

Information System Security

Information System Threats

Summary

- ▶ **History of hacking**
- ▶ **The different kinds of malwares**
- ▶ **The different kinds of cyber attacks**
 - Hacking
 - Denial-of-service attacks
 - Cryptography attacks
 - Technical attacks
 - Web vulnerabilities attacks
 - Fraud

History of hacking

► 1982: the first virus for Apple II and first worm

- The first virus "Elk Cloner" is developed by an American student.
- It runs on an Apple/DOS 3.3 computer.
- The principle: it displays fake screens or reversed screens and clicking noises.
- It is distributed via floppy disks.



► Jon HEPPS and John Shock develop the first worm in the Xerox Alto Research Center.

- They are used for distributed computing and automatically propagate to network level.
- Due to a programming error, this propagation takes place uncontrollably and quickly causes the computer paralysis

History of hacking

► 1986: First track of viruses on PCs

- The first computer virus to have massively attacked computers is "Brain", it infects only floppy disk 5 1/4 inches.
 - ✓ It pretends to be a defective element of the disk, so it is ignored.
 - ✓ Brain carries a message that is never displayed, but can be seen with a binary editor. The virus slows down the floppy disk drive and makes seven kilobytes of memory unavailable to DOS.

► 1988 : First Internet worm

- Robert Tappan Morris created the first Internet worm the "Morris Worm" or "Great worm".
 - ✓ The virus can resettle on an already infected system, it causes major disruptions. 10% of Internet computers (6 000) were infected.
 - ✓ This is the beginning of the first penalties for virus creators. Robert Tappan Morris was sentenced to more than 10 thousand dollars fine and 400 hours of community service. He is now a professor at MIT.

History of hacking

► 1996 : The first virus for Linux

- “Staog,” appeared in October 1996.
 - ✓ It installs itself in kernel memory and can infect files regardless of what user or privilege level.
 - ✓ Staog is not known to have ever been wild, and it had no destructive payload, so it likely never caused any damage.



History of hacking

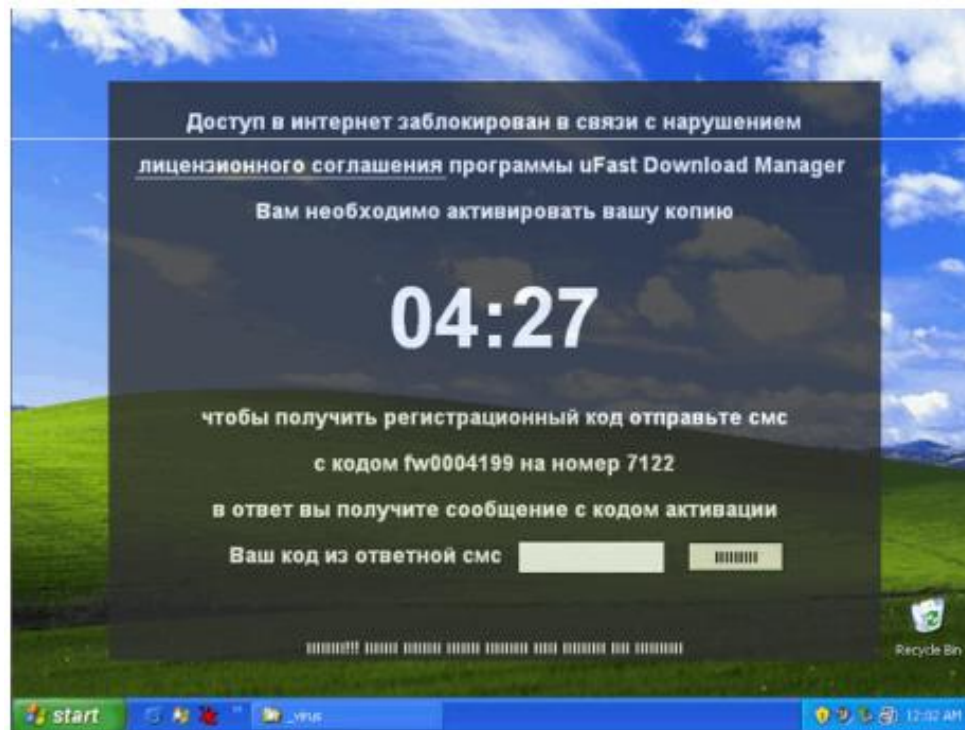
► 1998 : Macro and Java viruses

- “Laroux” is the first wild Excel virus detected. It was found in oil companies which were paralyzed by this virus.
 - ✓ This new macro virus settles into Excel tables.
 - ✓ The virus infects any Excel workbook saved or accessed.
- Word and PowerPoint are also victim of macro viruses.
- Java.StrangeBrew
 - ✓ Appearance of the first virus in Java code.
- Email is the vector of 85% of viruses.

History of hacking

► 2006: Cyber extortion

- Ransom with threat of destruction of information
- Restitution in exchange for payment



History of hacking

► 2007: cyberattack

➤ Cyberattack in Estonia

- ✓ On April 27, some Russian leading a DoS attack on the Estonian Internet networks
- ✓ Government websites are not accessible followed by banks, emergency services, etc.
- ✓ The attack causes riots



History of hacking

► May 2017: Wannacry

➤ Ransomware for Windows systems

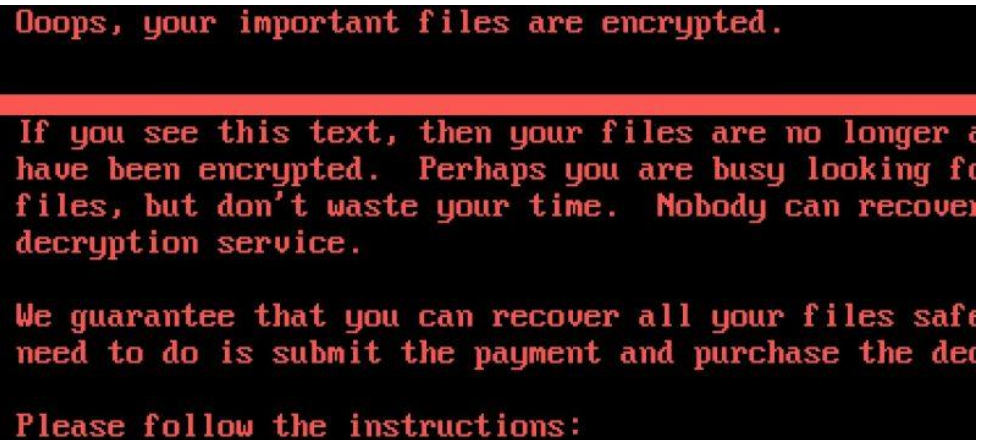
- ✓ Infected more than 300 000 computers in over 150 countries
- ✓ It propagates using EternalBlue (exploit of Windows SMB protocol) developed by the NSA (National Security Agency). It was leaked by the Shadow Brokers hacker group on April, 2017
- ✓ It is considered a network worm because it also includes a "transport" mechanism to automatically spread itself → it spreads out to random computers on every networks (local or Internet)
- ✓ French automobile manufacturer Renault was infected and had to stop the production in many factory to isolate and clean up infected computers
- ✓ The day after the initial attack in May, Microsoft released emergency security patches for end of life products (Windows XP, Windows Server 2003 and Windows 8)



