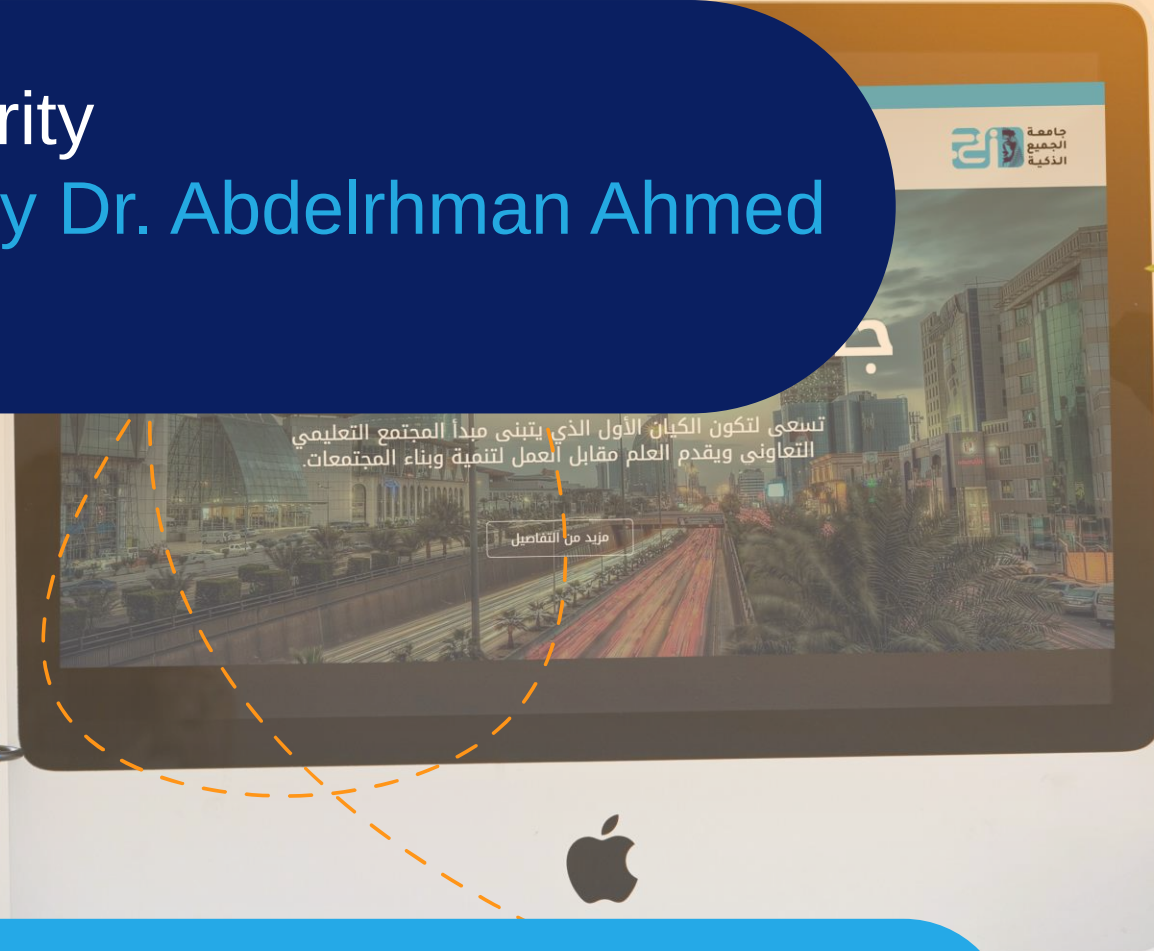


HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 4



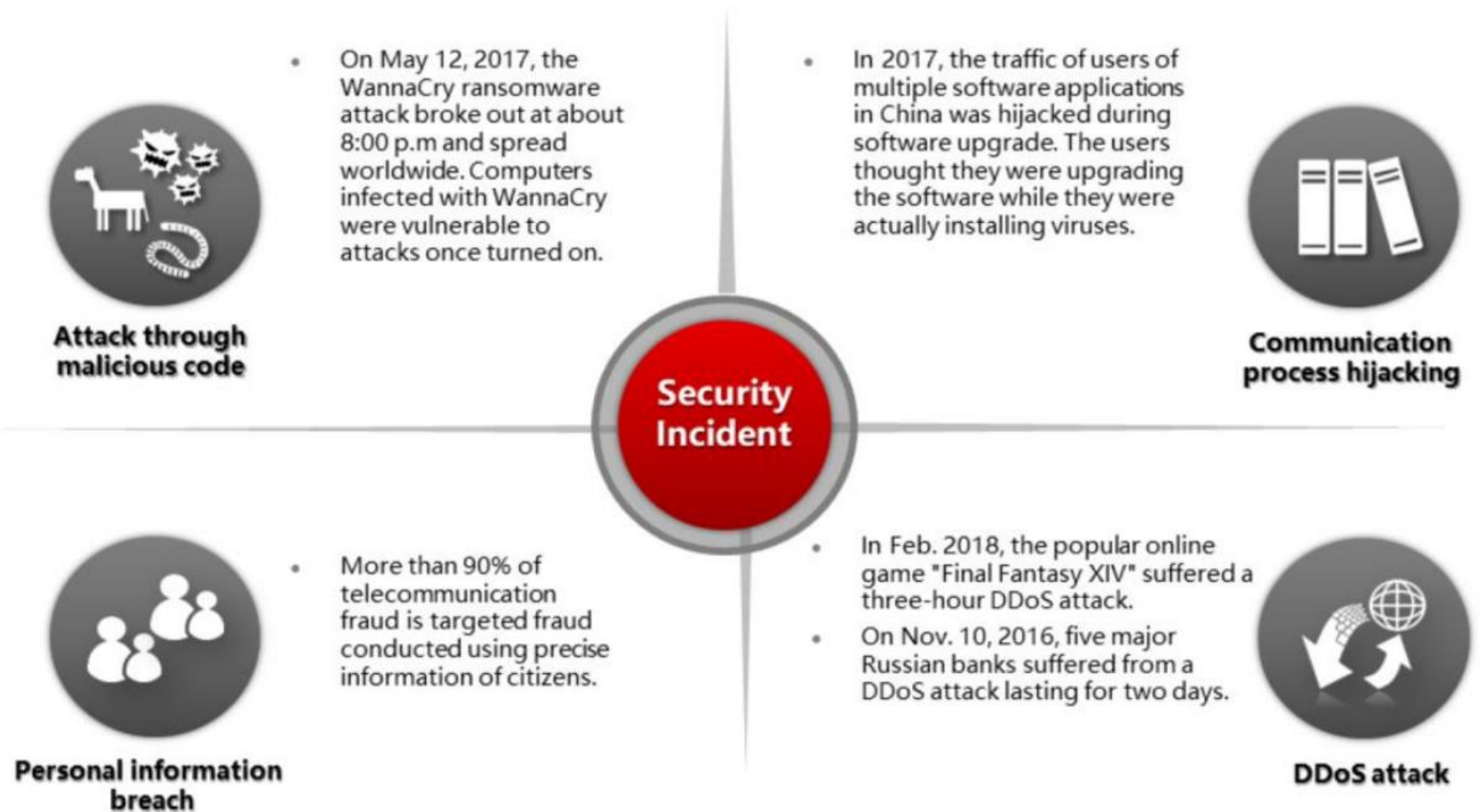
جامعة العنبر الذكية
EVERYONE'S SMART UNIVERSITY

