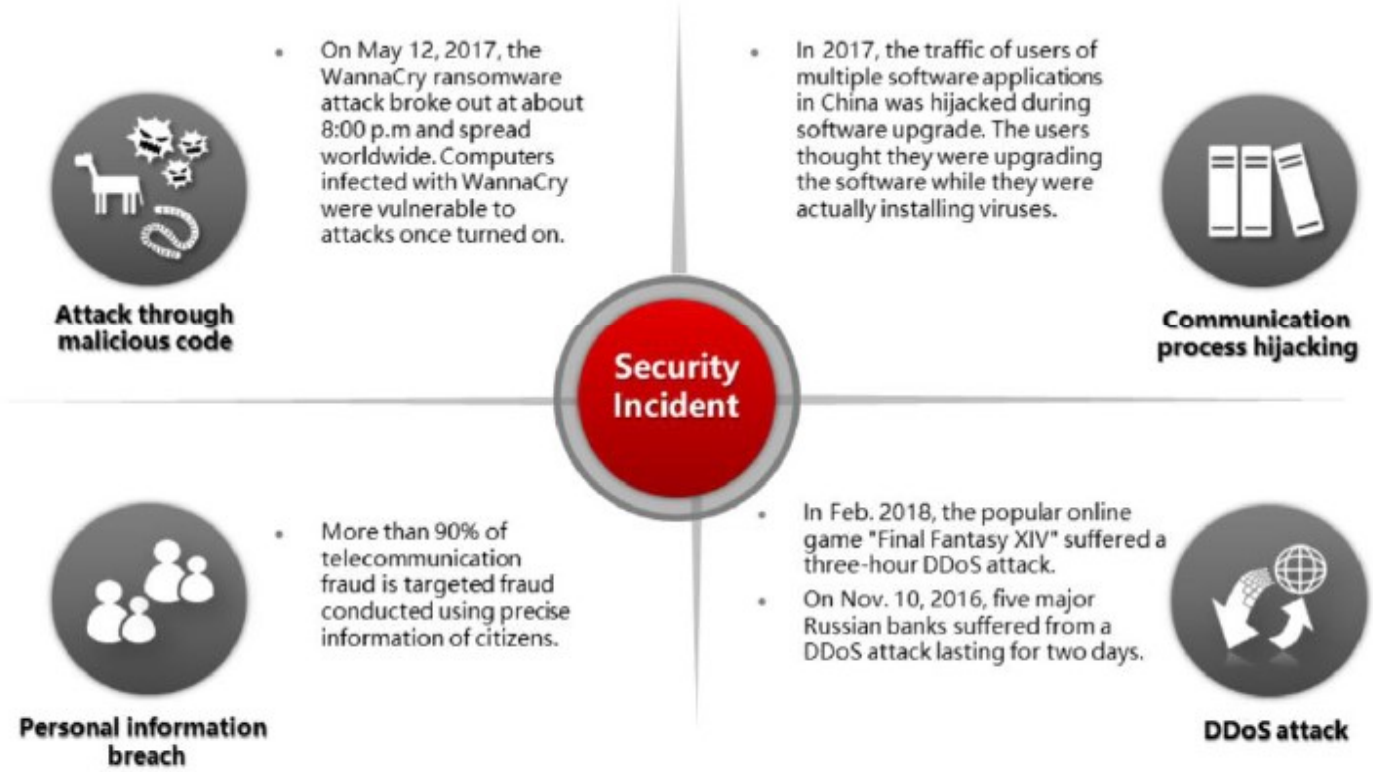
Common Information Security Threats

www.huawei.com

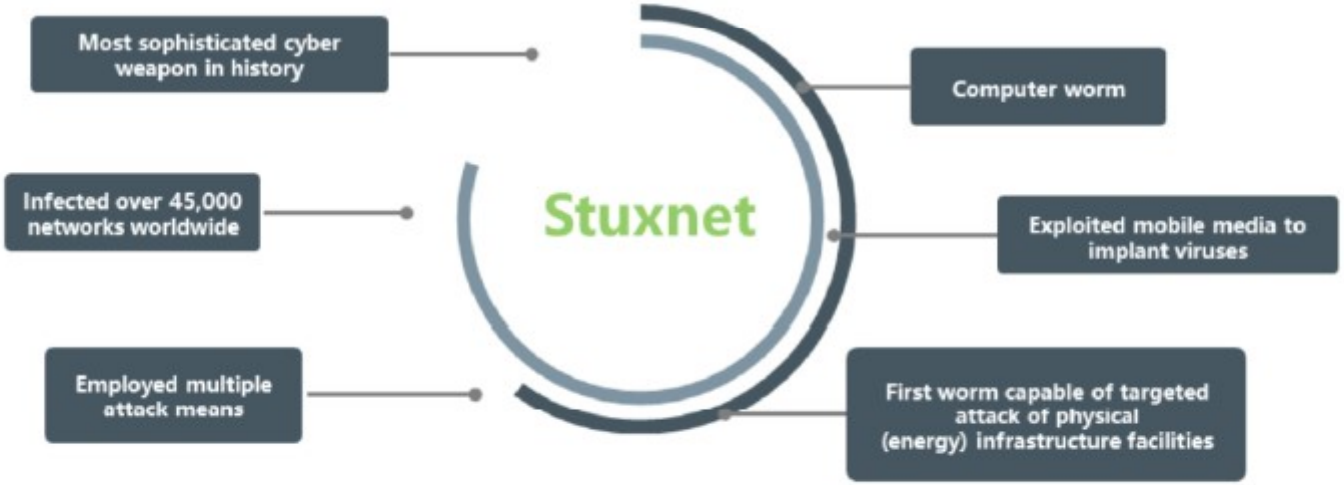
HUAWEI

Endless Security Incidents



Beginning of the Cyberwar - Stuxnet

- In February 2011, Iran suddenly announced it was to unload fuel from its first nuclear power station. Previously, the industry said Iran needed only one year to be capable of quickly creating nuclear weapons. However, the Stuxnet attack ruined one fifth of the centrifuges of Iran, postponing the research for at least two years, during which time the global landscape changed.



Evolution of Information Security Attacks

Forms of attack largely unchanged

Current attackers still use viruses, phishing, etc. to target vulnerabilities, much the same as in the past.

More sophisticated attack means

A major attack usually requires sophisticated deployment, long-term incubation, and a combination of multiple attack methods to achieve the ultimate goal.

Diverse attack purposes

The attack targets range from targeting personal computers to being used to influence economy, politics, war, energy, and even the global landscape.

Security Threat Categories

- DDoS attacks
- Network intrusion

- OS vulnerabilities
- Viruses (such as Trojan horses and worms)
- Phishing websites
- Data breaches

- Communication traffic hijacking
- Man-in-the-middle (MITM) attacks
- Unauthorized login to the system
- Weak security protection for Wireless Networks