History of hacking

► June 2017: Not Petya

- Wiper (delete data) masquerading as ransomware
 - ✓ It was designed to cause maximum damage, with Ukraine being the main target
 - ✓ The attack originated from an update of a Ukrainian tax accounting package called MeDoc → the attack was installed on an estimated 1 million computers in Ukraine
 - ✓ Like the WannaCry attack, NotPetya uses the EternalBlue exploit
 - ✓ NotPetya encrypted all of the files on the infected computers but didn't allow the decryption
 - ✓ French construction materials company Saint-Gobain was infected



Oops, your important files are encrypted.

If you see this text, then your files are no longer safe and have been encrypted. Perhaps you are busy looking for files, but don't waste your time. Nobody can recover your files without a decryption service.

We guarantee that you can recover all your files safely. The only need to do is submit the payment and purchase the decryption service.

Please follow the instructions:

History of hacking

► January 2018: Meltdown and Spectre Attack



- Meltdown and Spectre are 2 hardware vulnerabilities affecting microprocessors



- The exploit is viable on most major operating system (Windows, Linux, MacOS)
 - ✓ Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack **allows a program to access the memory**, and thus also the secrets, **of other programs and the operating system.**
 - ✓ Spectre **breaks the isolation between different applications.** It is a vulnerability with implementations of branch prediction by allowing malicious processes access to the contents of other programs' mapped memory
 - A website can read data stored in the browser for another website, or the browser's memory itself.

Different kinds of malwares

► Keyloggers: knowing the activity of the infected computer

- The software stores into a file all the keys you type on your keyboard or the moves of your mouse
- This can be done by:
 - ✓ Insertion of a device into the keyboard,
 - ✓ Video observation,
 - ✓ Intercepting incoming and outgoing requests,
 - ✓ Replacement of the keyboard driver,
 - ✓ Interception of the function in the kernel (misuse of the function code),
 - ✓ Script in an application (javascript)
- The file, often encrypted, is then repatriated by the malicious person who installed the malware
- Objectives: to get your passwords, logins, or information about you
- Solution : Strong authentication and antivirus



Different kinds of malwares

■ Virus

- A virus is a program which is self-reproduced by **infecting other programs**
- It must be run **manually**
- It is often written in assembler and fits into a normal program, mostly at the end
- Every time the user executes this "infected" program, it activates the virus that takes advantage of it to **integrate into other executable programs**
- Moreover, when it contains a payload, it can, after a certain time (which may be very long) or a particular event, perform a **predetermined action**
- This action can range from a simple harmless message to the deterioration of certain functions of the operating system or the deterioration of some files or even the complete destruction of all the data of the computer ("logic bomb")



Different kinds of malwares

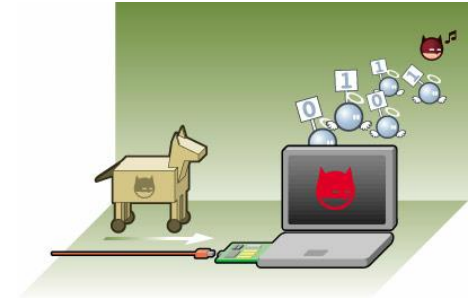
■ Worms

- A worm, unlike a computer virus, does not need a host program to reproduce. It exploits the different resources of the computer that hosts it to ensure its reproduction
- The goal of a worm is not just to reproduce itself. The worm also usually has a **malicious purpose**, for example:
 - ✓ Spying on the computer where it is located
 - ✓ Offer a backdoor to hackers
 - ✓ Destroy data on the computer where it is located or cause further damage
 - ✓ Send multiple requests to an Internet server in order to saturate it (DoS)
- The activity of a worm often has side effects like:
 - ✓ The slowing down of the infected machine
 - ✓ The slowing down of the network used by the infected machine
 - ✓ The crash of services or the operating system
- **Parades : updates and antivirus**

Different kinds of malwares

► Trojan

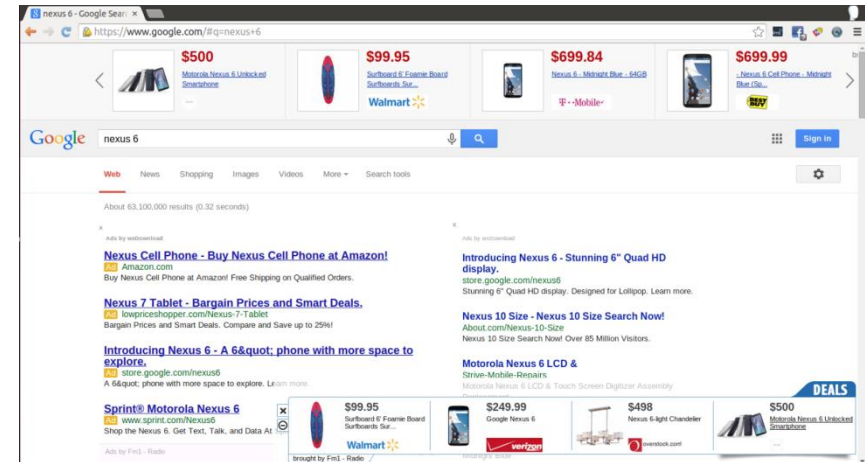
- The Trojan horse is apparently legitimate software, but contains malicious functionality
- The program inside the Trojan (or downloaded automatically) is called the "payload". It can be any kind of malware : virus, keylogger, spyware...
- The only aim of those programs is to benefit a third party the resources of your computer
 - ✓ For example, give a shell or manipulate devices
 - ✓ The attacker can bounce from your computer to other computers in the same network
- The cracked software can be Trojans that will attract the Internet user who tries to obtain free software that is not free