Common Information Security Threats

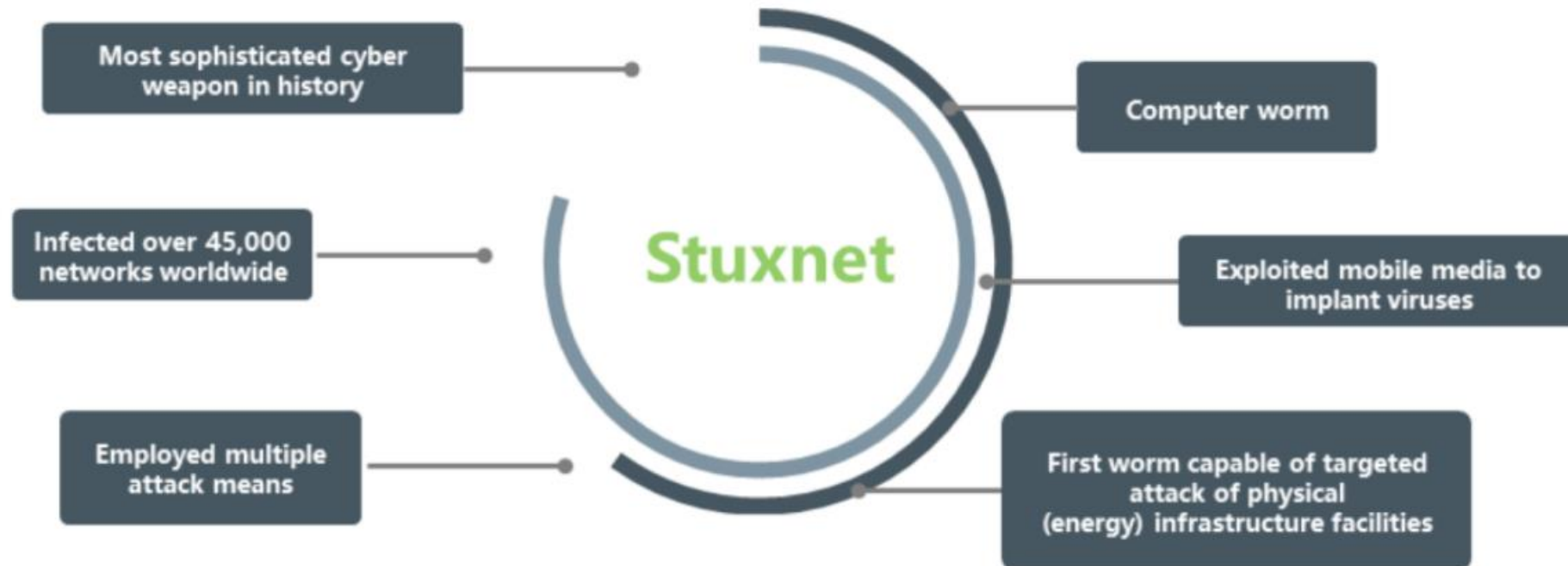
- **Information systems are often vulnerable and have sensitive, confidential information that needs to be communicated. Therefore, they are under threat in various scenarios and through various means.**
- **This class uses some case studies about common attacks to introduce possible threats to the information system.**

Objectives

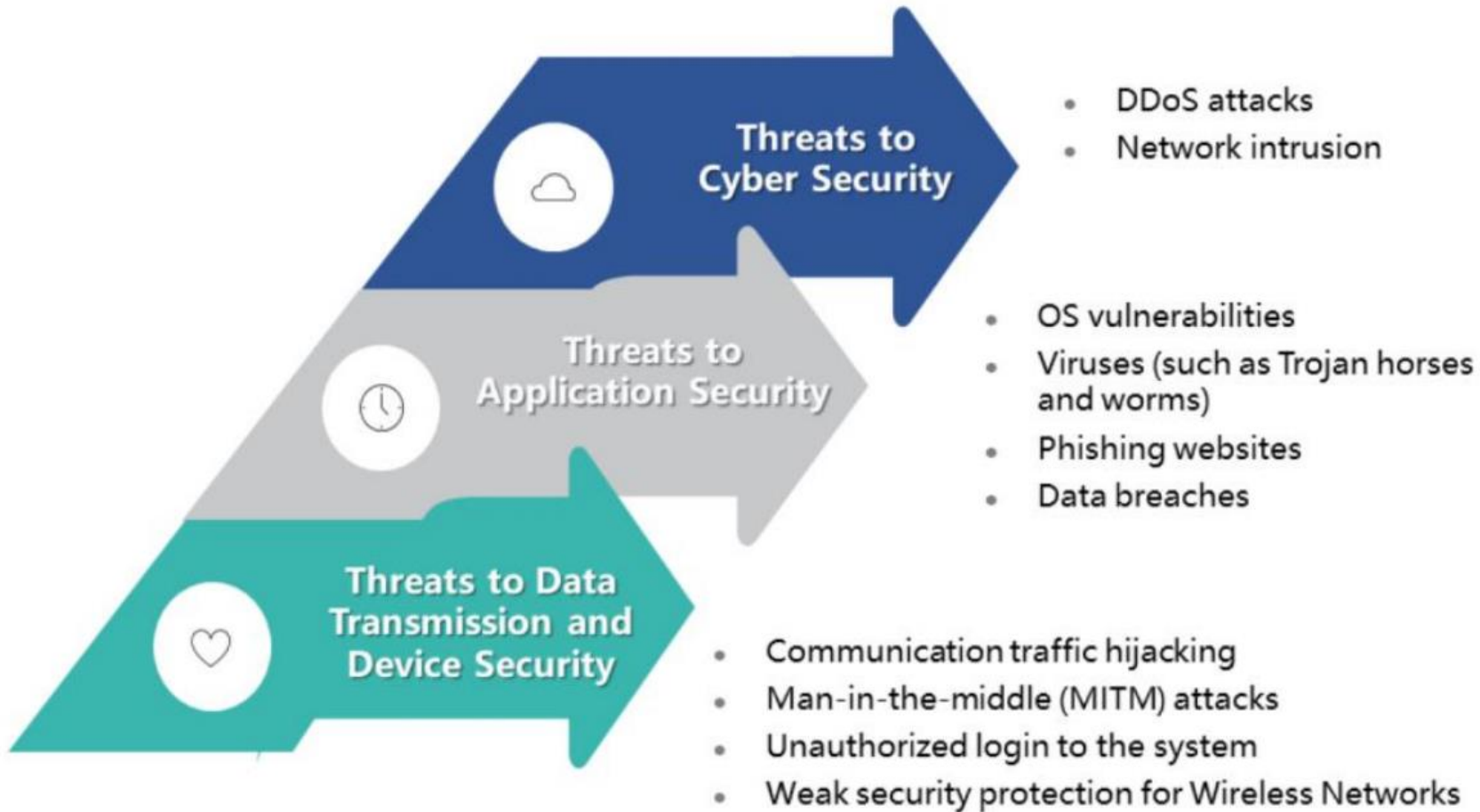
- **Upon completion of this course, you will be able to:**
 - ☐ **Categorize information security threats.**
 - ☐ **Describe common information security threat means.**