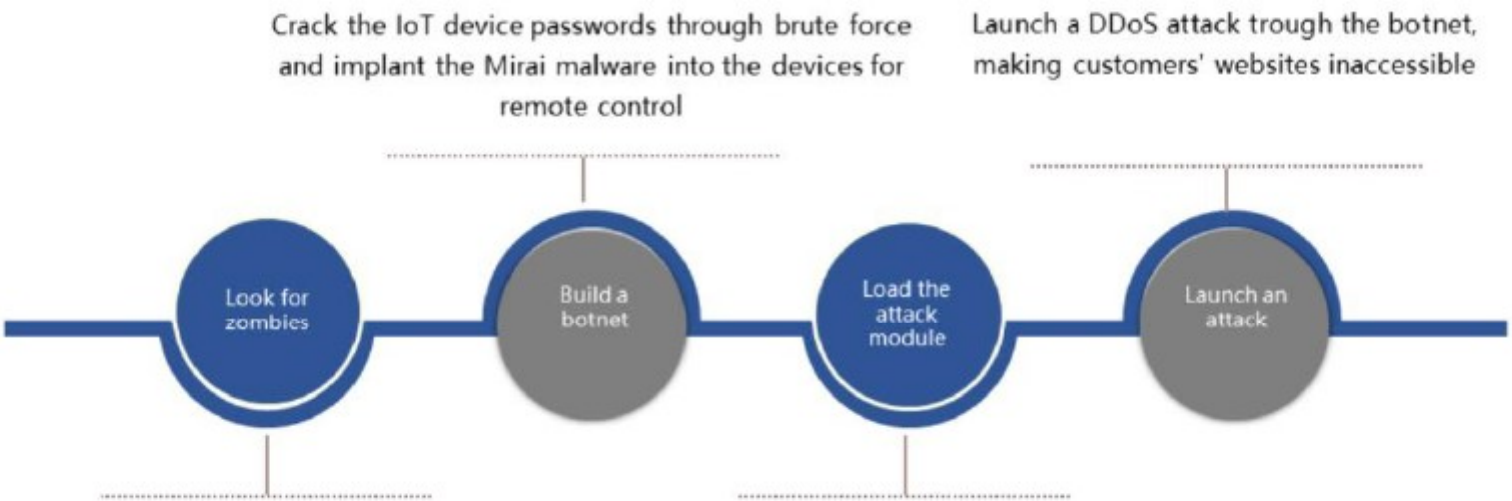
Contents

HUAWEI

DDoS Attacks Against Dyn DNS Service in the United States

- On October 21, 2016, the DNS service from Dyn in the U.S. was hit by DDoS attacks from about 11:00 a.m. to 5:00 p.m. UTC. The attacks paralyzed nearly half the networks in the United States.
- These large-scale DDoS attacks were launched from botnets formed by IoT devices, which were infected with Mirai malware.

Process of a Mirai Attack



What means were used in this attack?

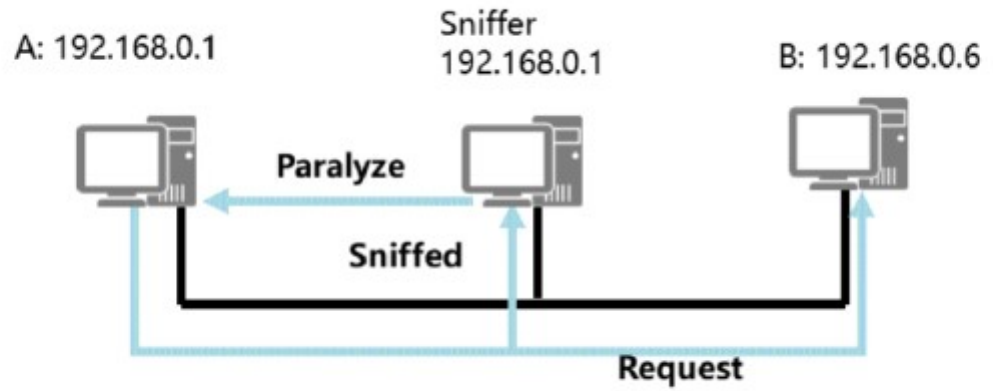
Scanning

- Scanning is a potential attack action. It does not directly interrupt network devices. However, it gathers relevant network information before an attack.

