CS-305-J7997 Software Security

Module Four – Artemis Financial Encryption for Archive Files

Computer Science Department

Southern New Hampshire University

Eric Farkas

3/26/2023

Artemis Financial is seeking advice on encrypting its archive files. These are long-term archives and they wish to employ best practices and the most secure cipher available. This report will detail best practices, risks, governance and ciphers. It will provide a recommendation and justification for that recommendation. The goal is to retain Artemis Financial as a client and assist in implementing the encryption for its archive files. This report addresses several points and questions restated in bold throughout.

**Consider security protection best practices to defend against various types of security attacks.**

After a review of technologies and best practices, the best method to protect this data would be AES (Advanced Encryption Standard). This method protects against many attack methodologies and has a variety of key combinations available to adjust security as needed. AES is used in applications similar to the file protection requested by Artemis supporting our research. AES is also used in higher-sensitivity applications such as financial and medical transactions and within many US government agencies. The currently recognized and utilized key combinations for AES are 128-bit, 196-bit and 256-bit. These are sometimes referenced as 10 rounds, 12 rounds, and 14 rounds respectively which refers to the number of processing steps required to decrypt the data. A more practical example would be decrypting 128-bit AES with a brute-force attack on a supercomputer would take 1 billion billion years. This value increases exponentially with higher key values. This is why it is used to secure many transactions, websites and government communications. As the cipher is commonly used, it is not expensive to implement and seems a great choice to align with Artemis Financial’s goals for protecting archived data. The addition of this technology to the Artemis systems could extend to protect other personal information and transactions as well.

**Consider and identify all the risks in your recommendation.**

All ciphers have keys. The risk associated with AES is the private key being shared or obtained by an attacker. This type of attack is of a brute force nature but from a side channel. Although this appears to be a significant risk, numerous mitigation strategies can be employed to ensure the key is not vulnerable. The most significant strategy is awareness. Users of the Artemis system should be trained on the importance of protecting their credentials and using strong passwords. A policy can enforce this, but the policy does little to stop social hacking. Artemis may also wish to require multi-factor authentication. This is a practice that forces a user to identify with both credentials as well as a known device or secondary system. This stops attackers from attempting to spoof a user and with proper training can give Artemis insight into a potential attack.

**Consider the most current government regulations and how they will be met.**

There are several regulatory agencies where compliance should be considered for a financial services company like Artemis. The Gramm-Leach-Bliley Act requires financial institutions to disclose how sensitive information is handled. This disclosure includes the storage and transmission of the data. Using AES-128 would meet the criteria put forth by the act regarding appropriate safeguards to the data which would put Artemis in a position of compliance. The Payment Card Industry Data Security Standard (PCI-DSS) defines security standards for any company that processes electronic monetary transactions. It would be reasonable to believe Artemis must comply with PCI-DSS. AES-128 meets the current minimum standard for transactions and storage of information such as routing and account numbers and would put Artemis in compliance. Artemis is a global company, so the General Data Protection Regulation (GDPR) should also be considered. While GDPR does not have data security guidelines, it requires transparency regarding how sensitive data is handled and an opt-out mechanism. AES-128 is common and generally an acceptable response for inquiries regarding the protection of sensitive data under GDPR.

**How will this algorithm cipher be used?**

Artemis can choose how the cipher will be used and the types of transactions covered. We recommend protecting files sent and received from the document archive initially but eventually extending the cipher to protect customer profiles, account information and transactions. This recommendation will increase customer confidence and prevent packet sniffing and intercept attacks. by making all information obtained unusable.

**What is the best cipher, and why?**

AES is the best non-proprietary or general-use cipher available. It is possible to develop better ciphers but these are typically used in private applications. As Artemis does not have a private system, using generally available ciphers is the best practice and would minimize inconvenience to customers. It would be reasonable to assume that Artemis also transacts with systems owned by other financial institutions. These systems would be compatible with AES and secure integrations would be greatly simplified. All applicable regulatory agencies trust AES for transacting and protecting sensitive information.

**What are the reasons why you might not choose the most secure cipher?**

I’m not sure there is a good reason not to use the most secure cipher. To answer the question, I believe compatibility and system resources would be the driving factors. As mentioned in the prior section, it is possible to use more or less secure ciphers but they tend to be used in situations where the entity has control of both ends of the communication. Artemis will not have this option as the primary use of their system is by customers and they don’t have control of the customers’ computing devices. The other may be due to computing power. Ciphers do take resources to run and it is possible that limited aged equipment may not support the cipher or its resource needs. This is not a good reason to use a less powerful cipher but a business reason to upgrade the hardware assuming a strong cipher is truly needed.

**What is the purpose of the cipher's hash functions and bit levels?**

Hash functions ensure data integrity, verify digital signatures and store secure passwords. The hash function takes in raw data and produces a predictable end product. This practice provides a mask to the data. What I mean is that a password stored as 8 characters means that a hacker can start with the known value of 8. This is not true with a hashed password as it may be 8 characters but it may look like 32 characters when stored making it much harder to perform a dictionary-style hack against. Hash functions also cannot be reverse-engineered into plain text. This is a significant difference when comparing the hash function to bit levels. Although reverse-engineering a bit level to plain text does require a secure key to do so.

**Explain the use of random numbers, symmetric versus non-symmetric keys, and so on.**

To be truly secure, the keys should be generated randomly and be unknown to the system. Random number generators take care of creating these keys securely. Symmetric keys use a bi-directional key. This means the same secure key is used to encrypt and decrypt the data. Symmetric keys are inconvenient outside of closed systems. Non-symmetric keys have public and private key components. The private key is known only to the system and should be well protected whereas the public key is known by all outside users of the system and is valued only to initialize a session. No relationship allows a public key to derive the private key which is why the public key can be shared without consequences.

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

Cryptography has been used throughout history. It seems rooted in secure communications primarily focused on troop movements. The Spartans used a leather strap to communicate during battle. The strap had to be wrapped around an appropriately sized rod to be readable. The Germans used the Enigma machine to send coded messages about troop movement and other military communications. Whitfield Diffie and Martin Hellman published a paper in 1976 introducing the first non-symmetric key and paving the way to modern encryption techniques. Modern public key infrastructure was introduced with AES around 2000. Although AES is recognized as a reliable encryption standard, there is a movement to create newer, more compatible methods. Tokenization is one of these methods that started with digital currency. Tokenization is desirable because it can be stored, transmitted and audited. This makes it desirable for monetary movement and more easily audited when dealing with sensitive data