- 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.

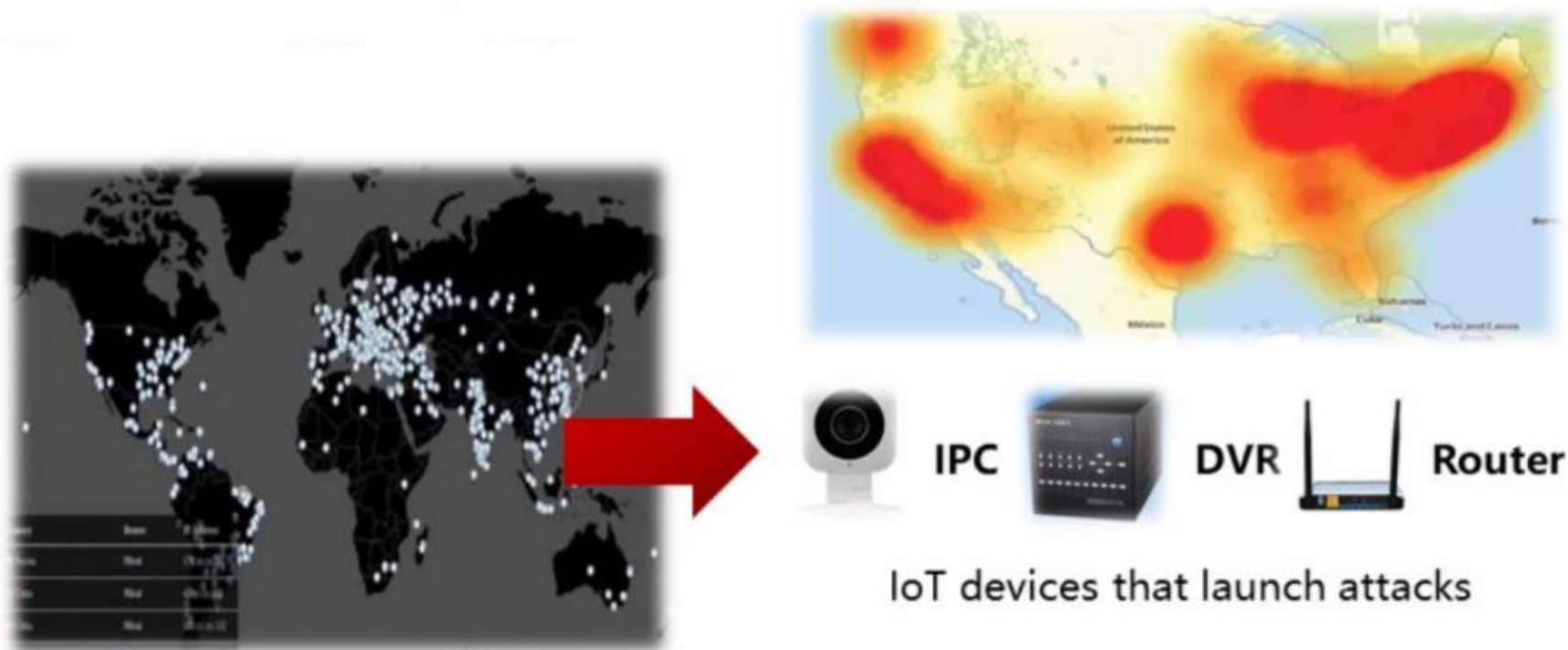




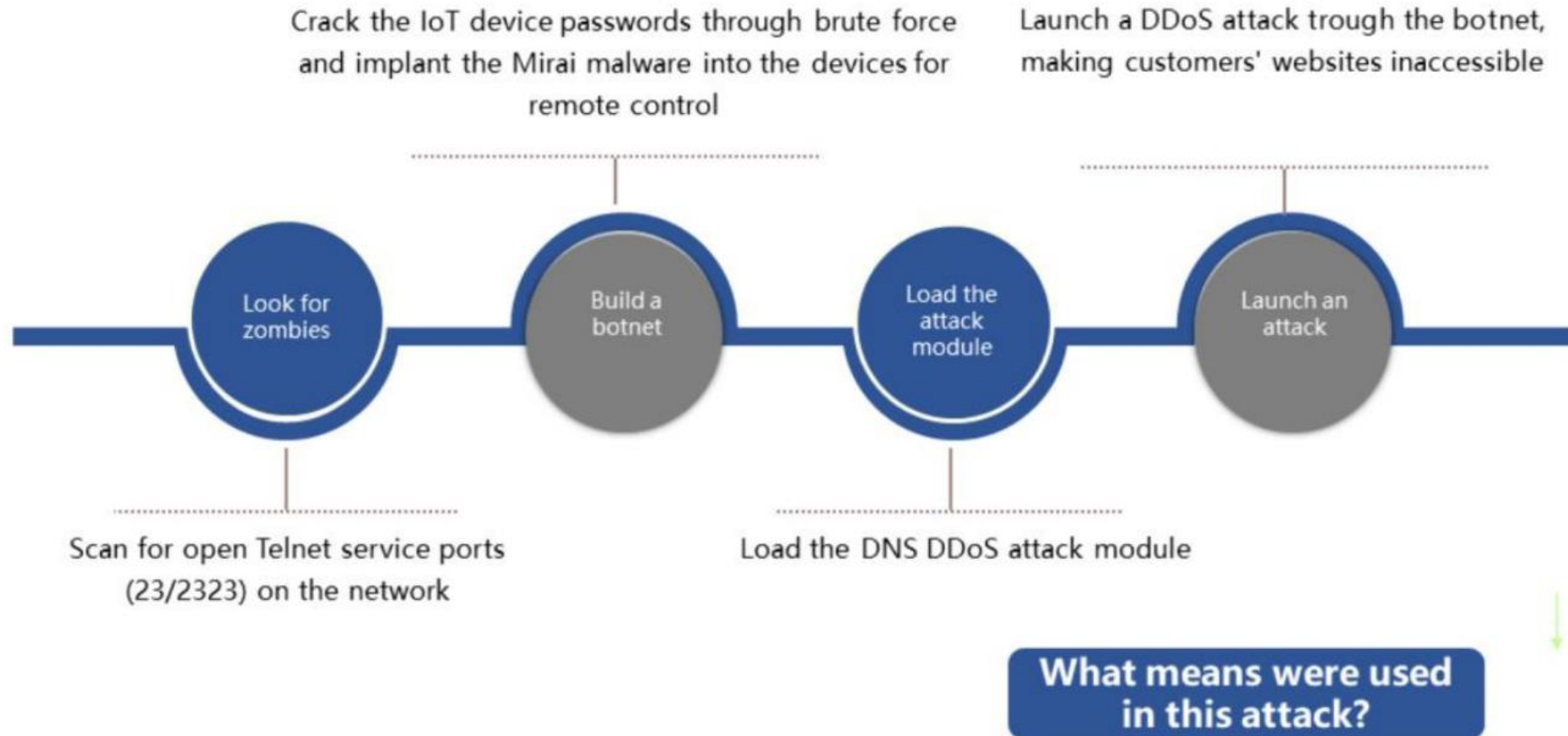


DDoS Attacks Against Dyn DNS Service in the United States

- 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 malwar



- Dyn is a DNS SaaS provider whose core service is providing managed DNS for its users. The DDoS attacks severely affected DNS services, preventing Dyn users from accessing their websites. Because Dyn serves many companies, the damage caused spread quickly, causing serious harm. More than 100 websites became inaccessible due to these attacks for as long as three hours. Amazon alone suffered a loss of tens of millions of dollars.
- The "zombies" launching the attacks mainly consisted of network cameras, digital hard disk recorders, and smart routers. The Mirai botnet infected millions of devices, of which only one tenth were involved in this attack.
- Currently, the Internet has many zombie hosts and botnets. Driven by the desire for profit, DDoS attacks have become a major security threat to the Internet.



- **Look for zombies:** By default, the remote login function is enabled for IoT devices to facilitate remote management of the administrators. An attacker can scan IP addresses to discover live IoT devices, which are then scanned for open Telnet ports.