Different kinds of malwares

Adware

- Advertising software usually contains two parts:
 - A useful part (usually a video game or a utility) that prompts a user to install it on his computer
 - A part that manages the display of advertising
- Objectives: make you come on a web site, show you some ads (which pay the creator of the adware) and potentially steal you some information about your private life
- Usually not really aggressive, it modifies start-up page of your browser or sets up a plug-in for searching on the web
- Techniques of new adwares can be close to malware changing the DNS servers on the computer (Trojan.DNSChanger) to redirect advertisements towards advertising agency controlled by the adware editor
- Solutions : antivirus



Different kinds of malwares

► Downloaders

- Close to trojan : it installs itself to the system and waits until an Internet connection becomes available to connect to a remote server or website in order to download additional programs (usually malware) onto the infected computer
- It secretly downloads malicious files from a remote server, then installs and executes the files
- Downloaders may be distributed as a file attachment to spam e-mails
 - ✓ The attached programs are typically labelled using legitimate-sounding program or document names, such as 'invoice' or 'accounts.exe', as a simple form of social engineering
 - ✓ On opening the file attachment, the Trojan-Downloader is installed

Different kinds of malwares

■ Rootkits

- A rootkit is a collection of computer software, typically malicious, designed to **enable access to a computer** or gain privileges while at the same time **masking its existence** or the existence of other software
- Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it
- Most rootkits are used to install malware on machines where access is obtained
- Objectives
 - ✓ To benefit a third party the resources of your computer
 - ✓ To spy : to access the data stored or in transit on the target machine
- Solutions :
 - ✓ Integrity check
 - ✓ Antivirus

Different kinds of malwares

- **All these malwares are made through vulnerabilities and associated attacks**
 - The vulnerabilities are increasing significantly for the following reasons :
 - ✓ No security in the projects (security is often added later)
 - ✓ Complexity of the information system
 - ✓ Marketing requirement (the software must be delivered at a specific date)
 - ✓ Too fast evolution of technologies

Different attacks

► Different kinds of attacks exist:

- Hacking
- Denial-of-service attacks
- Cryptography attacks
- Technical attacks
- Web vulnerabilities attacks
- Fraud

Hacking

► The exploits

➤ Principle

- ✓ An « exploit » is a computer program which exploits a vulnerability
- ✓ Each exploit is specific to a version of an application because it enables to exploits its vulnerabilities

➤ Aims

- ✓ Privilege escalation
- ✓ System takeover
- ✓ Cause a system error

➤ How to avoid

- ✓ Keep watching software news to know the new vulnerabilities and update the system and the applications

Creation of an exploit

Script

- Hackers rely on vulnerabilities to develop a software (or a script) which enable to use them

Payload

- Once the script which enables to exploit a vulnerability is written, hackers insert a « payload » (a part of the script which makes the malicious action)
- Example : data destruction, display of a message, spam mailing, opening of a shell...

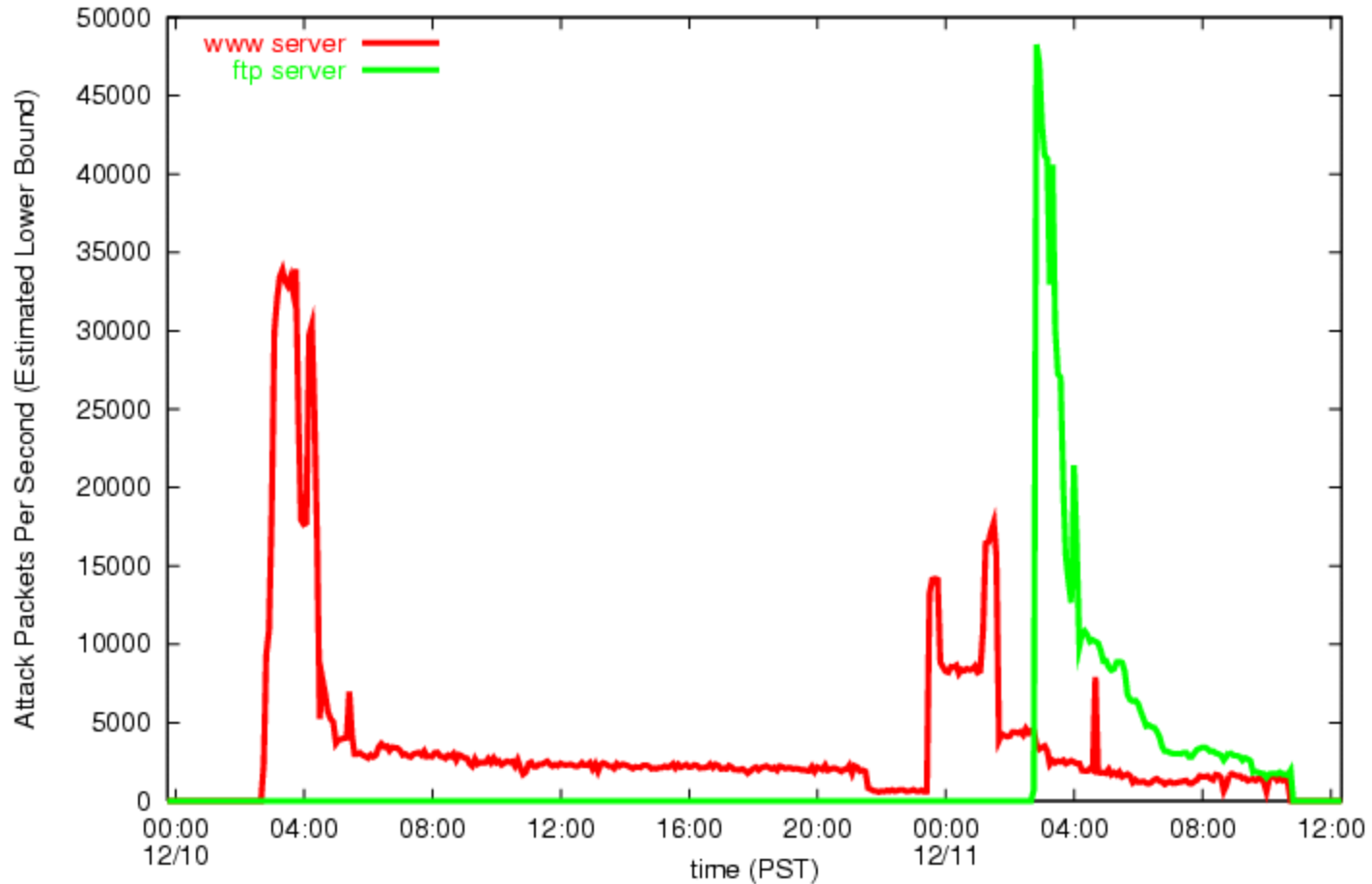
Distribution

- They just have to distribute the malicious software or to attract their targets on trapped web sites

