Symmetric and asymmetric encryption

Previously, you learned these terms:

- **Encryption**: the process of converting data from a readable format to an encoded format
- **Public key infrastructure** (PKI): an encryption framework that secures the exchange of online information
- **Cipher**: an algorithm that encrypts information

All digital information deserves to be kept private, safe, and secure. Encryption is one key to doing that! It is useful for transforming information into a form that unintended recipients cannot understand. In this reading, you'll compare symmetric and asymmetric encryption and learn about some well-known algorithms for each.

Types of encryption

There are two main types of encryption:

- **Symmetric encryption** is the use of a single secret key to exchange information. Because it uses one key for encryption and decryption, the sender and receiver must know the secret key to lock or unlock the cipher.
- **Asymmetric encryption** is the use of a public and private key pair for encryption and decryption of data. It uses two separate keys: a public key and a private key. The public key is used to encrypt data, and the private key decrypts it. The private key is only given to users with authorized access.

The importance of key length

Ciphers are vulnerable to **brute force attacks**, which use a trial and error process to discover private information. This tactic is the digital equivalent of trying every number in a combination lock trying to find the right one. In modern encryption, longer key lengths are considered to be more secure. Longer key lengths mean more possibilities that an attacker needs to try to unlock a cipher.

One drawback to having long encryption keys is slower processing times. Although short key lengths are generally less secure, they’re much faster to compute. Providing fast data communication online while keeping information safe is a delicate balancing act.

Approved algorithms

Many web applications use a combination of symmetric and asymmetric encryption. This is how they balance user experience with safeguarding information. As an analyst, you should be aware of the most widely-used algorithms.

Symmetric algorithms

- *Triple DES (3DES)* is known as a block cipher because of the way it converts plaintext into ciphertext in “blocks.” Its origins trace back to the Data Encryption Standard (DES), which was developed in the early 1970s. DES was one of the earliest symmetric encryption algorithms that generated 64-bit keys. A **bit** is the smallest unit of data measurement on a computer. As you might imagine, Triple DES generates keys that are 192 bits, or three times as long. Despite the longer keys, many organizations are moving away from using Triple DES due to limitations on the amount of data that can be encrypted. However, Triple DES is likely to remain in use for backwards compatibility purposes.
- *Advanced Encryption Standard (AES)* is one of the most secure symmetric algorithms today. AES generates keys that are 128, 192, or 256 bits. Cryptographic keys of this size are considered to be safe from brute force attacks. It’s estimated that brute forcing an AES 128-bit key could take a modern computer billions of years!

Asymmetric algorithms

- *Rivest Shamir Adleman (RSA)* is named after its three creators who developed it while at the Massachusetts Institute of Technology (MIT). RSA is one of the first asymmetric encryption algorithms that produces a public and private key pair. Asymmetric algorithms like RSA produce even longer key lengths. In part, this is due to the fact that these functions are creating two keys. RSA key sizes are 1,024, 2,048, or 4,096 bits. RSA is mainly used to protect highly sensitive data.
- *Digital Signature Algorithm (DSA)* is a standard asymmetric algorithm that was introduced by NIST in the early 1990s. DSA also generates key lengths of 2,048 bits. This algorithm is widely used today as a complement to RSA in public key infrastructure.

Generating keys

These algorithms must be implemented when an organization chooses one to protect their data. One way this is done is using OpenSSL, which is an open-source command line tool that can be used to generate public and private keys. OpenSSL is commonly used by computers to verify digital certificates that are exchanged as part of public key infrastructure.

Note: OpenSSL is just one option. There are various others available that can generate keys with any of these common algorithms.

In early 2014, OpenSSL disclosed a vulnerability, known as the Heartbleed bug

, that exposed sensitive data in the memory of websites and applications. Although unpatched versions of OpenSSL are still available, the Heartbleed bug was patched later that year (2014). Many businesses today use the secure versions of OpenSSL to generate public and private keys, demonstrating the importance of using up-to-date software.

Obscurity is not security

In the world of cryptography, a cipher must be proven to be unbreakable before claiming that it is secure. According to Kerchoff’s principle

, cryptography should be designed in such a way that all the details of an algorithm—except for the private key—should be knowable without sacrificing its security. For example, you can access all the details about how AES encryption works online and yet it is still unbreakable.

Occasionally, organizations implement their own, custom encryption algorithms. There have been instances where those secret cryptographic systems have been quickly cracked after being made public.

Pro tip: A cryptographic system *should not* be considered secure if it requires secrecy around how it works.

Encryption is everywhere

Companies use both symmetric and asymmetric encryption. They often work as a team, balancing security with user experience.

For example, websites tend to use asymmetric encryption to secure small blocks of data that are important. Usernames and passwords are often secured with asymmetric encryption while processing login requests. Once a user gains access, the rest of their web session often switches to using symmetric encryption for its speed.

Using data encryption like this is increasingly required by law. Regulations like the Federal Information Processing Standards (FIPS 140-3) and the General Data Protection Regulation (GDPR) outline how data should be collected, used, and handled. Achieving compliance with either regulation is critical to demonstrating to business partners and governments that customer data is handled responsibly.

Key takeaways

Knowing the basics of encryption is important for all security professionals. Symmetric encryption relies on a single secret key to protect data. On the other hand, asymmetric uses a public and private key pair. Their encryption algorithms create different key sizes. Both types of encryption are used to meet compliance regulations and protect data online.

Revision #1
Created 24 July 2023 10:54:24 by naruzkurai
Updated 15 August 2023 18:44:11 by naruzkurai