- **Build a botnet:** Some IoT device users use the default password directly or set a simple password (a simple combination of username/digits, such as "admin/123456") for their devices. These passwords are easily cracked by an attacker through brute force. After successfully cracking the password to a IoT device and logging in to it through Telnet, the attacker remotely implants the Mirai malware into the IoT device to obtain absolute control over the device.
 - ❑ After obtaining absolute control over the infected devices, in addition to using the devices to launch DDoS attacks, the malware can also cause serious damage to the systems, services, and data of the devices. For example, the malware can tamper with data, steal privacy, modify configurations, and delete files, and may further attack core service systems.
- **Load the attack module:** The attacker loads the DNS DDoS attack module on the IoT device.
- **Launch an attack:** The attacker launches a DDoS attack against DNS service from Dyn in the United States through the botnet, bringing down hundreds of customer websites.

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

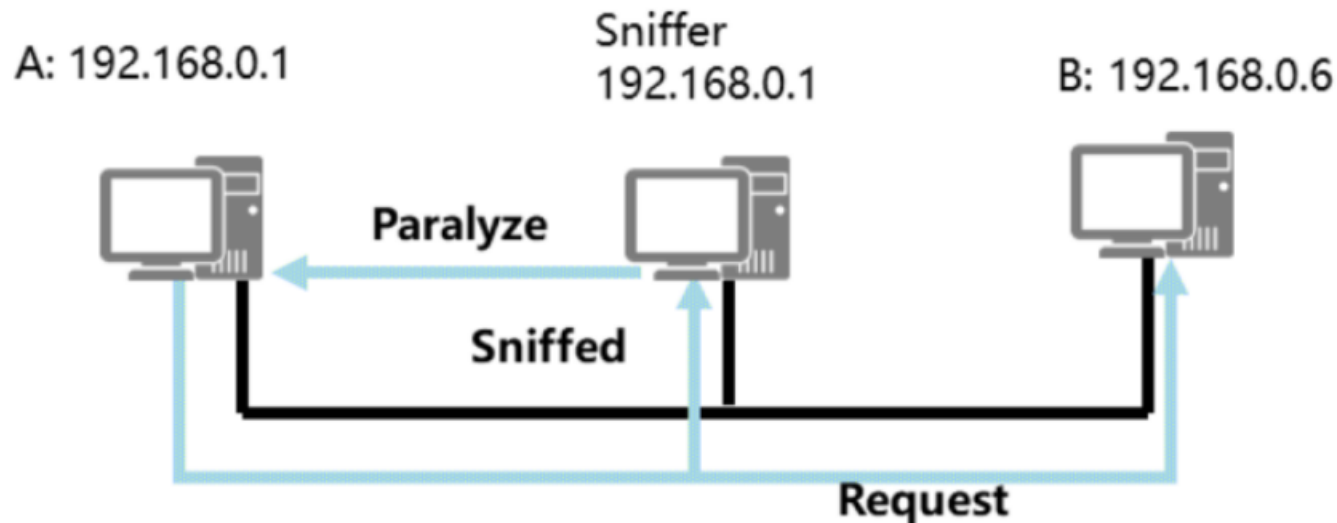
Address scanning

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.

Port scanning

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.