Vulnerabilities commonly used for hacking

- ▶ **Buffer overflow** : exceeds the area allocated by the local buffer variable
- ▶ **Heap overflow** : Can inject data in the variables allocated dynamically when running a program
- ▶ **Integer overflow** : Numerical value greater than the available storage space
- ▶ **Stack overflow** : Overwrites program areas outside the stack
- ▶ **Code injection** : sends untrusted data to an interpreter

Denial-of-service attacks



Denial-of-service attacks

► Distributed denial-of-service (DDoS)

- Principle
 - ✓ Mute a server by overflowing with useless traffic which comes from many computers
- More complex to implement because you need many computers to attack and submerge the server (botnet)
- The classical tool is composed with a master (command-and-control server) and many distant hosts (daemons). The hacker connects to the C&C and send an order to all his demons to attack a particular target with the method he chooses
- Nowadays, botnets can be composed with thousands of computers (average size : 20 000 computers)

Example of DDoS attack



1. A botnet operator sends out viruses or worms, infecting ordinary users' computers, whose payload is a malicious application — the *bot*
2. The *bot* on the infected PC logs into a particular C&C server
3. A malicious person purchases the services of the botnet from the operator
4. The malicious person provides the target to the operator, who instructs the compromised machines via the control panel on the web server, causing them to send out requests to the targeted service.

Cryptography attacks



Side-Channel Attacks

- ▶ In cryptography, we can review facts and infer the value of an encryption key
- ▶ It is possible to detect how much power consumption is used for encryption and decryption (the fluctuation of electronic voltage)
- ▶ It is also possible to intercept the radiation emissions released and then calculate how long the processes take
- ▶ Looking around the cryptosystem, or its attributes and characteristics, is different from looking into the cryptosystem and trying to defeat it through mathematical computations
- ▶ In 1995, RSA private keys were uncovered by measuring the relative time cryptographic operations took

Man In The Middle (MITM) attacks

► Principle

- The hacker has to be able to observe and intercept messages from a victim to another one

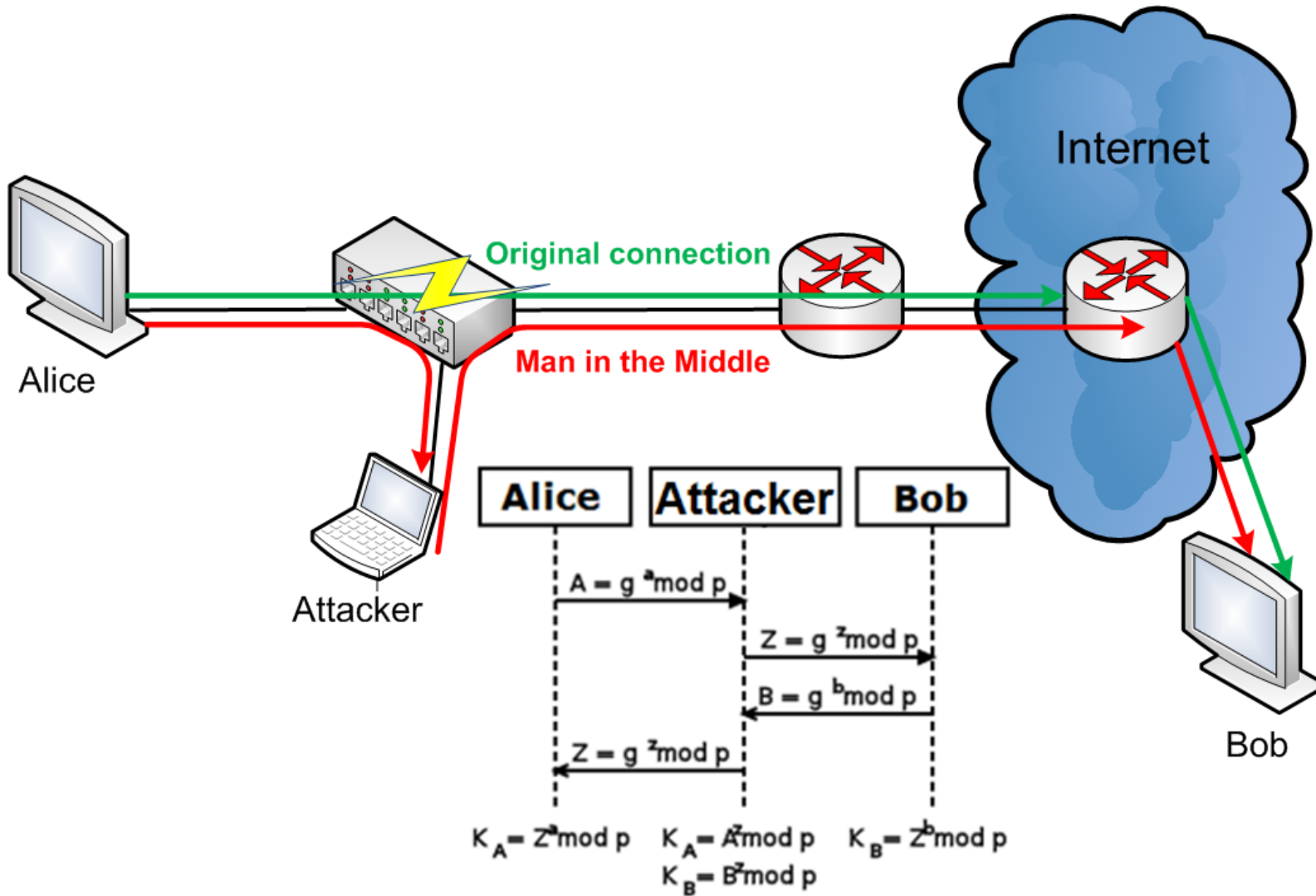
► Objective

- Intercept communications between the two people, without the two people noticing that the communication channel was compromised