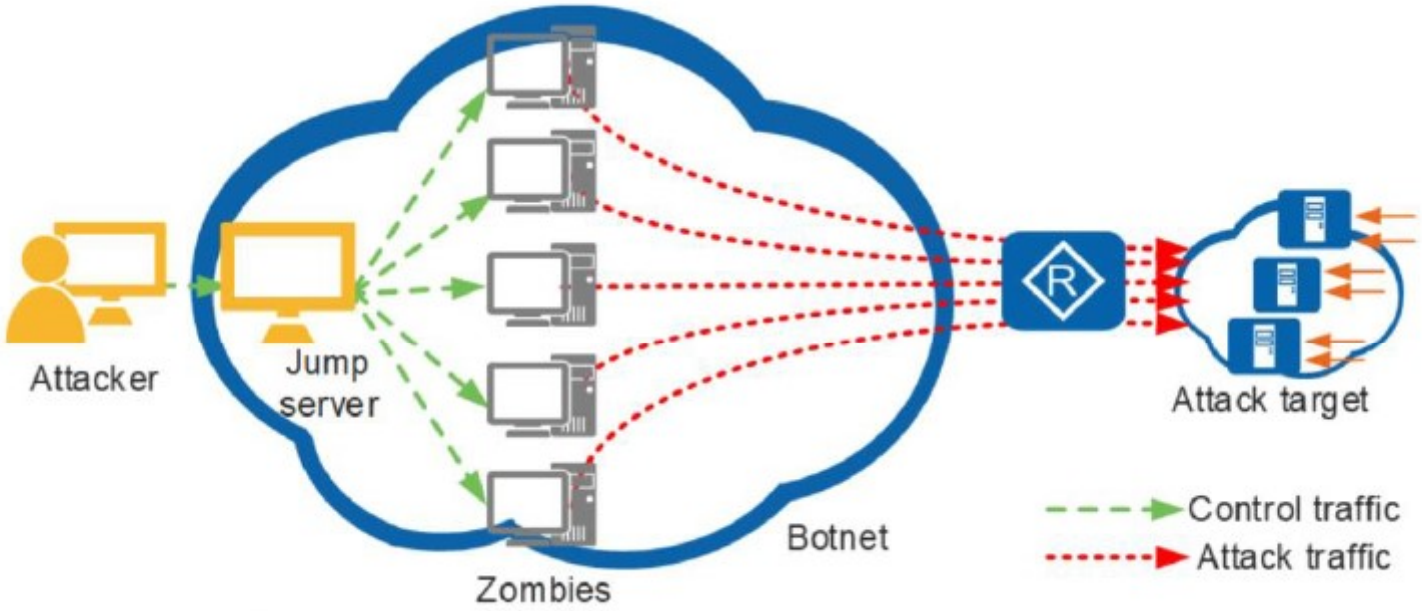
Address scanning	Port scanning
An attacker sends ICMP packets to destination addresses or uses TCP/UDP packets to initiate connections with certain IP addresses. By checking whether there are response packets, the attacker can determine which target systems are alive and connected to the target network.	An attacker probes the network structure by scanning ports to identify ports open to the attack target, so as to determine the attack mode. The attacker usually uses the Port Scan software to initiate connections to a series of TCP or UDP ports on a wide range of hosts. Based on the response packets, the attacker can determine whether the hosts use these ports for providing services.

Spoofing Attack - Obtaining the Control Permission

- Attackers can obtain the control permission by brute force cracking of passwords. Also, attackers can launch spoofing attacks such as IP spoofing to obtain access and control permissions.
- IP spoofing: An attacker may send packets with forged source IP addresses to target hosts to obtain superior access and control permissions.



Launching a DDoS Attack



- DDoS attacks:
  - Exhaust network bandwidth
  - Exhaust server resources

HUAWEI

Defense Measures for Cyber Attacks

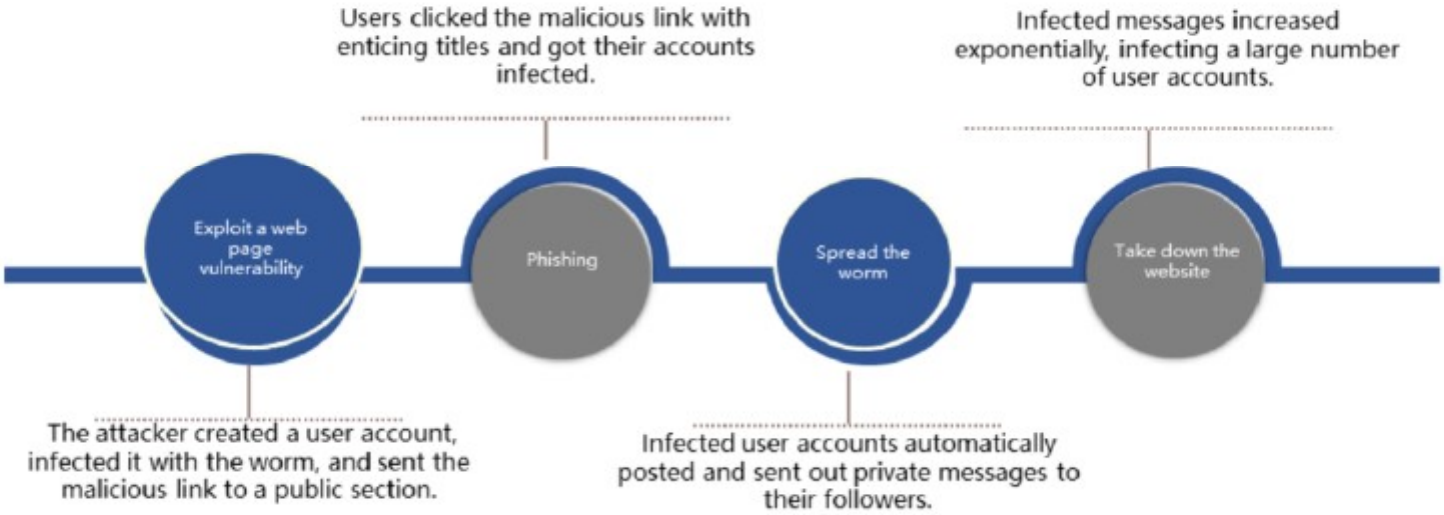
- Firewalls: Deploying firewalls at the intranet egresses of medium- and large-sized enterprises and data centers can efficiently defend against common DDoS attacks and traditional single-packet attacks.
- Anti-DDoS devices: Anti-DDoS solutions provide professional anti-DDoS services for carriers, enterprises, data centers, portal websites, online games, online videos, and DNS services.