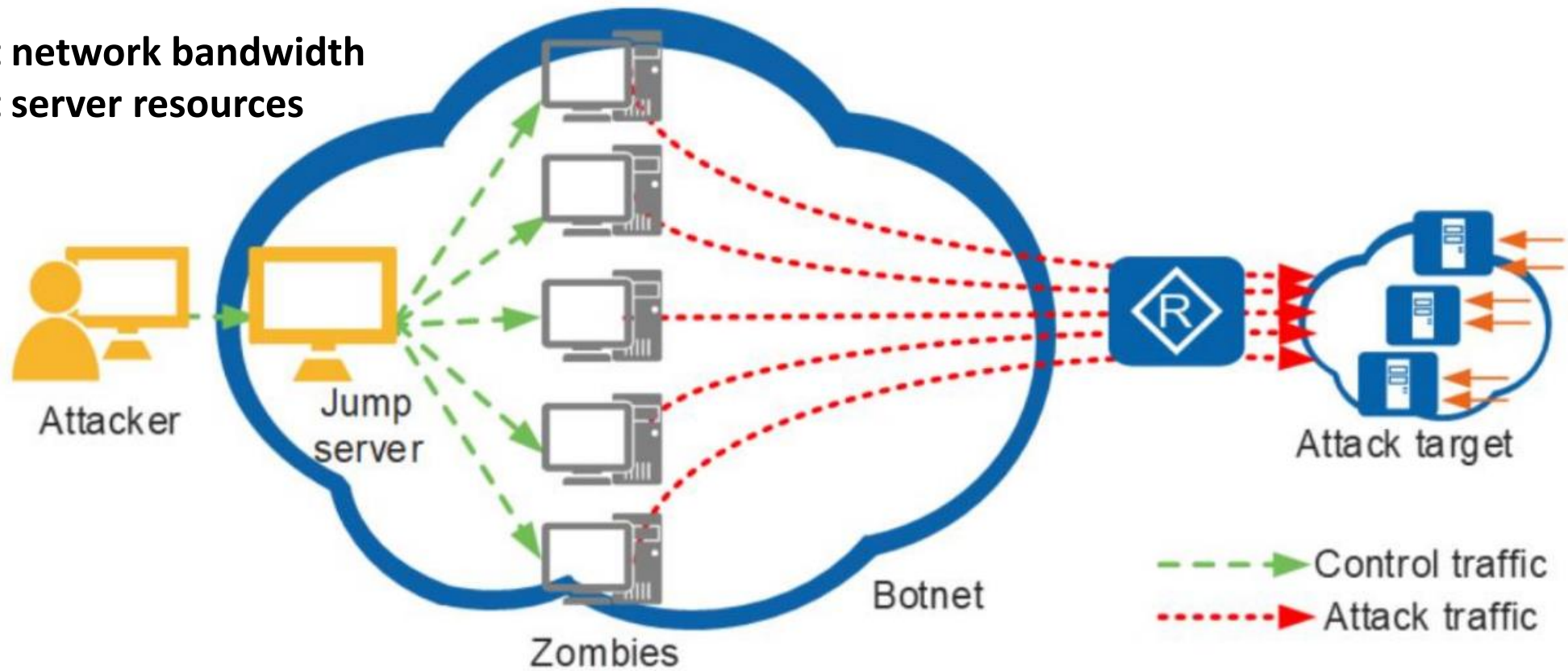
- Attackers can obtain the control permission by brute force cracking of passwords. Also, attackers can launch spoofing attacks such as IP spoofing to obtain access and control permissions.
- IP spoofing: An attacker may send packets with forged source IP addresses to target hosts to obtain superior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



- **IP spoofing is launched by exploiting the normal trust relationships between hosts. Hosts with IP address-based trust relationships use IP address-based authentication to determine whether to allow or reject the access of another host. Between two hosts with a trust relationship, users can log in to one host from another without password verification.**
- **The process of an IP spoofing attack is as follows:**
 - ❑ **Crash the network where a trusted host resides to launch the attack without resistance.**
 - ❑ **Connect to a port of the target host to guess the sequence and sequence increment value.**
 - ❑ **Masquerade the source address as the address of a trusted host and send a data segment with the SYN flag set to initiate a connection.**
 - ❑ **Wait for the target host to send a SYN-ACK packet to the compromised host.**
 - ❑ **Send the target host an ACK packet, with the source address masqueraded as the address of a trusted host and sequence number as that expected by the target host, plus 1.**
 - ❑ **After the connection is established, send commands and requests to the target host.**

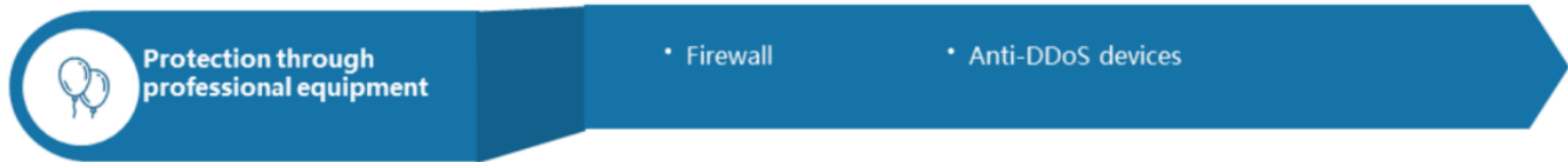
- DDoS attacks:

