Data Security Considerations

Selecting the Correct Cipher

Prepared By: Glenn Lehman

This document was prepared for CS-305-T2813 Software Security 22EW2 offered at SNHU and provides no warranty that it meets all security requirements of any specific real world application.

The selection of the optimal cipher algorithm for use by Artemis Financial to encrypt its long-term archive files requires the consideration of a few factors. This document briefly discusses government requirements, encryption methods, and cost considerations. It is not the intent to explain the mathematical complexity of encryption methods. Instead, this document provides a justified recommendation for the best-fit cipher algorithm.

First is the consideration of government requirements on the financial industry. The Federal Trade Commission Act protects the consumer from "deceptive practices," which include failure to "provide adequate security of personal information" (Group, 2022). The Gramm-Leach-Bliley Act was enacted on November 12, 1999, to formalize the authority of government agencies, including the FTC (Staff & Staff, 2022). These guidelines have been updated numerous times since 1999 but continue to have a common theme. That theme requires Artemis Financial to safeguard sensitive data (Staff & Staff, 2022). This solution requires selecting the correct cipher algorithm and ensuring all documentation withstands a government audit.

The risks to the data must be considered first to select the correct algorithm. These risks fit into a few broad categories, including unauthorized disclosure, deletion, or modification. Also, risks exist in the broad category of denial of service that would prevent access to archived information. Many of these risks are mitigated as part of the network design, user authentication, and the implementation of role-based security. For the remained of this document, only unauthorized disclosure will be considered. Specifically, the recommendation of an encryption method to protect the data should network access control, discussed in other proposals, fail.

Encryption is the best way to ensure that information, even if it gets outside the company's control. Encryption is the technical process of how data is converted using a cipher. Within the encryption process, a hash function mathematical maps data (the original message) to a bit array of fixed size (Speirs). The hash function utilizes a random seed to improve the generations of keys. Keys can be symmetric, where you need the same key to encrypt and decrypt, or asymmetric, where you need a combination of a private and public key. One last general category is how the cipher is applied. A cipher can be applied to a block of text or as a stream. Stream function like a one-time pad and are used on data where security is highly critical (Keyfactors, 2021).

Enough about encryption. Now we will examine how a selected cipher will be used when Artemis archives data. The process to store the information should take the clear message, apply a cipher and then store the document in the archive repository. Encryption should occur on the client side to prevent unencrypted data transfer over the intranet should a cloud-based storage system be implemented. When an authorized user retrieves a document, the information should be decrypted on the client side for the same reasons. The control of the key is a critical part of this process.

With key control, symmetric keys are most frequently used for bulk data transfer. Interestingly, asymmetric keys are used to securely exchange symmetric keys (Keyfactors, 2021). This fact highlights the importance of key protection in a symmetric encryption system.

So, given all these factors, what is the best choice for Artemis Financial to use as a cipher?

The Advanced Encryption Standard (AES) is recommended to be utilized with a key size of 256. Modern computer processors have an instruction set built into the processor (Gueron, 2010). This fact increases the encryption speed. In conjunction with this, the Transportation Layer Security should be utilized for end-to-end data transfer. In closing, AES was developed after Data Encryption Standard (DES) failed and has been the industry standard since around 2000.

Finally, even with the implementation of AES over TPS, the following general practices should be adopted.

1. A written policy is developed and reviewed by corporate legal.
2. Encryption libraries must be monitored for vulnerabilities on an ongoing basis.
3. Review computer hardware developments because quantum computing will make AES obsolete.

References

Group, G. L. (2022). *Data Protection Laws and Regulations Report 2022 USA*. International Comparative Legal Guides International Business Reports. Retrieved November 19, 2022, from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Gueron, S. (2010, May). White Paper Intel Advanced. Retrieved November 19, 2022, from https://www.intel.com/content/dam/doc/white-paper/advanced-encryption-standard-new-instructions-set-paper.pdf

Keyfactor. (2021, August 5). Types of encryption algorithms + pros and cons for each. Keyfactor. Retrieved November 19, 2022, from https://www.keyfactor.com/resources/types-of-encryption-algorithmns/

Speirs, W. R. (n.d.). Cryptographic hash functions - Purdue University. Retrieved November 19, 2022, from https://www.cs.purdue.edu/homes/ssw/cs355/hash.pdf

Staff, the P. N. O.; Staff, D. P. I. P. and C. T. O. (2022, February 11). Gramm-Leach-Bliley Act. Federal Trade Commission. Retrieved November 19, 2022, from https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

Staff, the P. N. O.; Staff, D. P. I. P. and C. T. O. (2022, September 13). How to comply with the privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act. Federal Trade Commission. Retrieved November 19, 2022, from https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act