Contents

HUAWEI

Worm Attack Against Weibo

- Sina Weibo (the Chinese Twitter) was once hit by a worm that affected over 30,000 users in less than an hour. The attack process was as follows:



Threats Brought by Vulnerabilities

- Vulnerabilities are defects in the implementation of hardware, software, or protocols or in system security policies. They allow attackers to access or damage systems without authorization.
- If system vulnerabilities are not fixed in time, the following attacks may occur:

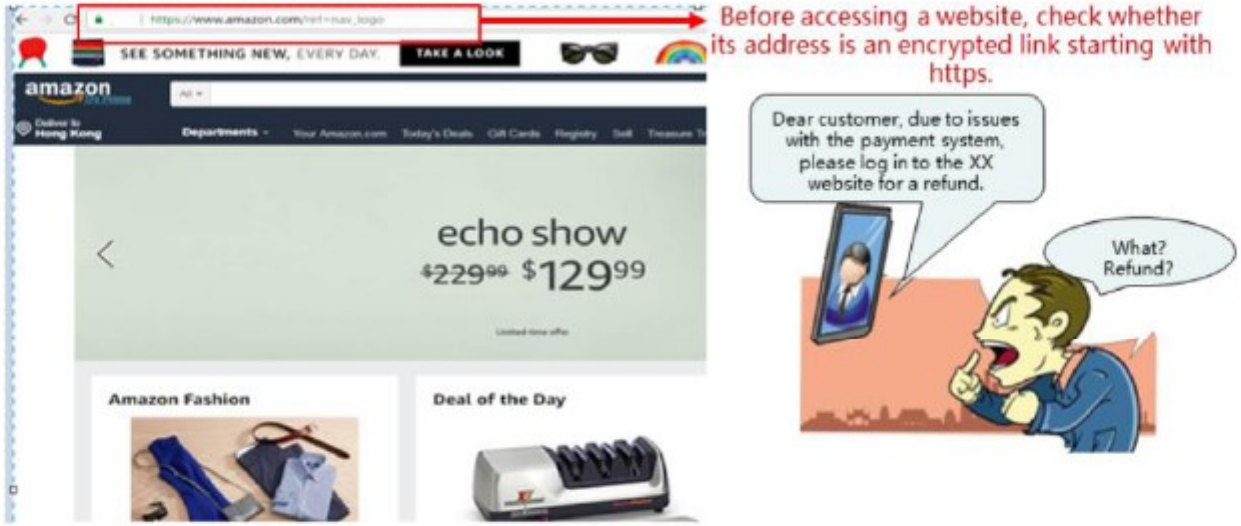
Injection

Cross-site scripting (XSS)

