Selvadurai Pathmathasan

CS 305 Module Four Written Assignment

Southern New Hampshire University

Professor: Nickloas Woodlock

As user perspectives, user need to consider defending against various types of security attacks user should use strong passwords, enabling multifactor authentication, integrate antivirus software, firewalls, regularly update latest version of its

software updates, avoiding clicking any suspicious websites harm the pc will prevent security risks.

As a developer all the security protections measures should be integrated in early stages of the development. Secure software development best practices are necessary because security risks in financial sectors is very high, adding many layers of security frameworks will prevent hacking, data breaches, these are most companies best adopted by developers must adhere to secure coding practices, such as input validation, secure data storage, and secure communication protocols. Secure coding practices help to prevent common security vulnerabilities such as SQL injection, cross-site scripting, and buffer overflow attacks.

The Spring Boot Framework itself is a great choice it’s a huge framework. It’s having a wide range of modules and frameworks that allow to create a resilient project with APIs and Spring Boot framework dependency injection with code reviews. Spring core, spring web, spring security, spring rest—all these great fits for enterprise applications

**Risk recommendations** will be immense if proper software development methodology not implemented like low code reviews and Code issues Low-quality code can be a major risk and can be caused by hasty work. Bugs and logical errors can be reduced by testing code and fixing issues as they arise. Also, if company may not fully understand or be able to accurately predict certain technical aspects of a new product development project

**Gramm-Leach-Bliley Act** This federal law protects consumer financial privacy by requiring financial institutions to safeguard consumer data and explain their information security practices, Fair Credit Reporting Act (FCRA): This is another relevant regulation for fintech developers. Safeguards Rule: This rule is a subset of the GLBA and outlines how non-bank financial institutions should protect customer data. The updated rule requires multi-factor authentication for all individuals accessing an information system.

Algorithm chipper concept description there are two types of symmetric encryption algorithms:

**Block algorithms**. Set lengths of bits are encrypted in blocks of electronic data with the use of a specific secret key. As the data is being encrypted, the system holds the data in its memory as it waits for complete blocks.

**Stream algorithms.** Data is encrypted as it streams instead of being retained in the system’s memory.

Some examples of symmetric encryption algorithms include (Advanced Encryption Standard) DES (Data Encryption Standard) IDEA (International Data Encryption Algorithm Blowfish (Drop-in replacement for DES or IDEA)

**Threat Modeling for Secure Software Development**

Threat modeling involves analyzing the software architecture and identifying potential security threats and vulnerabilities. This helps in designing the software with security in mind and implementing the necessary security controls.

**Testing** Regular security testing, including penetration testing and vulnerability scanning, can help identify potential security weaknesses in the software. This helps in fixing security issues before the software is deployed.

**Access Control** Access control ensures that only authorized personnel can access the software system. This includes implementing user authentication and authorization mechanisms, as well as role-based access control.

**Security Training** Developers and other personnel involved in the software development process should receive regular security training to ensure that they understand the importance of security and the best practices for secure software development.

Algorithm cipher will be used Cipher algorithms, such as encryption and decryption algorithms, are used in banking applications development to protect sensitive information and secure network communications: PGP A standard set of algorithms that provide cryptographic privacy and authentication. PGP can encrypt and decrypt payloads with multiple keys, and verify payloads with multiple signatures

Best chippers are Triple DES, Triple DES was designed to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the industry's recommended standard and the most widely used symmetric algorithm.

AES The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the U.S. Government and numerous organizations and is also found in Arcserve Unified Data Protection (UDP) software. Although it is highly efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy-duty encryption purposes.

Encryption at the Database Level Almost all commercial databases now support sometime of encryption in the database itself. Encryption at the database layer provides some distinct advantages: Encryption is optimized for database performance Encryption services are better integrated with other database access control services resulting in fewer security gaps.

Key reasons to not use the most secure cipher are it might cause loading slow web, mobile apps Performance impact: Highly secure ciphers can sometimes be computationally expensive, leading to noticeable slowdowns in applications, especially on resource-constrained devices or when dealing with large data sets.

Key management complexity: Managing secure keys for strong ciphers can be challenging, requiring robust key distribution and rotation mechanisms, which can add complexity to the development process.

Compatibility issues: Older systems or legacy applications may not support the latest and most secure ciphers, forcing developers to use less secure options for compatibility reasons.

purpose of the cipher's hash functions and bit levels,

In software development, a cipher's hash function is primarily used to ensure data integrity by generating a unique, fixed-length string (hash) that represents the original data, allowing verification if the data has been tampered with without needing to compare the entire data set

Bit Level and Security:

Higher Bit Level: Provides a stronger hash, making it harder to find collisions (where two different data sets produce the same hash).

Lower Bit Level: Offers weaker security, making it easier to find collisions, but may be suitable for applications where high security is not critical.

Common cryptographic hash functions used in software development:

SHA-256: Widely used, considered very secure with a 256-bit hash

MD5: Older, less secure, but still used in some applications

SHA-3: Newer standard with improved resistance to potential attacks

A diagram of a computer system

Description automatically generated

A diagram of a diagram

Description automatically generated

In cryptography, "random numbers" are used to generate unpredictable values that are crucial for secure key generation and encryption processes, while "symmetric keys" use the same key for both encryption and decryption, whereas "asymmetric keys" use a pair of different keys, one public and one private, for encryption and decryption respectively; essentially, symmetric encryption is faster but requires secure key exchange, while asymmetric encryption is slower but offers better key management for secure communication with unknown parties.

History of Describe the history and current state of encryption algorithms.

A diagram of a key to a cryptography

Description automatically generated

References

<https://www.newsoftwares.net/blog/how-do-banks-encrypt-data/>

<https://www.arcserve.com/blog/5-common-encryption-algorithms-and-unbreakables-future>

https://medium.com/@dfs.techblog/end-to-end-encryption

<https://www.perforce.com/blog/sca/best-practices-secure-software-development>

<https://convesio.com/knowledgebase/article/the-dangers-of-weak-cipher-suites-what-you-need-to-know/>