EXAMPLES OF CRYPTOGRAPHIC ATTACKS

Password Attack

Attacks related to passwords are often password cracking or password guessing. Attackers attempt to discover passwords by attempting reversed hash matching on stolen hashed passwords from databases. When trying to steal passwords, the attacker firs steals the database account for the database which stores all the users and their passwords. Most systems will store passwords securely by encrypting them. That way, passwords are not stored in plain text, so they are not readable. However, the attacker can take different patterns of passwords, use the same hashing algorithm on those patterns, and produce their own hashes. If the attacker gets a hash value that matches the hash value from the database, the attacker discovers the actual password. This is an example of reversed hash matching attack.

Password attacks are performed in two general ways. One way is by using dictionary attacks, and the other way is by using brute force attacks. A dictionary based attack is when a predefined list of possible passwords is used to try and perform reversed hash matching against a stolen database. In the brute force attack the attacker attempts all possible combinations of characters to discover passwords in the database. Brute force attacks are simplified, which means that their success is made easier due to many problems.

Number one is the weakness in the keys of the algorithm used to protect the passwords in the first place, mathematical weaknesses in the known algorithms, or exploiting implementation flaws in the software that uses the algorithm. Password attacks are not the only type of attacks out there. Other types of cryptographic attacks simply try to discover encryption key or the encryption algorithm used.

Analytic Attack

An analytic cryptographic attack is an algebraic mathematical manipulation that attempts to reduce the complexity of the cryptographic algorithm. If this attack is successful, the attacker is able to quickly deduce how the plain text is converted to the cyphered text.

Implementation Attack

An implementation attack exploits implementation weaknesses in software, protocol or algorithms.

Statistical Attack

Statistical attacks exploit statistical weaknesses in a cryptosystem, such as the inability to produce true random numbers or floating point errors caused by the CPU.

Other types of attacks focus on the hashing algorithms. This type of attack attempts to discover which two messages will result in the same hash values. This is known as the birthday attack.

Birthday Attack

The birthday attack exploits the probability that two messages using the same hash algorithm will produce the same message digest. So, it is exploiting collisions.

Meet-in-the-middle Attack

In a meet-in-the-middle attack the plain text is encrypted with every possible key at one end, and then a cryptographic message is then decrypted with every possible key at the other end. The result of the comparison can help to discover which algorithm is used and the secret key.

Man-in-the-middle Attack

In a man-in-the-middle attack, an attacker can intercept messages between two parties and possibly modify them.

Replay Attack

In a replay attack, an attacker intercepts session keys or authentication traffic and then replays them later to authenticate and gain access.

Countermeasures

Countermeasures include having good key management, using strong keys and using keys throughout key space. To protect ourself from password specific attacks, we should deploy strong password policies. A strong password policy means that we use multiple character types (uppercase, lowercase, numbers and symbols), minimum password length (for example, eight characters or more), etc. Also, users should not use dictionary words in their password, password should be changed on regular basis, and we should enforce account lockout and password history to prevent re-use. We should also audit our environment for excessive failed logons, and we should monitor the network for sniffing and password theft tools.

Source: http://www.utilizewindows.com/security/cryptography/459-examples-of-cryptographic-attacks