CRYPTOGRAPHIC ATTACKS

Birthday Attacks

Consider that you are searching for a hash collision. It will be more difficult to locate a hash collision if you're looking for one that generates a certain output as opposed to one that generates any output. The method of faking digital signatures known as a "Birthday Attack" takes advantage of this hash collision characteristic. If you have many, slightly different copies of the valid file that generate distinct hashes and you're seeking to locate a malicious file with the same hash, it will be simpler.

Birthday Attacks take their name from the Birthday Paradox, which states that there is a 50% chance that two individuals in a group of 23 will share the same birthday.

Hash Collisions

The outputs of hashing algorithms are fixed in length. For instance, Sha-256 always yields a 256-bit result. However, practically speaking, hashing algorithms typically don't have restrictions on the size of their limitations. This suggests that since there are more inputs than outputs, there must be outputs that can be produced from multiple inputs. A hash collision occurs when a hashing algorithm yields the same result for two different inputs.

In general, it is more difficult to detect hash collisions in hashing algorithms whose output sizes are big.

SSL Stripping

A version of the HTTP protocol protected by SSL is known as HTTPS. In a technique known as SSL Stripping, a cunning attacker can downgrade a connection from HTTPS to insecure HTTP. This enables an attacker to get around the security measures put in place by HTTPS, such as confirming that a website is actually the website it claims to be.

By setting up servers and browsers to exclusively accept HTTPS connections and reject regular HTTP connections, SSL Stripping can be easily avoided. One method servers can use to stop SSL stripping is the HTTP Strict Transport Security (HSTS) header.

Making Use of the Implementation

A door's strength depends entirely on the frame it is mounted in. Even while some forms of encryption are susceptible to mathematical attacks, it is frequently considerably simpler to simply "go past" the cryptographic protection altogether.

Session Replay Attacks

Attacks are known as "Session Replay Attacks" involve the "replay" of stolen data. For instance, even if they didn't have your credentials, if an attacker can intercept a communication where you log into your bank, they could be able to resend the same information and access your bank account.

It is possible to stop session replay attacks by timestamping requests, spotting suspicious data within a request, or making sure that each request is distinctive and only valid once.

Initialization Vectors

The initial state of a cryptographic method is determined by a value known as an Initialization Vector (IV), commonly referred to as a Nonce (Short for "Number Only Used Once"). A well-designed system will make it difficult to predict the IV because a predictable IV indicates that the cryptographic algorithm's output will also be predictable.

Sadly, not every system is well-designed. An initialization vector attack is a sort of attack where an attacker can access apparently protected data by disabling encryption by foretelling the IV used in it. A poorly constructed IV might use a pseudo-random number generator with a flawed design that enables an attacker to anticipate future IVs based on prior IVs, or it might start from the same value each time the machine is turned on.

Pass the Hash Attacks

Passwords that are properly stored are hashed with salt and are incredibly difficult to decrypt. The same procedure is used to verify that a password is typed correctly, and then it is compared to the right password's hash. They must match for the password to be accurate. What happens, though, if the right hash is stolen during an attack?

Given that it would be hashed again and yield a different result, most systems won't be vulnerable if the right hash is merely entered in the password field. Password hashes are nevertheless accepted as authentication credentials by some systems. The Pass the Hash attack, which is frequently used to log onto other computers in a compromised network, is known as that.

Another illustration of this kind of vulnerability would be if a website hashed the user's password client-side instead of using a secure connection for authentication. An attacker might obtain the hash from the unencrypted communication and use it whenever they wanted to log in. Sadly, this is not a made-up instance.

Only if an attacker can obtain the hash are pass the hash assaults feasible. An attacker might be able to steal the hashes of user accounts on a computer if they have local administrative access to it, and they might use those hashes to log into other machines. Systems for password management and vaulting are effective protections in this situation, as is making sure that the least privilege principle is applied to all accounts.

Conclusion

Although cryptography is a strong security technique, it is not a perfect solution. Like every security mechanism, if it is not used correctly or implemented, it can be circumvented and cannot offer full security.