Table of Contents

Cryptography

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography is closely related to the disciplines of cryptology and cryptanalysis.

Cryptography is most often associated with scrambling plaintext or ordinary text, sometimes referred to as cleartext into ciphertext this process is called encryption, then back again into plaintext this process is known as decryption.

Cryptography Attacks

A cryptographic attack is a method for circumventing the security of a cryptographic system by finding a weakness in a code, cipher, cryptographic protocol or key management scheme.

Attacks are typically categorized based on the action performed by the attacker.

An attack, thus, can be passive or active

Passive Attacks

The main goal of a passive attack is to obtain unauthorized access to the information. For example, actions such as intercepting and eavesdropping on the communication channel can be regarded as passive attack.

These actions are passive in nature, as they neither affect information nor disrupt the communication channel. A passive attack is often seen as stealing information.

Active Attacks:

An active attack involves changing the information in some way by conducting some process on the information.

For example, Modifying the information in an unauthorized manner. Initiating unintended or unauthorized transmission of information.

Alteration of authentication data such as originator name or timestamp associated with information Unauthorized deletion of data.

Other types of attacks

Dictionary Attack

This attack has many variants, all of which involve compiling a ‘dictionary’. In simplest method of this attack, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.

Brute Force Attack (BFA)

In this method, the attacker tries to determine the key by attempting all possible keys. If the key is 8 bits long, then the number of possible keys is 28 = 256. The attacker knows the ciphertext and the algorithm, now he attempts all the 256 keys one by one for decryption. The time to complete the attack would be very high if the key is long.

Birthday Attack

This attack is a variant of brute-force technique. It is used against the cryptographic hash function. When students in a class are asked about their birthdays, the answer is one of the possible 365 dates. Let us assume the first student’s birthdate is 3rd Aug. Then to find the next student whose birthdate is 3rd Aug, we need to enquire 1.25*□√365 ≈ 25 students.

Similarly, if the hash function produces 64 bit hash values, the possible hash values are 1.8×1019. By repeatedly evaluating the function for different inputs, the same output is expected to be obtained after about 5.1x109random inputs.

If the attacker is able to find two different inputs that give the same hash value, it is a collision and that hash function is said to be broken.

Man in Middle Attack (MIM)

The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.

Host A wants to communicate to host B, hence requests public key of B. An attacker intercepts this request and sends his public key instead. Thus, whatever host A sends to host B, the attacker is able to read.

In order to maintain communication, the attacker re-encrypts the data after reading with his public key and sends to B.

The attacker sends his public key as A’s public key so that B takes it as if it is taking it from A.

Buffer flow attack

A buffer is a temporary space for data storage. Buffer overflow occurs if the data is stored by a program or process in a buffer is greater than the maximum capacity of the buffer. The extra data can overflow into adjacent buffer corrupting or overwriting the valid data held in them.

Ping of death attack

Ping of death attack takes advantage of a weakness in TCP-IP protocol. The weakness is that many computer system can not handle an IP packet larger than the maximum IP packet size of 65535 bytes. Buffer overflow is occure in ping of death attack.

The ping of death sends ping packet larger than 65535 bytes to the victim by fragmenting the packets, then a receiving computer reassemble the packet a buffer overflow occure which aften cause computer to crash.

DoS Attack (Denial of Service Attack)

A Denial-of-Service attack or DoS is an attack targeting the availability of web applications. Unlike other kinds of attacks, DoS attacks' primary goal is not to steal information but to slow or take down a web site. The attackers' motivations are diverse, ranging from simple fun, to financial gain and ideology (hacktivism). A denial of service attack generates high or slow rate attack traffic exhausting computing resources of a target, therefore preventing legitimate users from accessing the website.

Teardrop attack

A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device.

Related Posts:

1. Types of Attack
2. Security threats
3. Computer and cyber security
4. Introduction to network security
5. Intrusion detection tool
6. Categories of security assessments
7. Security terminologies and principals
8. Intoduction to intrusion
9. Intrusion detection tool

10. Categories of security assessments
11. Intrusion terminology
12. Cryptography
13. SSH
14. MD5
15. Message digest functions
16. Digital signature
17. Authentication Functions
18. One way hash function
19. Hash function in network web security
20. Digital signature standard
21. SSL Secure socket layer