**Julio Pochet**  
**CSD370 – Module 4.2 Assignment: Secure Design Principles**

**🔐 Secure Design Principles – My Summary**

For this assignment, I reviewed secure design principles from three different sources:

1. **Textbook (CISSP Official Study Guide, Chapter 8)**
2. **OWASP Secure Design Principles**
3. **Saltzer & Schroeder’s 1975 Security Design Principles**

**✅ What All Three Sets Have in Common**

The following principles appear in all three sets:

* **Least Privilege** – Only give users or programs access to what they really need.
* **Fail-Safe Defaults** – Deny access unless it is clearly allowed.
* **Defense in Depth** – Use layers of protection, not just one.
* **Keep It Simple (Economy of Mechanism)** – Simple systems are easier to secure.
* **Usability (Psychological Acceptability)** – Security should be easy for users to follow.

**🔎 What Only Appears in One Set**

* **OWASP Only**: Secure by Default, Secure Deployment
* **Textbook Only**: Least Common Mechanism, Separation of Duties
* **Saltzer & Schroeder Only**: Separation of Privilege

Each source focuses slightly differently depending on the system or use case (enterprise, web app, theory).

**🧠 My Top 7 Secure Design Principles**

1. **Least Privilege**
2. **Fail-Safe Defaults**
3. **Defense in Depth**
4. **Secure by Default**
5. **Separation of Duties**
6. **Complete Mediation**
7. **Usability**

**💬 Why I Chose These**

These seven principles cover both the **technical** and **human** sides of security. Least privilege, separation of duties, and complete mediation protect against abuse and mistakes. Secure-by-default makes sure systems are safe without extra setup. Usability matters because if people find security too hard, they’ll find ways around it. All these together create a strong, simple, and realistic foundation for secure design in any system.

**📚 References**

* ISC². (2021). *CISSP Official Study Guide*, Chapter 8.
* OWASP. (n.d.). *Secure Design Principles*. <https://owasp.org/www-project-top-ten/>
* Saltzer, J. H., & Schroeder, M. D. (1975). *The Protection of Information in Computer Systems*. <https://www.cs.virginia.edu/~evans/cs551/saltzer/>