Q Attacks and Attack Types :-:

=>

In cryptography, attacks are the methods used to circumvent the security of a cryptographic system by finding a weakness in the code, cipher, cryptographic protocol or the key. It is also called cryptanalysis.

The goal / objective of performing a attack (crypt-analysis on a cipher text is to gain information about the original plain text.

Based on what information the attacker has access to, attacks can be classified as:

i> Cipher text only attack:
-> In this type of attack, the cryptanalyst has access only to the cipher text.

ii> Known plaintext:
-> In this form of attack, the attacker has information about the cipher text and the original plaintext corresponding to the cipher text.

iii> Chosen plaintext / chosen ciphertext.
-> In this type of attack, the attacker can gain access to ciphertexts corresponding to an arbitrary set of plain texts of their own choosing.

iv) Adaptive chosen plaintext

-> It is similar to chosen plaintext attack, except the attacker can choose subsequent plaintexts based on information learned from previous encryptions.

v) Related key attack

-> In this form of attack, the attacker has access to two related keys and their corresponding cipher texts. These keys are different but are known to be related in some matter.

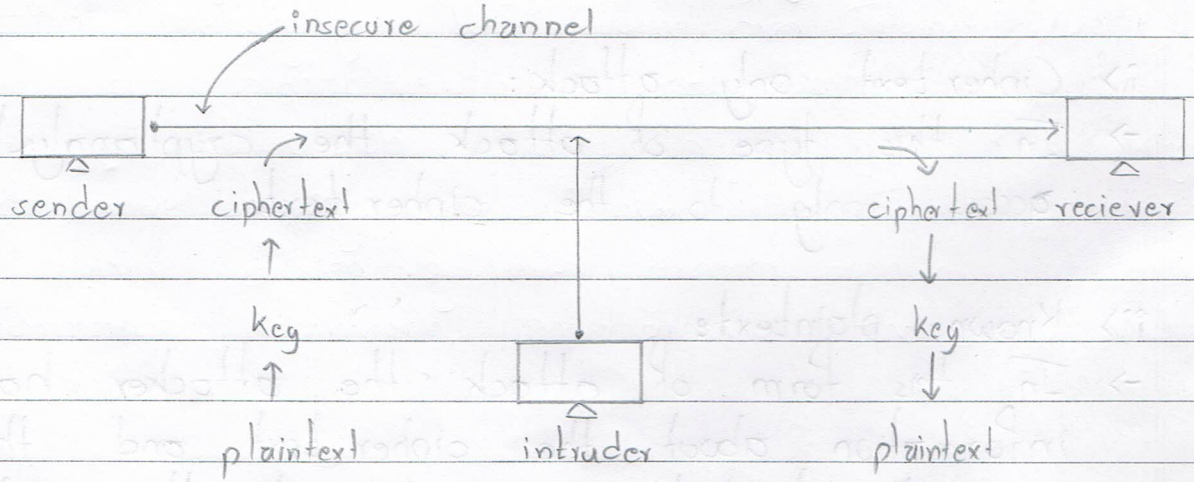

Fig:- basic model of an attacker/intruder in a cryptographic system

Q Attack Types:

i) Brute force attack

→ It is a type of cipher text only attack where the attacker tries out every possible key combination in order to decrypt the cipher text. Depending on the permutation of possible keys, brute force can either be feasible or not. If a key has n ~~numble~~ number of possible key combinations, then on average, it requires n/2 tries to obtain the key.

Despite the fact that brute forcing ~~can~~ will give the required plain text, it is not feasible for use in modern cryptology. Due to advancement in modern cryptographic algorithms, the time required for a brute force attack to decipher the information ~~it~~ is in terms of 100s of millions of years. And because the data is generally compressed, it becomes even harder to detect whether the brute forced key has resulted in the required plaintext or not.

ii) Man-in-the-middle attack

⇒ In man in the middle attack, the intruder overtakes the data transmission medium and relays all the information through itself. The attacker might be able to intercept the network during key exchange ~~whe~~ which will result in the

attacker being able to decrypt all further shared information.

iii> Side Channel Attack

=> They are the attacks based on the information gained from the physical implementation of a computer system rather than the implemented algorithm instead.

iv> Power Analysis Attack:

=> In this type of attack, the attacker analyzes the power consumption as a reference to get the information about what the computer is computing.

Q Viruses

=>

Viruses are malicious pieces of computer code / applications that when executed produces harmful and ~~unwanted~~ + unwanted result(s). If a virus is able to penetrate the security of the computer, then the affected areas are said to be "infected" with a computer virus. After infecting, they spread to other parts.

Virus can infect a computer system by using social engineering deception - psychologically manipulating people into performing actions; and exploit the security of the system. Since Microsoft Windows is the most widely used Operating System, most of the viruses in existence target it.

Viruses are written in order to gain profit (ransomware), desire to make a statement, personal amusement, to demonstrate that a vunerability in the system exists and so on. Because of the harmful nature of a computer virus, viruses cause a lot of economical damage each year by causing system failure, wasting computer resources, corrupting data, increasing maintainance cost, etc. To prevent this from happening in the first case, multitudes of anti-virus tools have been deployed. Anti-virus softwares detect the virus before it gets a chance to infect the system.

Q Worms

⇒

Worms are a type of virus, a malicious program designed to replicate itself and to spread to other computers. Any code designed to do more than spread the worm is typically referred to as the "payload". The most common payload for worms is to create a backdoor that allows the computer to be remotely controlled by the worm author as a "zombie". Network of zombified computers are commonly refered to as botnets.

While worms might not seem to manipulate the working of a system, they are still very harmful. A rapidly spreading worm can cause major disruption by increasing network traffic. To minimize the harm caused by worms, software developers have been deploying regular updates to the software. Since worms do not directly impact the system it has infected, they are harder to detect. A research has been put forth to help identify worms. The research suggests monitoring the number of network scans that a computer node makes on the network. If the computer is making alot of scans, it can be assumed that the computer has been infected by a worm.

Q Trojan Horse

=>

Trojan horse is a type of computer virus that misleads the user of its true intent in order to infect the system. The term is derived from an Ancient Greek story of a deceptive wooden horse that led to the fall of Troy.

Trojan horse viruses disguise themselves as useful applications. while hiding their real intent of infecting the computer. For example; a trojan horse might disguise itself as a calculator app while it is quitely spreading itself to different parts of the system and performing malicious actions. Trojans can also allow an attacker to access users' personal information, passwords, etc and even in worst cases they can be a ransomware. But unlike worms, trojan horses are generally not made to spread to ~~multi~~ magnitudes of other computers.

Since trojans disguise themselves as useful applications, they are harder to detect. Because of this reason, it is generally advised to not open on trusted ~~app~~ zip attachments in e-mails, download software from suspicious sites, or allow applications the right to gain higher level of access. an so on.