► During the exchange of public keys, if the man in the middle succeeds in replacing the exchanged public keys with his own public keys, he would be able to intercept all the messages, to decrypt them with his private keys and to sign them

► The role of a public key infrastructure (PKI) is to certify that the public keys correspond to both parties

Example of a MITM attack



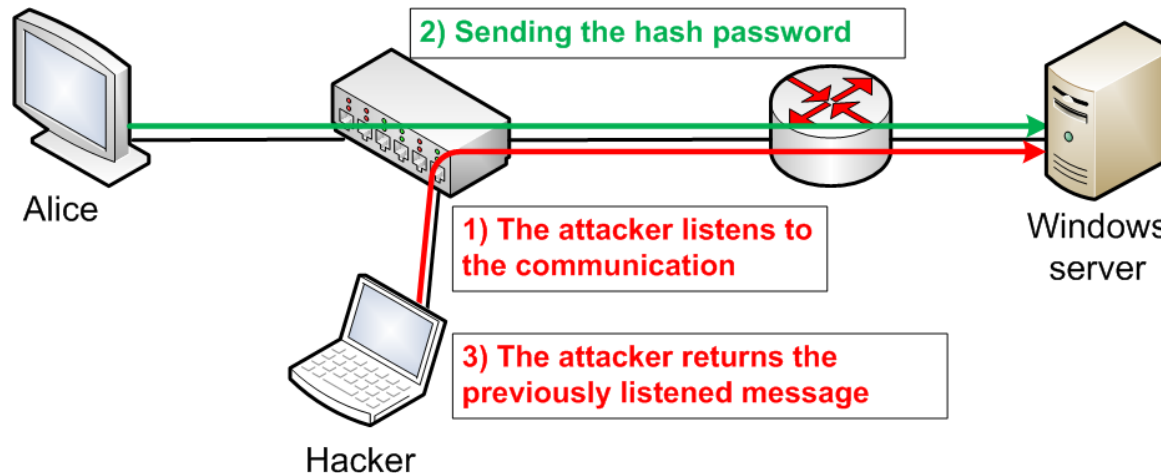
Replay attacks

- ▶ An attacker captures some type of data and resubmits it with the hopes of fooling the receiving device into thinking it is legitimate information
- ▶ Many times, the data captured and resubmitted are authentication information
 - The attacker is trying to authenticate himself as someone else to gain unauthorized access
- ▶ Timestamps and sequence numbers are two countermeasures
 - If a packet has a sequence number that has been previously used, this is an indication of a replay attack
 - Computer can be configure to only accept packets within a certain timeframe

Replay attacks

Principle

- A network attack in which a transmission is fraudulently repeated by a third party intercepting the packets on the line



Parades

- Using a Message Authentication Code (MAC)
- Using a Session ID
- Using One-Time Password (OTP)

Brute force attacks

■ Principle

- Test, one by one, all the possible combinations to find a password or a key
- Allows to break any password in a finite time regardless of the protection used

■ Complexity of Attack

- If the password contains N characters, the maximum number of attempts is the size of the "alphabet" used at power N

Type \ Password size	1 character	3 characters	6 characters	9 characters
Lowercase letters	26	17 576	308 915 776	$5,4 \times 10^{12}$
Lowercase letters and digits	36	46 656	2 176 782 336	$1,0 \times 10^{14}$
Lowercase, uppercase and digits	62	238 328	$5,6 \times 10^{10}$	$1,3 \times 10^{16}$

■ Parades

- Time limitation of connections
- Renewal of passwords

Technical attacks



Buffer overflow

► Principle

- Exploit a weakness in an application to execute an arbitrary code leading to an escalation of privileges (administrator rights)

► How does it work ?

- Injection in a buffer more data than it can contain

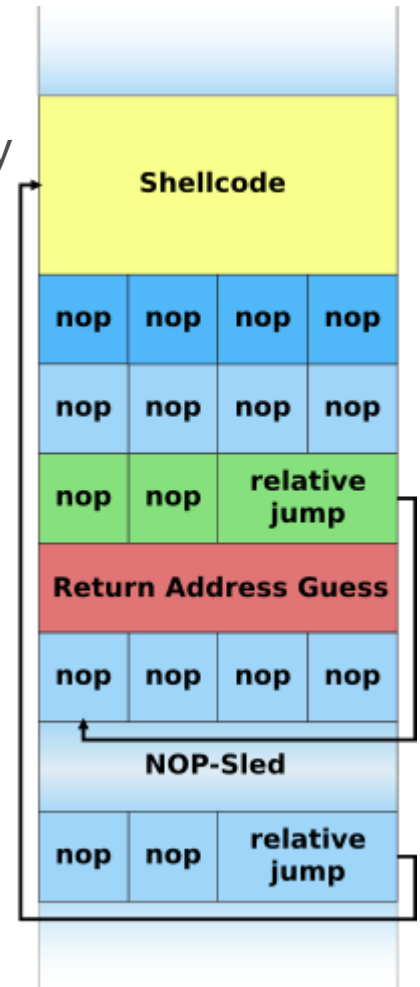
► Objective

- Overwrite addresses located just after the buffer to enable the application calls the hackers' code

