**Secure Design Principles**

Liz Hinz

CSD370-A339: Secure Software Development

Module 4.2 Assignment

Professor Nathan Braun

April 13, 2025

CSSLP Certified Secure Software Lifecycle Professional All-in-One Exam Guide, Third Edition Secure Design Principles (Conklin & Shoemaker, 2022):

* Good Enough Security
* Least Privilege
* Separation of Duties
* Defense in Depth
* Fail Safe
* Economy of Mechanism
* Complete Mediation
* Open Design
* Least Common Mechanism
* Psychological Acceptability
* Weakest Link
* Leverage Existing Components
* Single Point of Failure

OWASP – Principles of Security (OWASP, n.d.):

* Security by Design
* Security by Default
* No Security Guarantee
* Defense in Depth
* Fail Safe
* Least Privilege
* Compartmentalize
* Separation of Duties
* Complete Mediation
* Open Design
* Least Common Mechanism
* Psychological acceptability
* Usability & Manageability
* Secure the Weakest Link
* Leveraging Existing Components

7 Principles of Secure Design in Software Development (Biam, 2024):

* Security as Code
* Secure Defaults
* Least Privilege
* Separation of Duties
* Minimize Attack Surface Area
* Complete Mediation
* Failing Securely

Common in all Sets:

* Least Privilege
* Separation of Duties
* Fail Safe/Failing Securely
* Complete Mediation
* Leverage Existing Components/Minimize Attack Surface Area
* No Security Guarantee

Only appears once:

* Good Enough Security
* Security as Code
* Economy of Mechanism
* Single Point of Failure
* Security by Design
* Compartmentalize
* Usability & Manageability

My Secure Design Principles

* Least Privilege
* Separation of Duties
* Fail Safe/Failing Securely
* Complete Mediation
* Leverage Existing Components/Minimize Attack Surface Area
* No Security Guarantee
* Weakest Link
  + The main reason I included the first six entries in my list is that they were mentioned on all three referenced lists. Considering that three sources mentioned the same six secure design principles, they seem vital to include on my key principles list. They also cover ideas we have previously learned throughout our cohort. I also included weakest link since proper security relies on even the weakest components to be secure against attackers.

**References**

Biam, L. (2024, June 11). *7 Principles of Secure Design in Software Development*. Jit. https://www.jit.io/resources/app-security/secure-design-principles

Conklin, WM. A., & Shoemaker, D. P. (2022). *CSSLP Certified Secure Software Lifecycle Professional: Exam Guide.* McGraw-Hill Education.

OWASP. (n.d.). *OWASP Developer Guide | Principles of Security | OWASP Foundation*. Owasp.org. Retrieved April 8, 2025, from https://owasp.org/www-project-developer-guide/draft/foundations/security\_principles/