- ☐ Exhaust network bandwidth
- ☐ Exhaust server resources

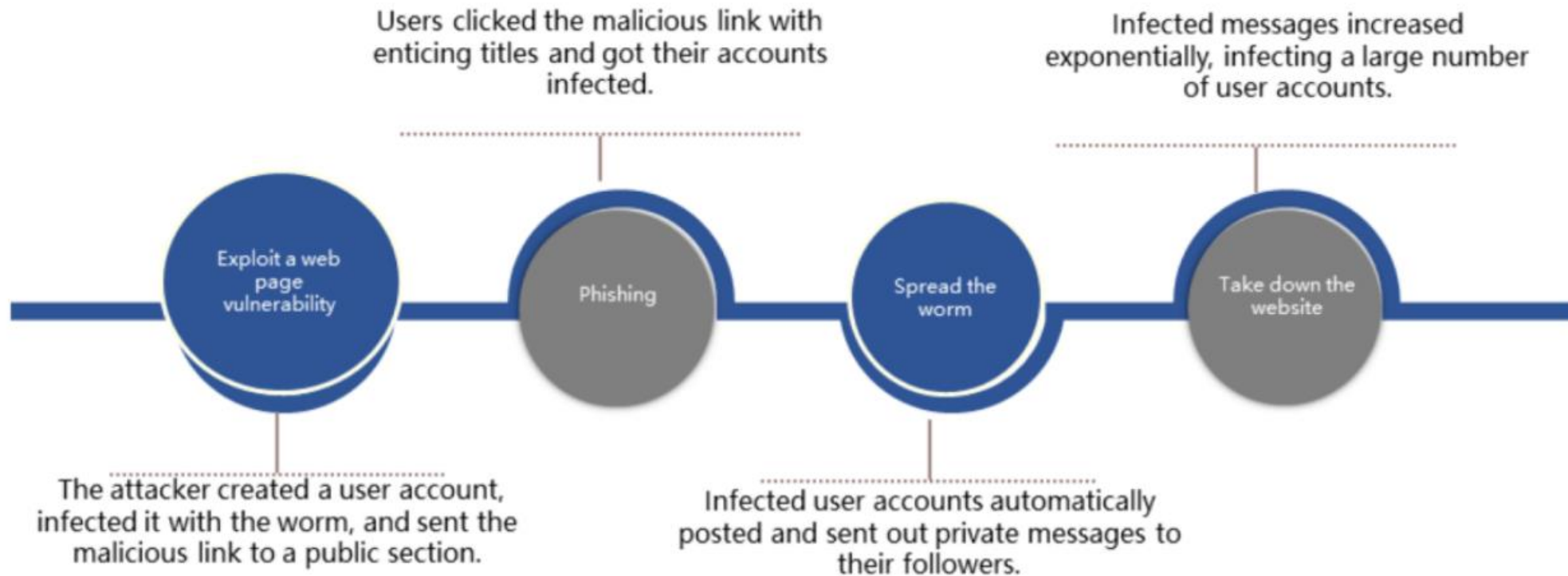


- A Distributed Denial of Service (DDoS) attack is a typical kind of traffic attack.
- In a DDoS attack, the attacker resorts to every possible means to control a large number of online hosts. These controlled hosts are called zombie hosts, and the network consisting of the attacker and zombie hosts is called a botnet. An attacker launches DDoS attacks by controlling many zombie hosts to send a large number of elaborately constructed attack packets to the attack target. As a result, links are congested, and system resources are exhausted on the attacked network. This prevents the attack target from providing services for legitimate users.
- DDoS attacks are divided into different types based on the types of exploited attack packets. Currently, popular DDoS attacks include SYN flood, UDP flood, ICMP flood, HTTP flood, HTTPS flood, and DNS flood.

- **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.



- 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:

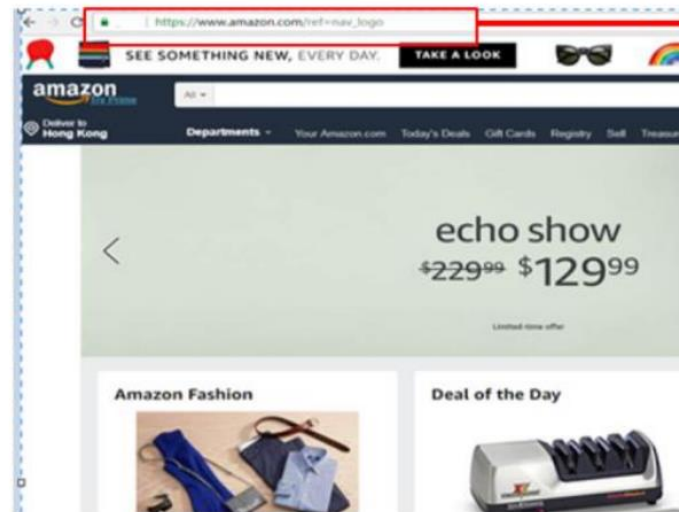


- Vulnerabilities are defects in the implementation of hardware, software, or protocols or in system security policies. They allow attackers to access or damage systems without authorization.
- If system vulnerabilities are not fixed in time, the following attacks may occur:



- The most common means of launching an SQL injection attack is to construct elaborate SQL statements and inject them into the content submitted on web pages. Popular techniques include using comment characters, identical relations (such as $1 = 1$), JOIN query using UNION statements, and inserting or tampering with data using INSERT or UPDATE statements.
- Cross-site scripting (XSS) is a type of code injection attack launched by exploiting security vulnerabilities of website applications. It allows malicious users to inject code into web pages to compromise users who view the pages. This type of attacks often involves HTML and client-side scripting language.

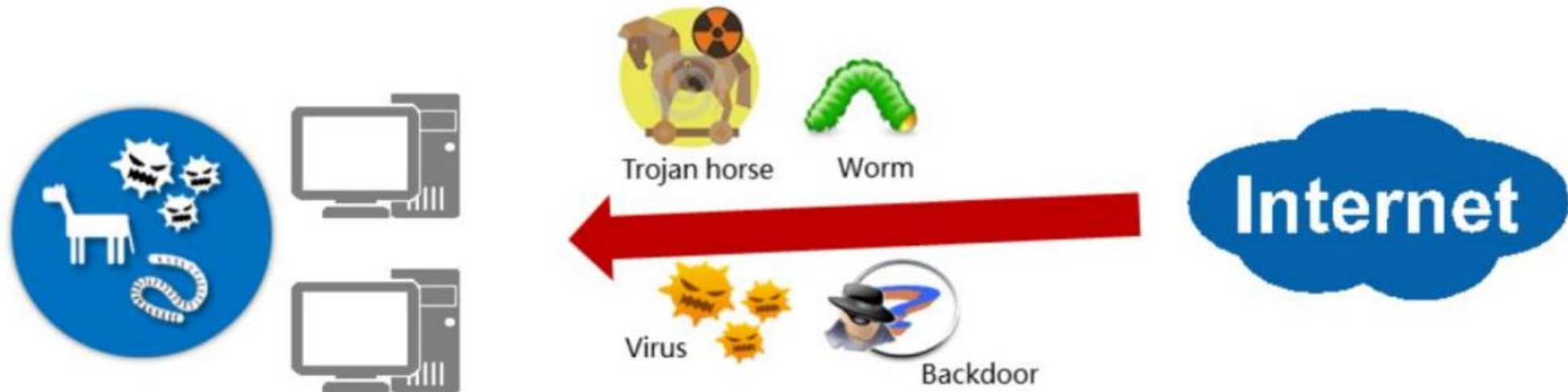
- "Phishing" is cyber fraud. It is the fraudulent attempt to obtain users' private information such as bank or credit card account and password, often for malicious reasons, by using the URL or web page content of an authentic website as disguise or exploiting vulnerabilities of authentic website server programs to insert dangerous HTML code into some web pages of the website.
- Phishing websites are generally divided into two types: The first type uses the idea of "winning a prize" as the bait to trick the user into providing sensitive information such as ID card number and bank card details; the second type uses a fake website masquerading as a genuine online bank or electronic transaction website to steal users' information such as bank card details or payment passwords to online accounts. The whole process is like fishing, giving these malicious websites the name "phishing websites". The phishing techniques are simple. They take advantage of people's desire for cheap prices or weak anti-fraud awareness. Once a user gets duped, his/her personal privacy information will be leaked and sold; or the attacker may use the bank card details provided by the user on the fake website to immediately steal the user's online assets.