Malicious code propagation

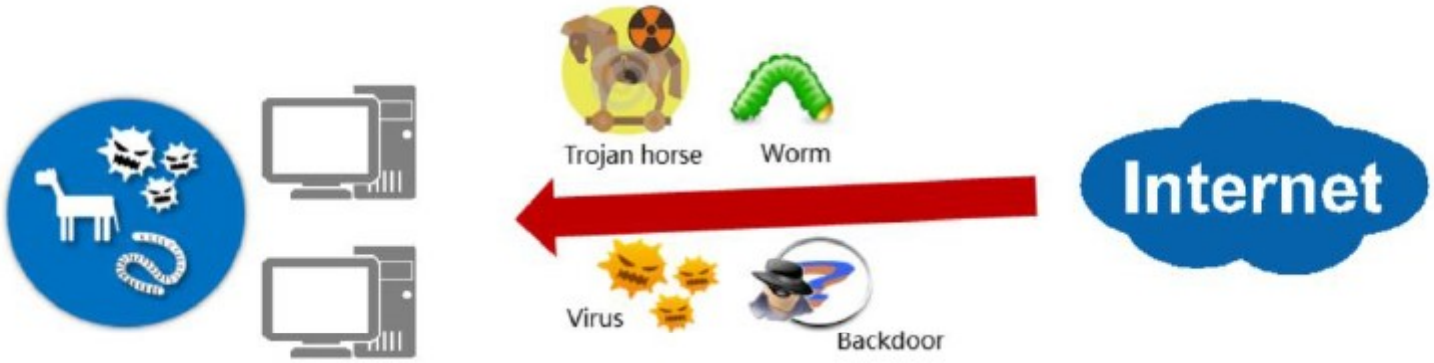
Data breach

Phishing



- "Phishing" is cyber fraud. It is the fraudulent attempt to obtain users' private information such as bank or credit card account and password, often for malicious reasons, by using the URL or web page content of an authentic website as disguise, or exploiting vulnerabilities of authentic website server programs to insert dangerous HTML code into some web pages of the website.

Malicious Code



- Malicious code is computer code that is deliberately developed or constructed to cause threats or potential threats to a network or system. The most common malicious code includes viruses, Trojan horses, worms, and backdoors.
- Malicious code is also called malware, which includes adware, spyware, and malicious shareware. Malware refers to software that is installed and run on a user's computer or other devices without explicitly notifying the user or obtaining the user's consent.

Defense Measures for Application Attacks

Regular vulnerability fixing
- Vulnerability scanning
- Patching

Improving information security awareness
- Constantly looking out for suspicious websites and links

