Principles of Cybersecurity Reference Guide

Ryan Coon

CYB-515

Dr. Edward Marchewka

October 16, 2024

|  |  |  |
| --- | --- | --- |
| Principle | Definition | Why the Principle is Important |
| Separation (of domains/duties) | Separation of duties, also known as segregation of duties, is a fundamental principle in cybersecurity. It's based on the idea that no single person should have enough authority to compromise the system on their own(Editor, 2022). | Separation of duties acts as a strong defense against various security threats by minimizing the potential for malicious activity, human error, and insider threats. |
| Isolation | Isolation in cybersecurity is a technique used to restrict potentially harmful code or software in a secure environment. It's also known as sandboxing. This technique helps to prevent malicious code from affecting other parts of a system or network(What is Isolation?, n.d.). | Isolation helps to protect sensitive information and data stored within the network. |
| Encapsulation | Encapsulation is a technique that involves hiding and protecting sensitive data and functions within a secure container(Encapsulation Vulnerabilities, n.d.). | Encapsulation plays a vital role in bolstering cybersecurity by minimizing vulnerabilities, safeguarding data integrity, and streamlining security management. |
| Modularity | Modularity refers to the design of systems and software in separate, interchangeable components. This makes it easier to update and maintain the system, as changes can be made to individual modules without affecting the entire system(Institute of Data, 2024). | Modularity in cybersecurity promotes a more secure, maintainable, and resilient system. |
| Simplicity of Design (Economy of Mechanism) | Is a fundamental principle that emphasizes keeping security mechanisms as straightforward and minimal as possible(D, 2023). | Simplicity of Design promotes a more secure, maintainable, and user-friendly system by minimizing complexity, reducing vulnerabilities, and facilitating effective security management. |
| Minimization of implementation (Least Common Mechanism) | Least Common Mechanism aims to reduce the amount of shared resources and mechanisms used by multiple users(Design Principles, n.d.). | Least Common Mechanism promotes a more secure system by reducing the likelihood of successful attacks, limiting the impact of breaches, and making security management more efficient. |
| Open Design | A  principle that states that the security of a system should not rely on the secrecy of its design or implementation(OWASP Developer Guide, n.d.). | Is an important principle because it promotes transparency and independent review of a system's security. |
| Complete Mediation | Ensures every access request to a system's resources is checked and verified against the security policy before being granted(Secure Design Principles, 2021). | Acts as a strong barrier against unauthorized access, ensuring that only authorized individuals can interact with sensitive data and resources. |
| Layering (Defense in Depth) | Is a strategy that uses multiple layers of security controls to protect a network from attack(Fruhlinger, 2022). | Layering is a proactive approach to security that creates a robust defense against a wide range of threats |
| Least Privilege | Granting the least amount of privilege possible, or access to the minimum resources required, preventing unauthorized access and limiting the potential damage if a security breach occurs(NSIT, n.d.). | Is a proactive approach to security that minimizes the risk of attacks and limits the damage if an attack does occur. |
| Fail-Safe Defaults (Open/Secure) | Operates on a simple yet powerful premise: unless a user is explicitly granted permission, access should be denied by default(D, 2024). | Promote a proactive security approach that minimizes risk and strengthens security posture. |
| Least Astonishment (Psychological Acceptability) | Emphasizes on designing security mechanisms in a way that users understand and expect(Tejas, 2024). | Promotes a user-centric approach to security, recognizing that users are an integral part of the security equation. |
| Minimize Trust Surface (Reluctance to Trust) | Principle that aims to reduce the number of potential entry points for attackers(Effective Strategies to Minimize Trust Surface in Cybersecurity, 2024). | A proactive approach to security that reduces risk and helps ensure the safety of your systems and data. |
| Usability | Refers to how easy and user-friendly security measures are for people to use(CSRC Content, n.d.). | It is about making security measures user-friendly so that people are more likely to use them effectively, ultimately leading to a stronger security posture. |
| Trust Relationships | Is a connection established between two entities, enabling secure communication and information sharing(What Does Trust Relationship Mean?, 2024). | They help to maintain a strong security posture while enabling seamless collaboration and information sharing between different entities |

References:

D, M. (2023, September 29). *The Power of Simplicity in Ensuring Robust Security*. Www.linkedin.com. https://www.linkedin.com/pulse/power-simplicity-ensuring-robust-security-marc-degli

D, M. (2024, April 3). *Fail-Safe Defaults*. Linkedin.com. https://www.linkedin.com/pulse/understanding-principle-fail-safe-defaults-marc-degli-xgxcc

Design Principles. (n.d.). In *Clemson University*. https://www.cs.clemson.edu/course/cpsc420/material/Design%20Principles/Design%20Principles.pdf

Editor, C. C. (n.d.). *Usability - Glossary | CSRC*. Csrc.nist.gov. https://csrc.nist.gov/glossary/term/usability

Editor, C. C. (2022). *Separation of Duty (SOD) - Glossary | CSRC*. Csrc.nist.gov. https://csrc.nist.gov/glossary/term/separation\_of\_duty

*Effective Strategies to Minimize Trust Surface in Cybersecurity: A Comprehensive Guide | SubRosa*. (2024). Subrosacyber.com. https://subrosacyber.com/en/blog/minimize-trust-surface

*Encapsulation Vulnerabilities*. (n.d.). Veracode. https://www.veracode.com/security/encapsulation-vulnerabilities

Fruhlinger, J. (2022, July 28). *Defense in depth explained: Layering tools and processes for better security*. CSO Online. https://www.csoonline.com/article/573221/defense-in-depth-explained-layering-tools-and-processes-for-better-security.html

National Institute of Standards and Technology. (n.d.). *least privilege - Glossary | CSRC*. Csrc.nist.gov. https://csrc.nist.gov/glossary/term/least\_privilege

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

*Secure design principles*. (2021, November 15). Cydrill Software Security. https://cydrill.com/cyber-security/secure-design-principles/#

Tejas Kotian. (2024, February 4). *The Principle of Least Astonishment (POLA*. Linkedin.com. https://www.linkedin.com/pulse/principle-least-astonishment-pola-tejas-kotian-byfee

*What Does Trust Relationship Mean?* (2024). Bizmanualz. https://www.bizmanualz.com/library/what-does-trust-relationship-mean?srsltid=AfmBOop2osKJZ10cxCuaCj6VoeoZIidOGDM2Mf041GyJ-kRD7p4B3qGz

*What is Isolation? Barriers for Safe Cyber Systems against Malicious Threats*. (n.d.). Cyberpedia.reasonlabs.com. https://cyberpedia.reasonlabs.com/EN/isolation.html

*What is Modularity in Software Engineering | Institute of Data*. (2024, February 23). Institute of Data. https://www.institutedata.com/us/blog/modularity-in-software-engineering/