Before accessing a website, check whether its address is an encrypted link starting with https.



- 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.



- Web browsing and email transmission are the main ways for viruses, Trojan horses, and spyware to access intranets.
- **Virus:** a set of instructions or program code compiled by an attacker by exploiting inherent vulnerabilities of computer software and hardware. A computer virus, when executed, replicates itself by modifying other computer programs and inserting its exact copies or possible evolutions to infect other programs, thereby damaging the computer systems and tampering with and compromising service data.
- **Trojan horse:** a malicious computer program exploited to control another computer. A Trojan horse usually has two executable programs: One is the client (the controller) and the other is the server (the controlled part). The "server" is implanted into a target computer, and the "hacker" refers to a computer that uses the "controller" to enter the computer that runs the "server". After the infected computer starts running, a Trojan horse "server" will open one or several ports, allowing hackers to not only steal important information on the computer but also damage internal computers.

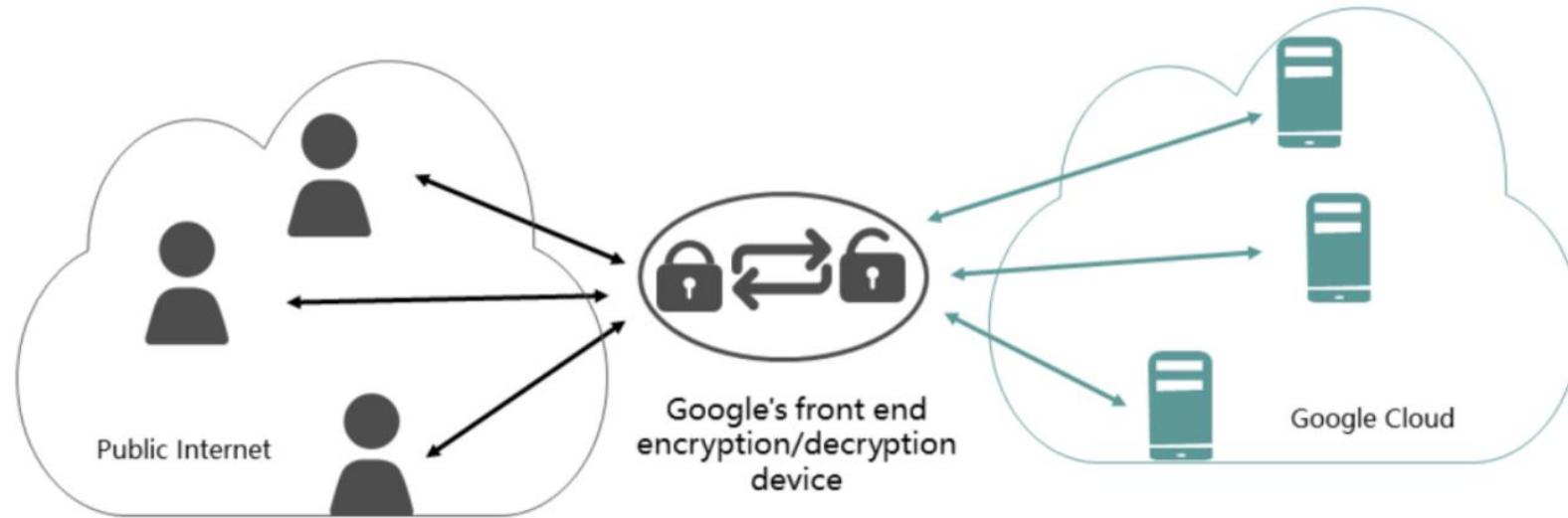
- **Worm:** a malicious program that can exploit the system vulnerabilities to propagate itself throughout the network. It uses the network to replicate and propagate itself through networks and emails. Major damage caused: A worm can consume host resources and even damage the host system, which may lead to DoS. Also, worm propagation causes network congestion. It may even cause the entire network to break down and become out of control.
- **Backdoor:** a covert function hidden in the program. It is usually designed by the programmer for convenient access to the system in the future.
- **Spyware:** a software program that allows attackers to install backdoors on users' computers without users' knowledge to collect user information. It collects, uses, and disseminates sensitive information of enterprise employees, severely affecting the normal business of enterprises.

- Using professional tools for vulnerability scanning and restoration on systems or personal computers can prevent virus intrusion and infection to a certain extent.
- As a border device, the firewall can block unauthorized network access, web page and email viruses, illegitimate applications, etc., to protect the intranet.
- WAF is short for Web Application Firewall. It is a protection device that protects web applications by executing a series of HTTP/HTTPS security policies.



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

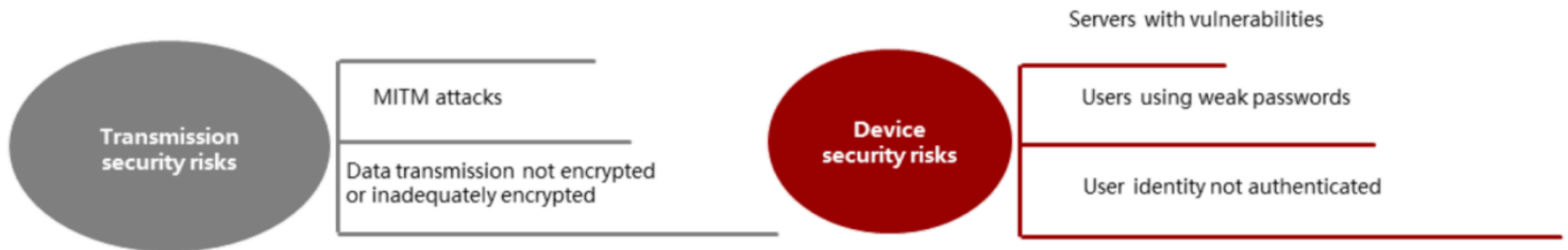
- More than half of the accounts and passwords of the microblogging website Tumblr were stolen by hackers.
- Hackers invaded the Tumblr server in a certain way and stole information of Tumblr users. Tumblr stated that the breach would not cause damage to users because the database information was encrypted. 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?