Protection through professional equipment
- Firewalls
- WAF
- Antivirus software


Regular vulnerability fixing


Improving information security awareness

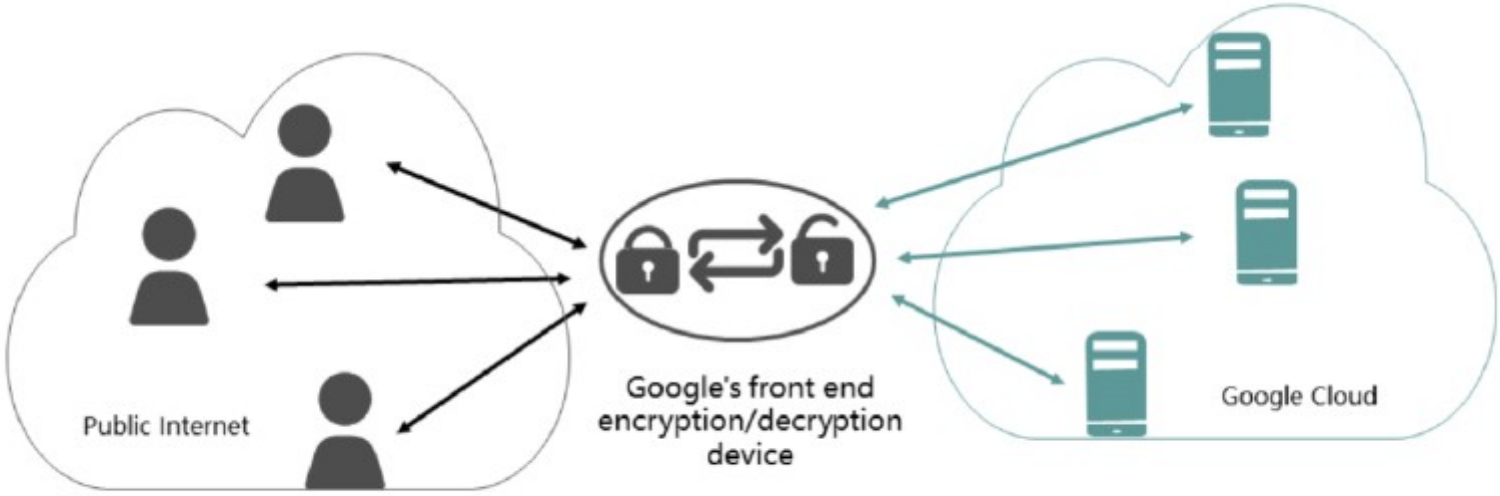

Protection through professional equipment

Contents

HUAWEI

Interception of User Communications

- The National Security Agency (NSA) U.S. listened to encrypted communication between Google (including Gmail) and Yahoo users on the cloud.
- The NSA exploited the encryption/decryption flaw of Google's front end server to circumvent the server and directly listen to backend plaintext data.



Tumblr User Information Breaches

- More than half of the accounts and passwords of the microblogging website Tumblr were stolen by hackers.
- Hackers invaded the Tumblr server in a certain way and stole information of Tumblr users. Tumblr stated that the breach would not cause damage to users because the database information was encrypted. However, the facts showed that the user information was encrypted using weak algorithms. After obtaining the encrypted user information, the hackers were able to quickly crack a large amount of user information.

Why are information breaches so frequent?

HUAWEI

Threats in Communication Process

What security risks will occur during communications?

Transmission security risks

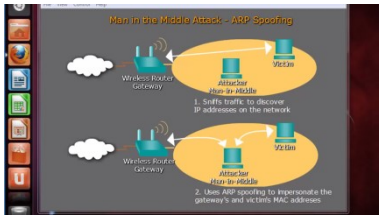
- MITM attacks
- Data transmission not encrypted or inadequately encrypted

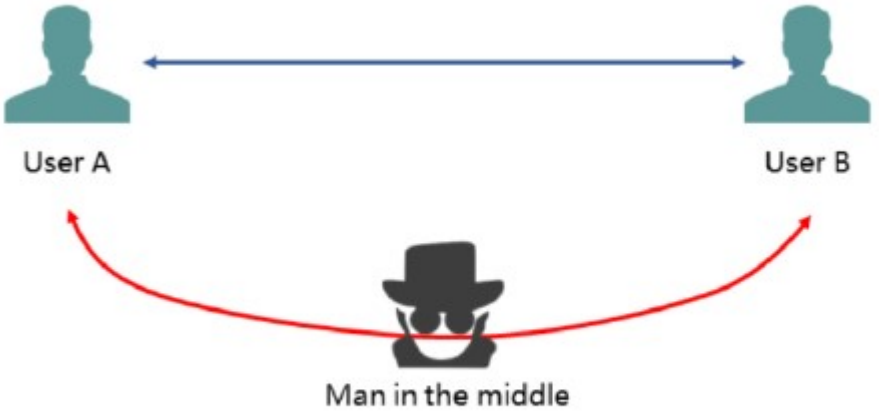
Device security risks

- Servers with vulnerabilities
- Users using weak passwords
- User identity not authenticated

MITM Attack

- Man-in-the-middle (MITM) attack: A type of indirect intrusion attacks. In MITM attacks, an attacker uses a variety of technical means to virtually place a controlled computer between two computers in the network. This controlled computer is called a man in the middle.
- Consequences of MITM attacks
  - Information tampering
  - Information theft





Information Not Encrypted or Inadequately Encrypted

- If information is not encrypted, information security may be compromised. However, even if data is encrypted, information may also be stolen and cracked.

Threat prevention suggestions

- Encrypt information before storage.
- Encrypt information before transmission.
- Use strong encryption algorithms.

Authentication Attack

- An attacker obtains a user's identity authentication information by certain means, and uses the identity information to steal sensitive information or carry out illegal acts. It is a common form of attack.
- Prevention suggestions
  - Install genuine antivirus software.
  - Use strong passwords.
  - Reduce the relevance between different passwords.