

Security: List of terms

Concepts

Worm

A worm is malicious software that has the ability to spread itself through computer networks. Unlike viruses, worms do not require user interaction to copy themselves to other systems. They can exploit security vulnerabilities to infiltrate new machines, often causing severe disruption to network operations.

SPAM

Spam is unsolicited email, usually sent in bulk, that is designed to advertise products or services. SPAM can also contain malware or phishing, which puts users' security at risk. Attempts to block spam in email communications and on social media platforms are standard in the security industry

Computer virus

A computer virus is a type of malware that requires user interaction to infect a system. Viruses attach themselves to other programmes or files and are activated when these files are run. They can cause a variety of problems, from data corruption to information theft.

Trojan horse

A Trojan horse is a type of malware that impersonates a legitimate programme to get the user to install it. Once installed, a Trojan horse can allow the attacker to access the system, steal data or perform other harmful actions. It is important to be careful when downloading and installing software, especially from unknown sources.

Rootkit

A rootkit is malware that allows unauthorised people to gain and maintain access to a computer system without the user's knowledge. The name 'rootkit' is derived from the word 'root', which refers to an administrative account on UNIX systems, and 'kit', meaning a set of tools. Rootkits often alter components of the operating system to hide their presence, which makes them extremely difficult to detect. Main features of rootkits:

- Silent installation: Rootkits can be installed on a system by an attacker after gaining administrative access.
- Concealment: They are able to hide their presence and other malware.
- Difficulty of detection: They use techniques that may prevent them from being detected by

security software, including altering system files.

Spyware

Spyware is a type of malware that searches and collects data from a computer, often without the user's knowledge. It can record a user's activities, such as personal data entered, browsing histories or locations, and then transmit this information to a remote server. Key features of spyware:

- **Data collection:** Spyware collects personal data and can also track a user's online activities.
- **Uncontrolled activity:** Spyware can change browser settings, introduce adverts or other unwanted programmes.
- **Hidden nature:** It runs in the background, unnoticed by the user, making it as dangerous as a rootkit.

The file extensions most commonly containing viruses

The files that pose the greatest risk are **.exe**, as these are applications that can directly run on the system. **.docx** and **.xlsx** files with macros can also be dangerous, especially if users are not careful. **.pdf** files are the safest, but can also contain threats. It is important to always scan files before opening them, especially if they come from unknown sources. If you need additional information on virus protection, let us know!

Extension	Description
.exe	Executable programs that are most commonly used to spread viruses. When run, they can install malware on a computer.
.pdf	Although PDF files are usually safe, they can contain malicious scripts and links that lead to malware.
.docx	Microsoft Word files can be used to spread macros that run malware, especially if the user allows them to run.
.xlsx	Excel files can also contain macros that can be used to infect the system with malware if they are run by users.

Spoofing attacks in different layers

Layer	Type of spoofing attack
1 Physical layer	Physical spoofing: impersonation of network signals to take control or collect data.
2. Data link layer	MAC Spoofing: changing the MAC address of a device to disguise its identity or to impersonate another device on the local network.
3. network layer	IP Spoofing: impersonating the IP address of another device, which can enable a DDoS attack or security bypass.
4. Transport layer	TCP Spoofing: manipulation of TCP packets to intercept a session or authenticate a user.
5. Session Layer	Session Hijacking: taking over an active user session, allowing an attacker to pretend to be another user.
6 Presentation layer	Poor encryption or lack of security means that transmitted data can be manipulated or falsified.

Layer	Type of spoofing attack
7 Application layer	HTTP Spoofing: impersonation of far-flung servers to launch an attack on web applications.

Types of encryption algorithms and hash functions

Symmetric encryption algorithms

Symmetric encryption algorithms use the same key to encrypt and decrypt data. The key must be securely transmitted between the parties.

Algorithm	Description
AES (Advanced Encryption Standard)	One of the most widely used algorithms, used in various standards such as the SSL/TLS protocol.
DES (Data Encryption Standard)	An older algorithm, now considered unsafe due to its short key (56 bits).
3DES (Triple DES)	Secures data by using the DES algorithm in triplicate. It is more secure, but slower.
Blowfish	A fast algorithm that is flexible in terms of key length (from 32 to 448 bits).
RC4	A streaming algorithm that was popular for encrypting communications, now considered unsafe.

Asymmetric encryption algorithms

Asymmetric encryption algorithms use a pair of keys: public for encryption and private for decryption.