► Difficult to implement for the attacker

► Parade

- Check program entries



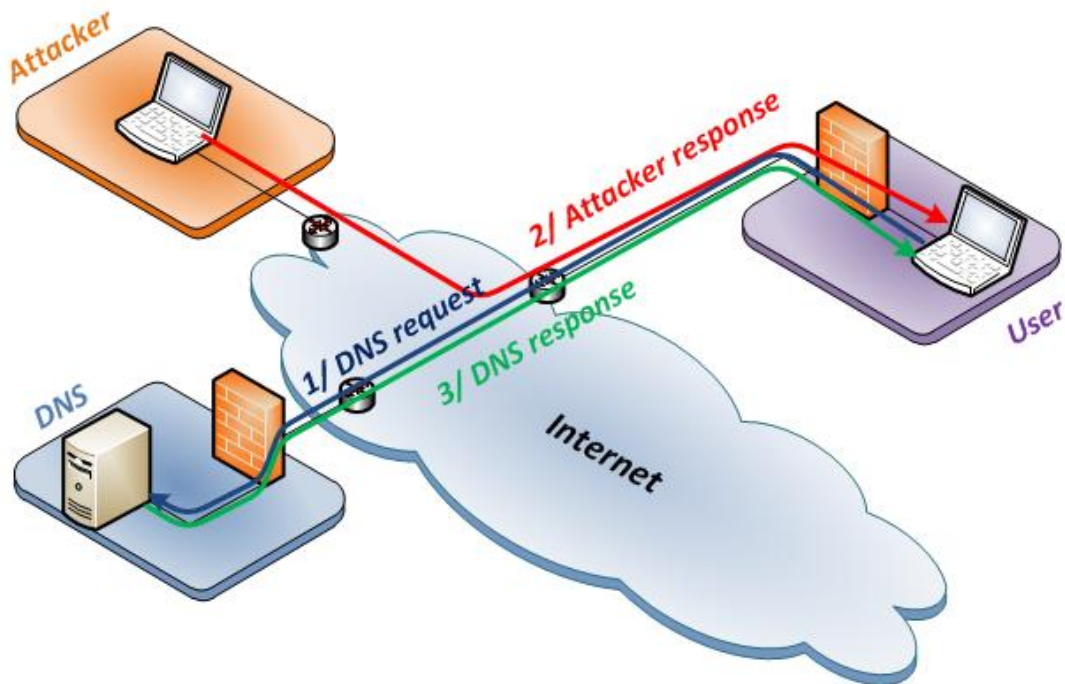
DNS spoofing

► Principle

- Redirect users unwittingly on a malicious web site

► DNS ID spoofing

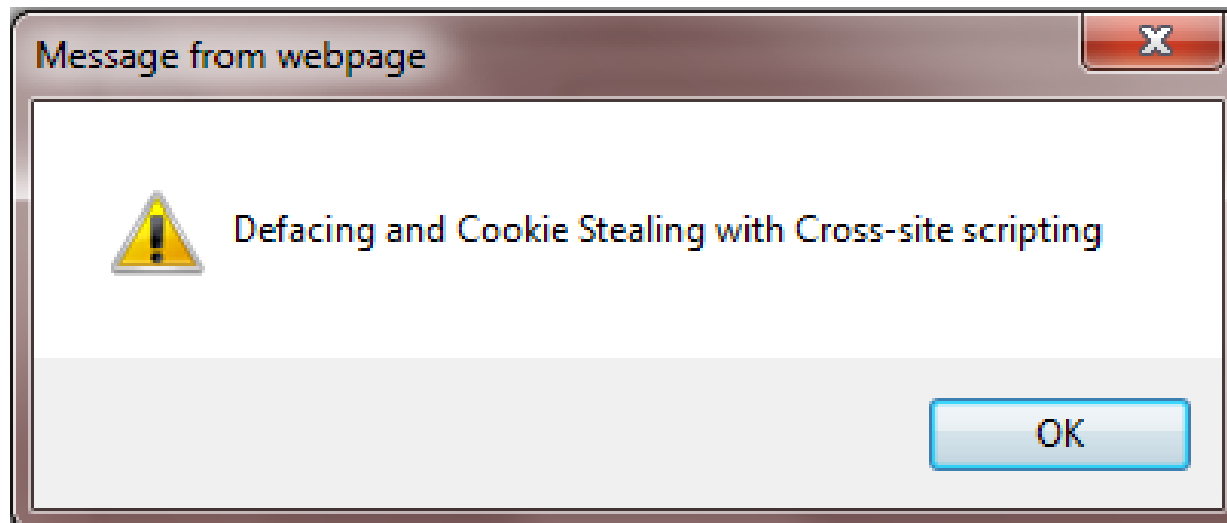
- Send the answer to the DNS request before the DNS server by recovering or guessing the ID to match hacker's IP with a particular address



DNS cache poisoning

- DNS servers have a cache for storing a while the correspondence between a name and an IP address
- DNS cache poisoning
 - ✓ The attacker has a DNS server with a domain name (attacker.com)
 - ✓ He asks the target DNS server to join the IP corresponding to attacker.com
 - ✓ The DNS server will look for the answer from the DNS server attacker.com
 - ✓ The attacker's DNS replies with the IP, but adds information on other sites in its response (google.com is the IP w.x.y.z)
 - ✓ The target server inserts the malicious information in the cache where it remains for some time
- Solution
 - ✓ Check that the response corresponds to what was expected (the IP of the requested domain name and nothing else)

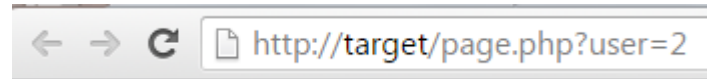
Web vulnerabilities attacks



URL manipulation

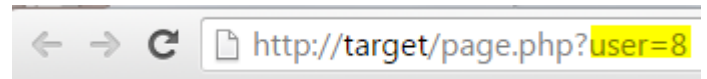
► Principle

- Manipulating parts of an URL, to gain access to normally protected space on a web server



► Objective

- Access to administration interface
- Get non-public information
- Alter the website



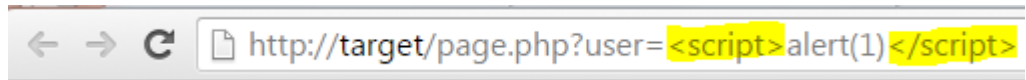
► How to avoid

- Make sure the server protects access to directories containing sensitive data → Check the existence of a session on each page
- Disable the display of files in a directory containing no index file ("Directory Browsing")

Cross Site Scripting (XSS)

■ Principle

- Run a script from a malicious link or recording data on a site vulnerable to XSS
- The sites are vulnerable to XSS if they are running the HTML tags present in the URL



■ Objective

- Get the cookie of the victim to the site to obtain the credentials or at least the ID of the session
- Redirect the victim on an other website
- Execution of any script javascript

Cross Site Request Forgery (CSRF)

■ Principle

- Run a script from a malicious link on a site vulnerable to CSRF relying on the fact that the user will be connected to use of user authentication

