Frederick Brehm

5/28/2024

SNHU

CS 305

Module 4 Assignment

**1. What security protection best practices do you need to consider to defend against various types of security attacks?**

There are several different types of security protection best practices that can be utilized when securing data. A few of the simpler ones that will act as a front-line defense against potential attacks are incorporating strong passwords, firewalls, and continuously updating your software. However, the one security practice that will act as a foundation to building a long-lasting defense is encryption and decryption. This can be done by using secure socket layers which are now referred to as transport layer security. Certificate authorities are utilized in the TLS which sends and asks for a trusted key and if both sides have been verified and trusted a secure communication channel is created. There are two types of encryptions known as symmetric and asymmetric, where a secret key is used for scrambling information. This encryption is known as symmetric because it allows the same key to be used for both encrypting and decrypting. For Artemis Financial and determining what type of algorithm cipher to deploy, I would suggest using AES, advanced encryption standard.

**2. What are the risks of your recommendation?**

AES is the trusted standard algorithm used by the United States government, as well as many small and large organizations. AES is widely considered invulnerable to all attacks except for brute force. Symmetric means that keys are used for both encryption and decryption of data, therefore if potential attackers gained access to these keys they would have access to all data. For example, if you were to use a public Wi-Fi network and you used the key, it could be intercepted by a potential attacker and used to cause harm. AES encryption and decryption is also resource intensive and can be slower on devices that are older.

**3. What government regulations do you need to consider? How will these regulations be met?**

The NIST or National Institute of Standards and Technology with hand in hand with the government to ensure that the government, companies, and even citizens can be pleased knowing that the best encryption and decryption software is in place. Government, companies, and citizens all have extremely sensitive information that can range from bank cards and personal information on a simple home computer, or hundreds of thousands of files stored in databases used by the government and large companies. These regulations are met by utilizing AES which has the best protection to date. Even though more expensive for its high resource use, if the government only required a minimal standard of security, then personal information would be breached, causing millions or even billions of dollars lost.

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

The AES algorithm is used by creating keys, typically in the form of a public key and a private key. When two recipients need to send or receive data the sender’s algorithm encrypts the data. Once received, decryption will then take place on the receivers end through utilization of a private key.

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

AES or advance encryption standard is the best cipher. It is both vastly supported and recommended by the NIST and the government. AES is also known to be impenetrable, except for the case of a brute force attack. AES also offers 3 different levels, 128-bit, 192 bits, and 256-bit form. 128-bit form is already considered to be extremely successful, and this creates room to expand and improve using different bit sizes. Regardless, many internet security experts believe AES is and will continue to be the go-to standard for encrypting data.

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

Computers and processors continue to improve in every way and there is no reduction in technological advancement anytime soon. This means that extremely fast processors and super computers or eventual “quantum computers” will be able to break AES encryption in a matter of days. For example, Shor’s algorithm is based off making a guess of number factors, then making a bad guess and improving that guess to a good one to decrypt the data. No matter what algorithm we currently use the need to decommission or commission another type of algorithm will be necessary to safely encrypt data.

**7. Explain the purpose of the cipher's hash functions and bit levels?**

The goal of a hash function is to reduce the number of input bits to a fixed length. Hash functions typically generate a unique number that represents a value. There are different types of hash values such as string and integers. The main purpose of the cipher hash function is to efficiently map data of arbitrary size to a fixed size value, otherwise known as indexes in a hash table.

AES can come in three different bit levels including 128, 192, and 256. The main difference between these bit levels will be the length of the secret key that each use. The longer the key the harder it will be for a potential attack.

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

Symmetric and asymmetric are both encryption type algorithms typically used for cryptography which is used for encryption rather than signing. Asymmetric cryptography involves the use of two keys, a public key, and a private key. The private key is kept with only the sender and the public key can be known by anyone. Asymmetric algorithms are not typically used.

The government and corporations most often use symmetric cryptography. It is also used for encryption rather than signing. There is only one key in this type of algorithm which scrambles information to keep it secret. The reason it is called symmetric cryptography is because the same key is used to encrypt and decrypt data.

Random numbers are important in cryptography. Things such as TCP sequence, TLS nones, password salts, and DNS source port number all rely on random numbers. In cryptography this can be referred to as randomness. Randomness is important as it always creates new number sequences. Java has made this easy as they provide a class called SecureRandom that delivers an unpredictable sequence of numbers whenever you need them.

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

Cryptography stems from the Greek words “hidden writing” and is the practice of encrypting transmitted information so it can only be interpreted by the intended recipient. In ancient times the earliest cryptography can be found around 1900 BC. One of the first implementations was found by using non-standard hieroglyphs carved into the wall of a tomb from the Old Kingdom of Egypt. In the medieval era around the year 800 an Arab mathematician by the name of Al-Kindi invented the frequency analysis technique for cipher breaking, which represented one of the most monumental breakthroughs in cryptanalysis. Frequency analysis entails using linguistic data like the frequency of certain letters or letter pairings and parts of speech and sentence construction to reverse engineer private decryption keys. Fast forward to 1467, Leon Battista Alberti appeared and became known as the father of modern cryptography. His work most clearly explored the use of ciphers incorporating multiple alphabets known as polyphonic cryptosystems. In 1975 IBM created the DES (data encryption standard) which was the first cryptosystem certified by the NIST and was good enough to withstand even the strongest of computers during that time. However, in response to advancements in computing power, the DES was replaced by the AES (advance encryption standard) algorithm. AES uses a much longer encryption key which can also be shortened or lengthened depending on the bit, and to date cannot be cracked by modern hardware.

References

Schneider, J. (2024, January 10). *A brief history of cryptography: Sending secret messages throughout time*. IBM Blog. https://www.ibm.com/blog/cryptography-history/

GeeksforGeeks. (2024, May 20). *Hash functions and types of hash functions*. https://www.geeksforgeeks.org/hash-functions-and-list-types-of-hash-functions/

Manico, J., & Detlefsen, A. (n.d.). *Iron-clad Java*. O’Reilly Online Learning. https://learning.oreilly.com/library/view/iron-clad-java/9780071835886/ch06.html#ch06lev1sec1