****

# Practices for Secure Software Report

Table of Contents

[Document Revision History 3](#_Toc102040754)

[Client 3](#_Toc102040755)

[Instructions 3](#_Toc102040756)

[Developer 4](#_Toc102040757)

[1. Algorithm Cipher 4](#_Toc102040758)

[2. Certificate Generation 4](#_Toc102040759)

[3. Deploy Cipher 4](#_Toc102040760)

[4. Secure Communications 4](#_Toc102040761)

[5. Secondary Testing 4](#_Toc102040762)

[6. Functional Testing 4](#_Toc102040763)

[7. Summary 4](#_Toc102040764)

[8. Industry Standard Best Practices 4](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **August 12th, 2023** | **Brooklen Ashleigh** | **Analysis of SSL server test configuration.** |

## Client



## Developer

Brooklen Ashleigh

## Algorithm Cipher

For encrypting Artemis Financials’ archive, I recommend using the 256-bit AES cipher. AES, or Advanced Encryption Standard, uses a Rjindael cipher, and has been adopted by the U.S. Government, which regulates it. It is one of the strongest ciphers available and has become an industry standard, as it is highly secure and cannot be cracked with brute force attacks (Daniel, 2023). The use of AES is governed by U.S. export control. However, the use of this encryption for copy protection and password protection is an exception, and I, therefore, do not believe Artemis Financial would have any problems using it to encrypt their archive, even if their financial system had dealings overseas.

This cipher will be used to encrypt Artemis Financial’s archive, which is a data-at-rest scenario, meaning that an efficient symmetric cipher is a good choice. Though other ciphers, like Blowfish, may be faster in some scenarios, AES’s robust defense and the fact that the data being encrypted is an archive means that speed is not the top priority. Rather, using AES at its 256 bit key length will utilize its maximum security potential, thereby protecting Artemis Financials’ sensitive records.

One might not choose the most secure cipher if it is not compatible with the application, if one only has control of one end of the encryption, or if it doesn’t suit the scenario. For example, symmetric encryption works well with data that is stored and at rest, while asymmetric encryption works well for data that is being transferred between two sources, as in the case with encrypted communication or files being transferred between server and user. If Artemis Financial wishes to use encryption in other applications such as end-to-end communication, utilizing a different cipher may be justified.

**Justification**

AES utilizes a 256-bit cipher hash that takes chunks of various-sized inputs and creates a hash value of the same length, regardless of the input size. This creates a nonsensical representation of the data that is being enciphered and stores it, while still being able to decipher it as needed using the same key. The bit level of the cipher used can be selected based on the application’s requirements. Generally, larger bit sizes mean more security, but also more resources to decrypt. AES is a fast cipher, so using larger bit levels is encouraged so as to maximize security. Because Artemis Financial is seeking to encrypt an archive, which is data at rest, it makes sense to use a symmetric cipher. A symmetric cipher uses the same key to encrypt and decrypt its data. Symmetric ciphers can encrypt and decrypt data more quickly than asymmetric ciphers (Daniel, 2023). The downside to a symmetric cipher is that it uses a single key, which is vulnerable to attackers if not implemented in a secure way. Asymmetric ciphers, by contrast, use both a public and private key that are linked together. Both must be used in tandem, with the public key being used to encrypt, and the private to decrypt. Asymmetric ciphers can be more secure but are generally slower and more resource intensive.

Ciphers are an evolving technology like any other in the computer science realm. They are created, then tested, and when vulnerabilities are found, they are phased out and replaced by newer, more robust successors. SSL has been replaced by TLS. A well-used cipher, DES for example, was found to fail against brute force attacks, which is why it was discontinued and dropped from usage. Others are not used because they are inefficient and, in the case of 3DES, take three passes to secure data. As technology evolves, it may be necessary to switch ciphers. In order to account for potential vulnerabilities, ciphers should be accounted for when dependency testing applications.

Currently, the most popular ciphers have different use cases. Some are faster than others, but the level of encryption available is also considered, along with its weakness or lack of weakness against different types of vulnerabilities. AES is a great choice, all around industry standard cipher that is well-supported by experts and doesn’t have major pitfalls or downsides. It should be used until a new successor is created with proven reliability and security.