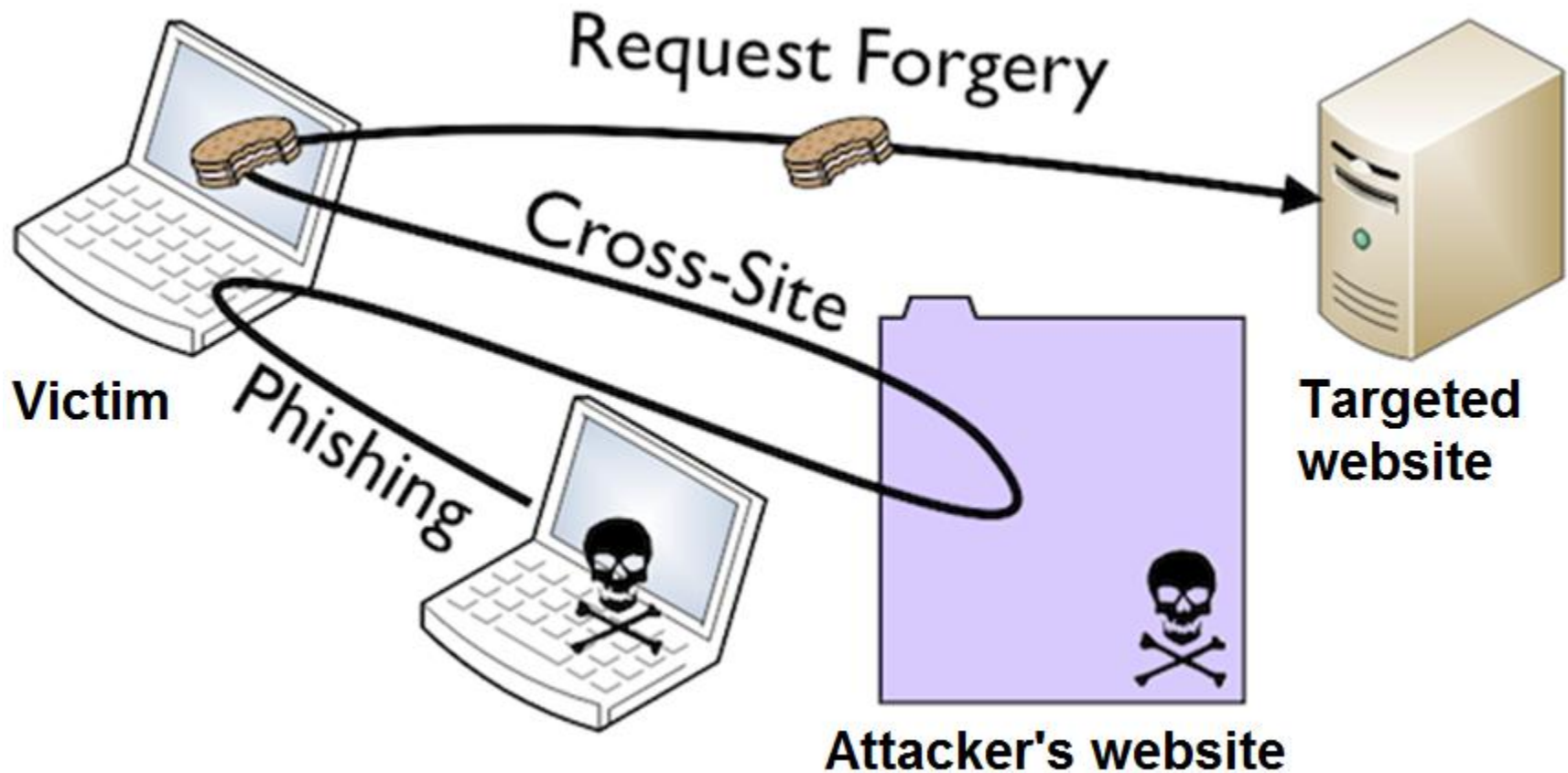
■ Objective

- Perform an action on a site for a person who has special rights (eg delete a message by sending an email to the website administrator)
- The sites are vulnerable to CSRF if they perform actions with a link without requiring user confirmation

■ Pre-requisites

- The attacker gets to know the link that allows to perform an action
- Requires that the victim is connected or has a persistent session

CSRF example



- ▶ The attacker's website can execute javascript on the computer of the victim in order to steal his session on the website targeted by the attack

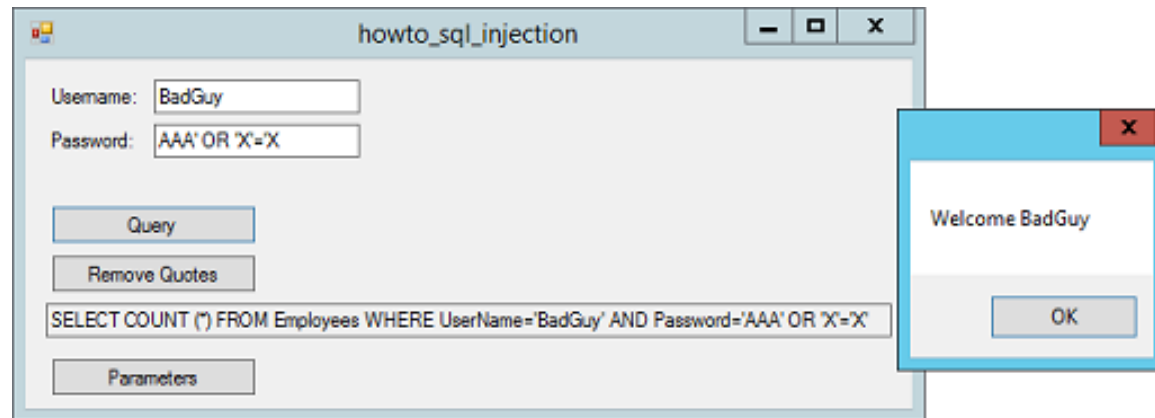
SQL injection

► Principle

- SQL command injection attacks are attacks against software or websites based on databases

► Objective

- Get information without authorization
- Destroy the database
- Alter the database



► Principle

- SQL statements are inserted into an entry field for execution

Fraud



Social engineering

► Principle

- It is a technique of obtaining information from users by telephone, email or direct contact

► Objective

- Obtain personal information

► How to avoid

- Learn about the identity of the caller by asking specific information (name, company, phone number)
- Verify information provided
- Wondering about the sensibility and confidentiality of the information requested

Phishing

► Principle

- Technique used by fraudsters to obtain sensitive information by masquerading as a trustworthy entity in an electronic communication

► Objective

- Commit identity theft
- Acquire sensitive information (usernames, passwords, credit card details)

