Cryptography Best Practices

Tyler Chotikamars University of Arizona Global Campus

CYB 400 Cryptography

Michael Hayden

January 24th, 2022

Cryptography is a tool that can be used to protect data whether it is at rest, in transit, or even in use. The real-world applications of cryptography can range from being used within our government, by the military, and even within the private business sector. Basic cryptography is the practice of transforming information so that it is secure and cannot be accessed by unauthorized parties (Ciampa, 2020). The process of cryptography that is used today is called encryption. Within encryption today the encryption used information goes through three stages. These include plaintext, ciphertext, and cleartext. Plaintext describes unencrypted data in its original form, ciphertext is plaintext but it is scrambled in a way that is unreadable without decryption. Cleartext is readable data that is not meant to be encrypted. Today we'll be discussing a plan of action for mitigating a security breach, describe how the incorporation of a cryptographic algorithm can secure data, and how one can defend an attack using cryptography.

There are many different types of attacks that could occur within a business environment. Some attacks can range from malware, social engineering, and espionage or data interception. For attackers they can benefit from this by selling customer data, intercepting other sensitive data, and maybe even blackmail in some cases. To prevent these kinds of vulnerabilities, companies can devise a cryptography plan designed to mitigate security breaches. A great first step in creating a plan to mitigate security breaches is to first educate staff members. The more educated employees are of potential attacks, the easier it will be to protect against them. Educating employees about the tactics that social engineers use such as authority, intimidation, consensus, scarcity, urgency, familiarity, and trust is a sure way to mitigate security vulnerabilities. Implementing security measures to ensure people are who they say they are over the internet is one sure way to mitigating social engineering attacks. Educating employees of

basic attacks such as phishing will help prevent these kinds of social engineering attacks from happening. Many companies will send phishing links to their own employees to see how likely they are to falling for the attacks so that the company can promote more education about possible attacks. It is also important to educate people who are higher up within the company as they are more susceptible to attacks as they would have access more vital information. Another vital step in devising a plan for mitigating a security breach includes physical security. This can range from securing physical access to any IT infrastructure, to destroying any sensitive data. Destroying sensitive data includes the physical form such as papers and documents to prevent dumpster diving, and properly disposing of sensitive information such as customer data. Another implementation into the cryptography security plan includes encryption through software and encryption through hardware. A good example of encryption through software could include full disk encryption. Full disk encryption is particularly good for encrypting laptops or even computer systems in the office as it will deter any attackers that have physical access. Hardware encryption refers to the encryption of hardware devices such as USB drives and hard drives. Implementing a hardware security model should be a part of the initial cryptography plan.

There are many scenarios where incorporating a cryptographic algorithm to secure data is essential for the overall health of a company. Data breaches can account for millions of dollars' worth in damages, which leads to why it is important to have a cryptographic plan in place. A scenario including social engineering could be where an outside attacker impersonates a fellow employee, thus taking advantage of an individual within our network. By doing this they can bypass security implementations and cause damage to the company internally. A different scenario that cryptography can protect against would include attackers trying to intercept data in transit. In this case attackers can intercept data while it is in transit and can alter the message or

just scrape information. With strong encryption, there would be no way for the attacker to view the message unless they had a key to it or unless they decrypted the message themselves. In order to ensure that the person who sent you the message or email is who they say they are, we can make use of digital certificates. Digital certifications can be used to verify the integrity of incoming information as well as verify outgoing data. These certificates are used as containers that store the user's public key and is digitally signed by a trusted third party.

One typical cyber-attack that is relevant within cryptography and today's technology includes man-in-the-middle attacks. These kinds of attacks are ones where attackers can pose as a legitimate sender, or even alter the contents of a message. This means that if the CEO of the company emails you, an attacker can alter the message, intercept it, or even just scrape data as a means of spying on the conversation. To defend from this type of attack we can use encryption and certificates to ensure the integrity of the incoming transmissions and verify outgoing data. A known, secure cryptographic algorithm that could be used in a business environment to secure data is the advanced encryption standard (AES). This symmetric cipher makes use of 128 bits and performs three steps on each block of plaintext. The number of bits used within this algorithm is dependent on the size of the key and can range from 128 bits to 256 bits. Within AES-256, there are 13 rounds performed, within each round the bits are substituted and rearranged and thrown into a special computational mathematical formula based on the new arrangement of bit (Ciampa, 2018). Since AES is the standard for government encryption with no known vulnerabilities, it is the best option to choose when defending against a man-in-the-middle attack. Using this cryptographic algorithm will allow the sender to securely share data and receive data, while decrypting the information with a private key. There are other great examples of cryptographic algorithms that can also be used within this use case; however, AES

is probably the most secure. Symmetric cryptographic algorithms use the same single key to encrypt and decrypt data (Ciampa, 2018). With this type of algorithm, it is essential that the private key stays confidential to ensure the security of the data being transferred. Conversely, for this scenario, an asymmetric cryptographic algorithm could also be used to the same effect. Within this type of algorithm two keys are used instead of one, which is also why this method is known as public key cryptography. A public key is one that is known to everyone and freely distributed, while the private key is only known by the owner of the key. This algorithm allows the sender to encrypt data using the recipients public key, which then can only be decrypted by the recipients' private key. An asymmetric cryptographic algorithm that could be used this way is known as Digital Signature Algorithm (DSA) and this algorithm is periodically updated by NIST. With a digital signature, users can verify the sender, prevent the sender from disowning the message, and prove the integrity of the message. Another advantage of having so many different types of cryptographic algorithms available, is that for an attacker to decrypt information, they would have to go through the extra step of figuring out which algorithm was used to encrypt the data.

Cryptography is not a one all solution for computer systems, however it can be greatly beneficial when it is applied to the correct use cases that it exists for. Businesses and governments use cryptography as a mean of ensuring integrity and confidentiality since often they deal with sensitive information that could be detrimental when it is in the wrong hands. Enabling cryptographic algorithms correctly can mitigate attacks and save millions of dollars when implemented correctly. Cryptography includes a broad range of security implementations that can include social engineering to actual cryptography, and that is why it is still used and implemented in today's day in age. Having a plan of action for mitigating a security breach is

essential for many companies and the proper incorporation of cryptographic algorithms is the best way to secure data and defend against attacks.

References:

Ciampa, M. (2018). *CompTIA security+ guide to network security fundamentals* (6thed.). Cengage Learning.

NIST. (2022). Computer Security Resource Center. Retrieved from: https://csrc.nist.gov/glossary/term/man_in_the_middle_attack