CS-305 4-2 Written Assignment: Algorithm Ciphers

Jerimey Burnside

09/28/2024

Artemis Financial,

Best Practices in Security Protection: Considering security protection best practices, there are brute force attacks, cryptanalysis attacks, and side-channel attacks that an organization needs to guard against. In counter risks, the following are the best practices to be done:

Strong Encryption Algorithms: By using properly established and vetted encryption algorithms.

Key Management: Strong key management practice should be used through generating, storing, distributing, and rotating keys.

Regular Updates: Recommend updating cryptographic libraries and software periodically to be safe from recently identified flaws.

MFA: Enforce MFA in order to introduce another layer of security.

Access Controls: Implement access controls to make sure that only a limited group has access to encrypted data.

Risks of Recommendation: Following are the major risks of the recommended encryption algorithm:

Implementation Flaws: The implementation by wrong methods may lead to loopholes.

Key Management Failures: Poor key management may lead to unauthorized access.

Performance Overhead: The strong encryption algorithms have some performance overhead. Government Regulations: There exist several government regulations that are to be taken care of, namely:

General Data Protection Regulation, GDPR: Accordingly, the law requires appropriate protection of personal data of all EU citizens.

Health Insurance Portability and Accountability Act: In the U.S., this act is required for the protection of health information.

Federal Information Processing Standards: Standards about cryptographic modules deployed by federal agencies in the U.S.

The algorithms that meet the requirements of FIPS 140-2 will be used for encryption, and all the other protection measures regarding data will be designed in compliance with regulations.

Cipher Algorithm Usage: The algorithm cipher selected shall be utilized in encrypting long-term archive files. This shall include large volumes of sensitive financial data requiring secure, extended-term storage.

Best Cipher Recommendation: Artemis Financial would be best suited with the Advanced Encryption Standard with a 256-bit key length. It is widely recognized to be quite robust and efficient. It has been adopted by the U.S. government for use in securing sensitive data, and generally finds widespread use all over the world.

Reasons Not to Choose the Most Secure Cipher: Inasmuch as AES-256 is very secure, there may be a number of reasons in given situations for considering ciphers that are less secure, including, among others:

Performance Consideration: There are cases when less secure ciphers offer better performance due to lesser computational overhead.

Compatibility Issues: The older systems or applications may not support newer or more secure ciphers.

However, taking into consideration that financial data is sensitive, security should be of higher importance than performance or compatibility issues.