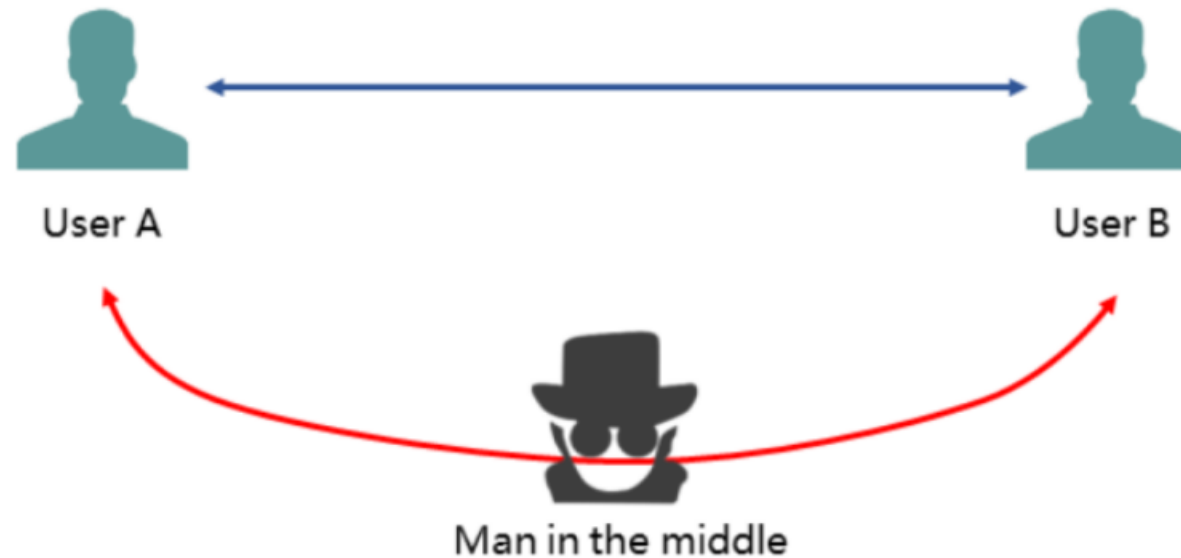
What security risks will occur during communications?



- **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.

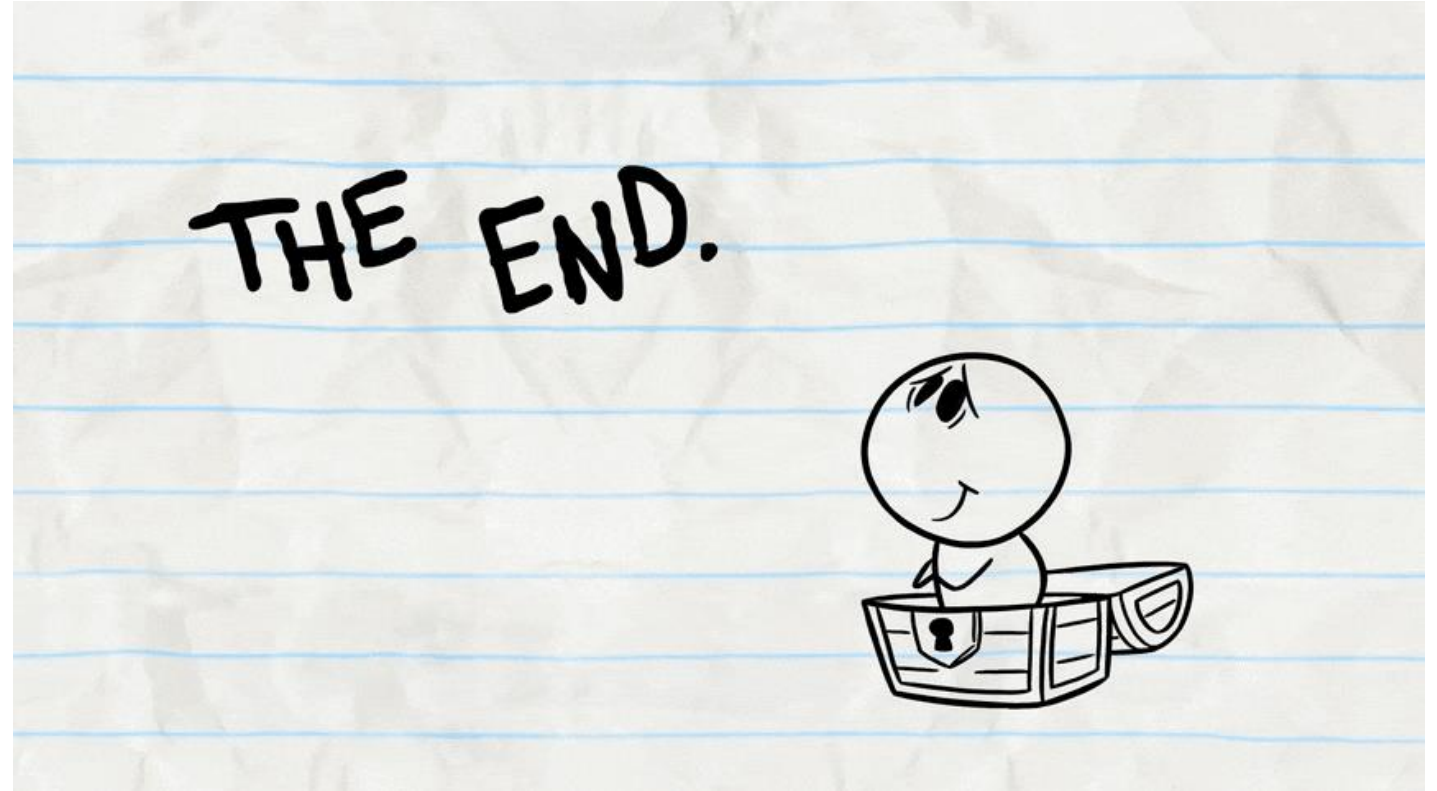
- An attacker obtains a user's identity authentication information by certain means, and uses the identity information to steal sensitive information or carry out illegal acts. It is a common form of attack.
- Prevention suggestions:
 - ❑ Install genuine antivirus software.
 - ❑ Use strong passwords.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



The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY