Least Privilege**

- Chapter 8: Designing systems so components and users have only the permissions necessary, reducing risk from exploited vulnerabilities.
- Secure Development and Deployment Guidance: Securing environments and repositories with access controls.
- 7 Principles: Limit access for users and system components to strictly what is necessary.

2. **Separation of Duties**

- Chapter 8: Designing systems to preventing misuse by a single entity.
- Secure Development and Deployment Guidance: Part of team collaboration and review processes, ensuring no single individual controls all aspects.
- 7 Principles: Dividing tasks and privileges to minimize risks of errors or malicious actions.

3. **Authorized Access**

- Chapter 8: Every access to sensitive operations be authorized each time, avoiding assumptions about prior checks.
- Secure Development and Deployment Guidance: Ensure authorized access to resources.
- 7 Principles: Every resource access request to be authenticated and authorized consistently.

4. **Fail Safe**

- Chapter 8: Systems should fail to a safe state, maintaining security during failures.
- Secure Development and Deployment Guidance: Focuses on planning for security flaws, ensuring systems handle issues without compromising security.

- 7 Principles: Systems should default to a secure state during errors, avoiding exposure of sensitive information.

5. **Security Culture and Knowledge**

- Chapter 8: Encourages learning from past mistakes and integrating security into the development lifecycle.
- Secure Development and Deployment Guidance: "Secure development is everyone's concern" Emphasizes keeping security knowledge sharp.
- 7 Principles: Rooted in DevSecOps, focuses on fostering a culture of security awareness across teams.

6. **Protecting the Development and Deployment Environment**

- Chapter 8: Includes securing configuration parameters and memory management, which tie to environment security.
- Secure Development and Deployment Guidance: Focuses on securing the development environment, code repository, and CI/CD pipeline.
- 7 Principles: Security as code and minimizing attack surfaces.

Unique Principles Across All 3 Resources

Unique to Chapter 8

- Declarative vs Imperative Security: Security defined in containers (declarative) vs embedded in the code (imperative).
- Cryptographic Agility: The ability to update cryptographic functions when needed.
- Memory Management and Type Safety: Focus on secure memory allocation and preventing type-errors.
- Least Common Mechanism: Avoids shared mechanisms that could create unintended information pathways.

Unique to Secure Development and Deployment Guidance

- Clean and Maintainable Code: Focus on code quality and simplicity to reduce errors that come from complexity.
- Planning for Security Flaws: Have a plan for inevitable bugs and vulnerabilities.

Unique to 7 Principles of Secure Design in Software Development

- Security as Code: Automate security as part of CI/CD.
- Secure Defaults: Ensure defaults are secure.
- Minimize Attack Surface: Limit unnecessary features and services.

My Key Principles

- Integrate security throughout the SDLC
- Implement access control
- Culture of security
- Reduce exposure

These principles provide a base culture of security through automation while limiting the attack surface of software. They are a mix of cultural and technical principles that together ensure secure software is a focus of the organization.

Sources

Secure Coding Practices Chapter 8

https://www.ncsc.gov.uk/collection/developers-collection

https://www.jit.io/resources/app-security/secure-design-principles