Southern New Hampshire University

CYB 300 Milestone Three Worksheet

I. Security Analysis Table

Security Analysis Table		
Fundamental Security Design Principles	Describe how the FSDPs relate to PKI (2–3 sentences)	Describe how the FSDPs relate to the CIA triad (2–3 sentences)
Isolation	Isolation in PKI ensures that the key management processes are segregated to prevent unauthorized access. This isolation protects the keys from external threats and accidental exposure.	Isolation helps maintain confidentiality and integrity by limiting access to sensitive data and systems only to authorized entities, which minimizes the risk of data breaches.
Modularity	Modularity in PKI allows different cryptographic functions to be independently managed and updated without affecting the entire system, enhancing adaptability and maintainability.	Modularity supports availability by ensuring that the failure of one module does not compromise the security or functionality of the entire system.
Minimization of Implementation	Minimizing the complexity of PKI systems helps reduce potential vulnerabilities and the likelihood of security gaps, making the systems more secure and easier to manage.	A simpler design improves reliability and maintainability, thereby supporting the integrity and availability of the system.
Layering	Layering in PKI involves multiple levels of security controls to protect the keys and certificates, such as using both physical and cryptographic protections.	Layering enhances all aspects of the CIA triad by providing redundant security measures, which help prevent data breaches and ensure system resilience.

Least Privilege	Implementing least privilege in PKI restricts access rights for users, accounts, and computing processes to only those resources necessary for legitimate activities, minimizing potential misuse.	This principle directly supports integrity and confidentiality by limiting access to data and resources to authorized users only.
Fail-Safe Defaults/Fail Secure	Fail-safe defaults in PKI ensure that if a component fails, it does so in a secure state where no sensitive data is exposed.	Fail-safe mechanisms protect data integrity and availability by ensuring that systems revert to a secure state in the event of a malfunction.
Trust Relations	Trust relations in PKI manage how trust is established between entities, ensuring that only trusted certificates and keys are used within an organization.	Strong trust relationships support all three pillars of the CIA triad by ensuring that data interactions and transactions are secure and reliable.

II. Scenario-Based Short Response Questions

A. **Temporary Contractor**: The use of CAs as part of PKI provides a mechanism for key management and secure communications. If you were asked to provide access to information systems to a temporary contractor, what areas of a PKI and CIA triad would you be concerned with? Which of the FSDPs most applies here?

When providing access to information systems to a temporary contractor, it is essential to consider both the Public Key Infrastructure (PKI) and elements of the CIA triad—confidentiality, integrity, and availability. In PKI, the primary concern is ensuring that the contractor's digital credentials, which include certificates issued by a Certificate Authority (CA), are secure and properly managed. These certificates authenticate the contractor's identity and authorize access to specific systems or data. From the perspective of the CIA triad, data integrity is critical, as any unauthorized changes could lead to misinformation or corrupt practices. To maintain confidentiality, we must ensure that we do not disclose sensitive information to unauthorized individuals. The 'Least Privilege' principle is highly applicable in this situation, as it limits the contractor's access to only those resources vital for their task. This approach minimizes potential risks, such as accidental data exposure or intentional data breaches. Implementing such measures helps maintain a secure and controlled environment, which is crucial when involving external parties in internal systems.

B. **Cryptography**: As part of PKI, a cryptographic system is established. Explain how cryptography is used and what forms of implementation can be accomplished.

Cryptography is a fundamental component of Public Key Infrastructure (PKI) and vital in securing organizational communications. It involves using algorithms to encrypt and decrypt data, ensuring that sensitive information remains confidential and is only accessible to intended recipients. In PKI, cryptography helps create secure connections between users and systems by encrypting data transferred over these connections, making it unreadable to anyone who might intercept it. This includes SSL/TLS for securing websites and PGP for email encryption. Cryptography implementation can vary based on the organization's specific needs, such as the data sensitivity or the required level of security. For instance, more robust encryption methods may be necessary for highly confidential data to prevent advanced cyber threats. By utilizing cryptography effectively, organizations can protect the integrity and confidentiality of data, ensuring that it is accurate and secure from unauthorized changes or disclosures. The strategic application of cryptographic techniques is crucial for maintaining the trustworthiness and security of organizational communications and data storage.