► How to avoid

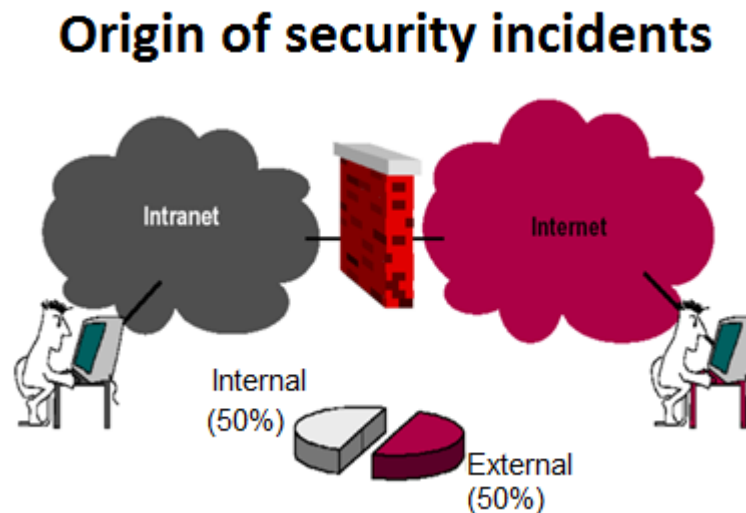
- Verification of the web address in the browser address bar is the first parade (spelling of the phishing domain name can be close to the real name)
- Visit the website by manually typing the address into your browser (avoids the problems of unicode characters)
- Verify the identity of the site with its certificate

Origin of security incidents

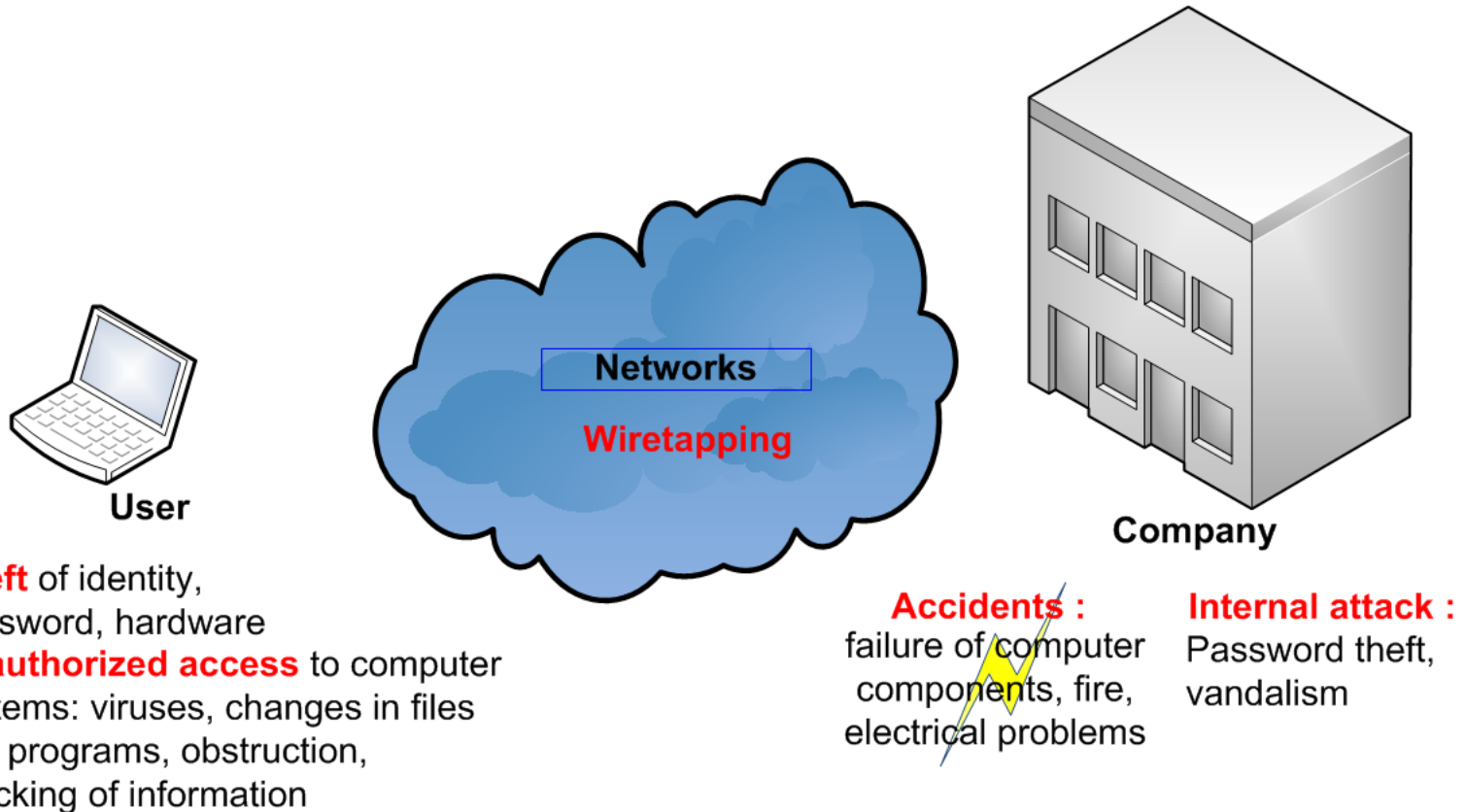
Security incidents can come from outside the IS but also from the inside.

It may be:

- An error of a user running an undesirable treatment, unintentionally erases data or inserts malware unknowingly
- An issue with the backup preventing data restoration
- A malicious act from an external hacker running a virus or modify the information of a database



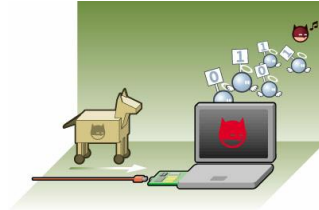
Example of threats



Scenario of Advanced Persistent Threat

1. Hack a user's computer from the Internet

- Trapped website (0day or unapplied update)
- Attachment in a malicious email



2. Running a Trojan and communication with a server on the Internet

3. Internal network mapping

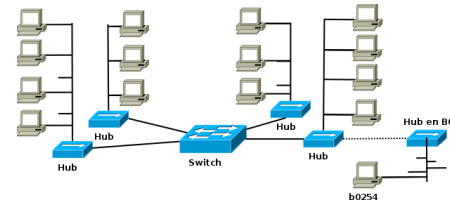
4. Attack and take control of servers

5. Exfiltration of passwords

6. Taking control of other computers in the network

7. Content Exfiltration

8. Erasing traces of exfiltration



How to protect?

► Knowing the information system



► Control the network



- Control of internal/external exchanges (FW, IPS/IDS)
- Secure administration

► Secure the terminals

- Encryption
- Antivirus/antispyware



► Manage Users



► Physically Secure

► Controlling IS security