Kevin Bagayas

7/28/2024

CS305 – Module 4 Assignment

In considering security protection best practices in terms of Artemis Financial requirements, it is important to keep in mind the importance of data security and always put in practice utilizing latest security updates and technologies. These are important considering they are dealing with sensitive client information and their financials. They would need a robust system and also to properly encrypt and store long-term archive files.

I would recommend the Advanced Encryption Standard (AES) as an encryption algorithm cipher for its long-term file archiving based on the list of Java Security Standard Cipher. It is the commonly used algorithm to encrypt and decrypt protected data. It uses 128-, 192- and 256-bit level security which it makes more secured.

The risks involved with my recommendation would be that the security environment tends to evolve with constant threats every year. An example would be a supercomputer deciphering it making it obsolete. Another risk would be using the different bit levels not considering the storage and making the system slower.

In terms of government regulation, the AES is generally accepted and set initially as a standard in terms of encryption of electronic data by U.S National of Standards and Technology. This algorithm cipher will be used to encrypt Artemis Financials’ long term archive files. In terms of the banking and financial sector, they would be using the 256-bit AES encryption to protect digital files and transactions. This makes AES ideal for these kind of processes/transactions because of its multiple rounds of encryption making it harder to break or hacked. The only disadvantage that I would not choose AES is when used with low-end devices it tends to be slow.

The use of hash functions in AES is wherein it takes a variable bit string as input and outputs a fixed-length string. According to (Jena, 2024), the AES is a symmetric block cipher algorithm with a block/chunk size of 128 bits. Converting these individual blocks and join them together once encrypted to form the ciphertext.

The use of “symmetric encryption uses the same key for both encryption and decryption, while asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption” (*Poggi,2021*).

The constant evolution of encryption in today’s digital world, greatly affected the importance of security and privacy. The AES or even the other encryption systems are deemed sophisticated back then but the constant threats of today’s security may pave for more advanced encryption systems that would be unbreakable and more secure.

Sources:

*Types of Encryption: Symmetric or Asymmetric? RSA or AES? | Prey Blog*. (2021, June 15). Preyproject.com. <https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes#:~:text=Symmetric%20vs%20Asymmetric%20Encryption>

‌Jena, B. K. (2023, February 9). *What Is AES Encryption and How Does It Work? - Simplilearn*. Simplilearn.com. <https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption>

‌