Algorithm	Description
RSA (Rivest-Shamir-Adleman)	The most popular asymmetric algorithm, based on the factorisation of large numbers.
DSA (Digital Signature Algorithm)	Used mainly for digital signatures using public and private keys.
ECC (Elliptic Curve Cryptography)	Uses mathematical elliptic curves, offering a high level of security with shorter keys.
ElGamal	An algorithm using asymmetric keys, often used in public key cryptography.

hash functions

Shortcut functions (hash functions) are used to convert input data into fixed-length values, ensuring data integrity.

Function	Description
SHA-256	Part of the SHA-2 family, popular in cryptography, it generates a hash length of 256 bits.
SHA-3	The latest version of the SHA algorithm that works with different hash lengths.
MD5	An older hash function, now considered unsafe due to vulnerability to collisions.
RIPEMD-160	A hash function that generates a 160-bit digest, used in a variety of applications.

Types of attacks on computer systems and networks

Cross-Site Scripting (XSS) attack

A cross-site scripting attack involves the insertion of a malicious script into a website, allowing the attacker to perform unauthorised actions in the context of the victim's browser. It can lead to session theft, user data or account takeover. These attacks can be of various types:

- Stored XSS: a malicious script is stored on the server, e.g. in a database.
- Reflected XSS: the script is sent back as part of an HTTP request and executed immediately.

Man-in-the-Middle (MitM) attack

The MitM attack consists of intercepting and modifying communications between two parties that are believed to be communicating directly. The attacker can:

- Eavesdrop on data sent between the user and the server.
- Alter messages before they are delivered to the recipient.
- Introduce malware.

Distributed Denial of Service (DDoS) attack.

A DDoS attack is a form of attack in which a large number of infected computers (zombies) send a large amount of traffic to a target, thereby overloading the server or network. The aim is to prevent a service from functioning normally. It can be performed in a number of ways:

- Flooding: excessively floods the server with requests.
- Amplification: exploits server vulnerabilities to increase the amount of data sent.

Concentrated attack (Single Point of Failure)

A concentrated attack refers to vulnerabilities in the IT infrastructure that can be attacked to cause system failure. In this context, there can be various threats such as:

- Malware: intentional infection of key components.
- Data deletion: destruction or theft of data stored in sensitive locations.

Variation of break time depending on key length.

Change of break time depending on key length

Example for the XOR algorithm: [Security: XOR Vernam key space](#)

The break time of an encryption algorithm is proportional to the number of possible key combinations.

Each time the key length is increased by one bit, the number of combinations doubles. Mathematically speaking, for a key of length n bits, the number of possible keys is 2^n . Example: Extending the key by 6 bits

- Number of keys for the current key n : 2^n .
- Number of keys for key extended by 6 bits: $2^{(n+6)} = 2^n \times 2^6 = 64 \times 2^n$

Calculation example

Suppose we have a 64-bit key:

- Number of possible keys: 264 (about 18.4 trillion keys).
- After extending the key by 6 bits (up to 70 bits):
- Number of possible keys: 270 (approximately 1.18 quintillion keys).

Changing the breaking time

If we assume that the time required to break a given key is equal to T , then:

- Break time for a 64-bit key: T .
- Break time for a 70-bit key: 64 times longer ($64T$).

Password Power

Choosing a strong password is crucial for protecting data and systems. Let's take a look at the passwords provided, assessing their complexity, length and elements that make them difficult to crack.

"I'm a genius"

- Length: 15 characters
- Complexity: Uses only lowercase letters, no special characters or numbers.
- Evaluation: Although the password is relatively long, its lack of differentiation (only lowercase letters) makes it an easy target for dictionary attacks. An attacker can quickly look up popular phrases in a particular language.

"I think therefore I am"

- Length: 19 characters (including spaces).
- Complexity: Contains diacritical marks (ć, ñ), but spaces between words can be problematic.
- Evaluation: Although the password is long and contains special characters, the presence of spaces makes it less practical. Also, it may be easier to guess as it is a well-known philosophical phrase.

"Bolek&Lolektobay".

- Length: 20 characters
- Complexity: Contains upper and lower case letters and a special character (&).
- Evaluation: This password is on the right track, but the reference to well-known fairy tale characters makes it more vulnerable. Those trying to crack this password can easily guess based on popular cultural themes.

"Alibaba+40 robbers"

- Length: 22 characters
- Complexity: Contains upper and lower case letters, special character (+) and numbers.
- Rating: This is by far the most difficult password to crack of all those listed. The high length, variety of characters and unique combination make it much less vulnerable to attacks.