## Certificate Generation

A screenshot of a computer

Description automatically generated A screenshot of a certificate

Description automatically generated

## Deploy Cipher

A black background with white text

Description automatically generated

## Secure Communications

A screenshot of a computer

Description automatically generated

## Secondary Testing

A computer screen shot of a black screen

Description automatically generated

A computer screen shot of a computer code

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

## Functional Testing

A screenshot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A black screen with many small squares

Description automatically generated with medium confidence

## Summary

The SSL Test Server has been refactored to address the following major areas of security concern:

* Cryptography
* APIs

This was facilitated by:

1. Switching from an http protocol to an https protocol.
2. Utilizing a hash function to provide unique checksums to verify the integrity of content
3. Conducting an OWASP vulnerability check to assess known issues with program dependencies

In order to address these security concerns, first, a self-signed certificate was generated in a keystore for use within the project. A certificate is unique and verifies that the client user is connecting to a verified source. The unique password and identification of the certificate was used in the application properties; the server is unable to start if that password or identification is incorrect. This ensures that the program is not compiled or launched with invalid information. In a production environment, this certificate allows a secure https connection between the client and the server, as discussed below.

Additionally, check sum functionality was added to the program. This check sum creates a unique unchangeable identifier for a piece of data that can then be compared to make sure that the contents of a file have not been changed. This makes sure that, for instance, when someone downloads important data, they can check to make sure that data is coming from its intended source and hasn’t been changed by a third party. This functionality was implemented by creating a function that takes raw data as a parameter and returns the unique SHA identifier.

To ensure the security of APIs, an OWASP dependency vulnerability check was conducted to verify the known security risks of each dependency used within the application. There are many historical vulnerabilities for each piece of the application, and those vulnerabilities must be assessed to first, see if they apply, second, to see if they can be updated or patched, and third if they can be lived with as a known vulnerability.

## Industry Standard Best Practices

## The use of SSL/HTTPS connectivity, encryption, checksums, and dependency checking are all industry standard methods of ensuring the security of a company’s transfering of data. The Artemis Financial project has been refactored to comply with these standards.

SSL certificates are used (and are now functionally required) to ensure that a website is legitimate and that a user is connecting to the site they intend to. Certificate Authorities issue SSL certificates on their own authority and knowing a certificate has been issued by a valid Certificate Authority lends legitimacy to a website and one’s connection to it.

As outlined by CISA.gov, “If a website has a valid certificate, it means that a certificate authority has taken steps to verify that the web address actually belongs to that organization. When you type a URL or follow a link to a secure website, your browser will check the certificate for the following characteristics:

1. The website address matches the address on the certificate.
2. The certificate is signed by a certificate authority that the browser recognizes as a "trusted" authority. (*Understanding website certificates: CISA* 2023)“.

In the past ten or so years, web protocols have been put in place to require the use of SSL certificates, or else trying to access a website is met with a huge warning barrier that the connection to the website might not be safe. This is to ensure that a connection is secure and less vulnerable to third-party interception. This is especially important when transmitting important identifying or financial information. Of course, this process is automated, and could potentially fail. One can check a certificate on their own using their own internet browser to ensure that the site they’re accessing has a certificate issued by a reputable CA.

The first approach to securing software dependencies is to find vulnerabilities using a dependency check, as performed above. Then, the development team must understand the vulnerabilities in play to decide if they apply to the current application. Some vulnerabilities only apply to certain use cases, such as the springboot vulnerability that affects “Spring MVC if it’s used together with a reverse proxy cache.” If vulnerabilities apply, then the team must analyze whether those vulnerabilities have been patched and if it is safe to upgrade those dependencies to a newer, usually safer version. If those dependencies are used with specific version numbers by modules or APIs, the same must be considered to see if it is possible to update to the newest versions of those APIs, then check to see if those vulnerabilities have been patched.

As reported above, some vulnerabilities apply to versions of software that are no longer supported by their developers, which means that those packages must be updated to a more recent version. Using actively supported software is integral to maintaining secure programs.

If vulnerabilities are live and have not been patched yet, developers must work to attempt to account for the functionality that the individual defects apply to, if possible. More robust input validation or time delays may help stymie improper validation or potential Denial of Service attacks, given by the vulnerabilities above.

Of course, dependency checks can give false positives. Therefore, applicable vulnerabilities should be checked against revolving vulnerability databases such as those maintained by the NIST and CVE. Those false positives can be suppressed as per the judgment of the development team using a suppression file.

Overall, these methods of security are used to help ensure that a third party who seeks Artemis Financials valuable information cannot access it. It is important to maintain the integrity of a company’s information, as losing the trust of customers is damning and often unfixable, and may tarnish a company's reputation. It is important to be vigilant and focus on security as part of normal business operations, from the beginning of a development cycle to its end.

References

CISA.gov. (2023, July 26). *Understanding website certificates: CISA*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/news/understanding-website-certificates