Information Security

Information Security

- means protecting data from those who do not have permission to access it.

Threats and Defenses

Authentication and Authorization

Authentication is the process of verifying that you really are the person who has the right to access a particular device, whether it is your local machine or the remote server.

Authorization

Governs what authenticated user is allowed to do. Enforcing authorization rules is also one of the jobs of the operating system. The operating system maintains access control lists (also called permissions) that specify exactly what the user is allowed to do with each data file. Depending on who the users are, they have various levels of privilege such as follows:

- read access (can read a particular file)
- write access (can modify a particular file)
- execute access (can run a particular program file)
- delete access (can delete a particular file)

Threats from the Network

Once your handheld device, PC , or web server is connected to the internet, there are many more possibilities for harm. Most of these security threats come in the form of **malware** (malicious software) that can attack an individual computer.

Viruses, worms, trojan horses, and denial of services are the most common attacks.

Virus

A virus is a computer program that, like a biological virus, infects a host computer and then spreads. It embeds itself within another program or file. When that program or file is activated, the virus copies itself and attacks other files on the system.

Worm

Worm is very similar to a virus, but it can send copies of itself to other nodes of a computer network without having to be carried by an infected host file. It is a self-replicating piece of software that can travel from node to node without any human intervention.

Trojan Horse

is a computer program that does some legitimate computational task but also unbeknownst to the user, contains code to perform the same kinds of malicious attacks as viruses and worms. It might also upload files or capture the user address book to send out spam, hide a keystroke logger that captures the user's password and credit card numbers or even put the computer in someone else control in the future.

Denial of Service

it is typically directed at a business or government website. The attack automatically directs browsers, usually on many machines on a single web address at roughly the same time. The result causes too much network traffic to the targeted site that it effectively shutdowns legitimate users

Beware of Phishing

Phishing is a common method used by cybercriminals to trick individuals into revealing sensitive information such as credit card numbers account numbers and passwords.

Defense against the dark arts

Here are a few simple guidelines you can protect yourself against almost all the attacks discussed so far.

- Be sure your computer has up-to-date **antivirus software** from a reputable company. Such software can detect viruses, worms, and trojan horse by the distinct "signatures" those programs carry. It cleans your machine of infected files.

- Be sure your computer has up-to-date **firewall software**. It guards the access points to your computer blocking the communications to or from sites you do not permit and preventing certain operations from being initiated across the internet.

- Be sure your computer has up-to-date **antispyware**. It routinely scans your computer for any "spyware" programs that may have infected your machine that capture info on what website you have visited and what passwords and credit card numbers you have used.

- Set up your browser to use a pop-up blocker.
- Always install the latest security patches or updates to use your operating system.
- Don't send personal or financial information in response to any email.

White hats vs Black hats

White hats - are the security experts who try to keep us safe in cyberspace.

Black hats - are the bad guys who try to ferret out computer system weaknesses for financial gain or control.

These two groups are locked in constant battle.

Encryption

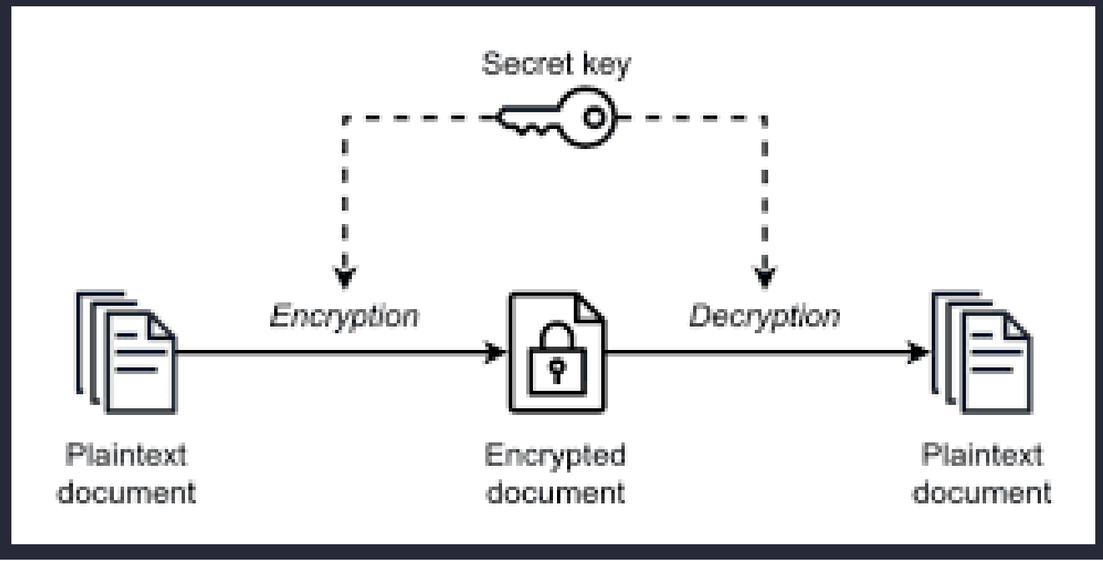
Much of the focus of info security is to devise defenses so that the "bad guys" can't steal our information. if, despite all these precautions personal files, or sensitive data are illegally accessed and fall into the wrong hands, we can still protect their content through the process of encryption. The purpose of encryption is to make information meaningless even if someone does manage to steal it.

Encryption Overview

Cryptography is the science of "secret writing" A message (plaintext) is encoded (encrypted) before it is sent, for the purpose of keeping its content secret if it is intercepted by the wrong parties. The encrypted message is called ciphertext. The ciphertext is decoded (decrypted) back to plaintext when it is received.
More formally, encryption is the process of using an algorithm to convert information to a representation that cannot be understood by anyone without the appropriate decryption algorithm; **DECRYPTION** is the reverse of encryption, using an algorithm that converts ciphertext back to plain text.

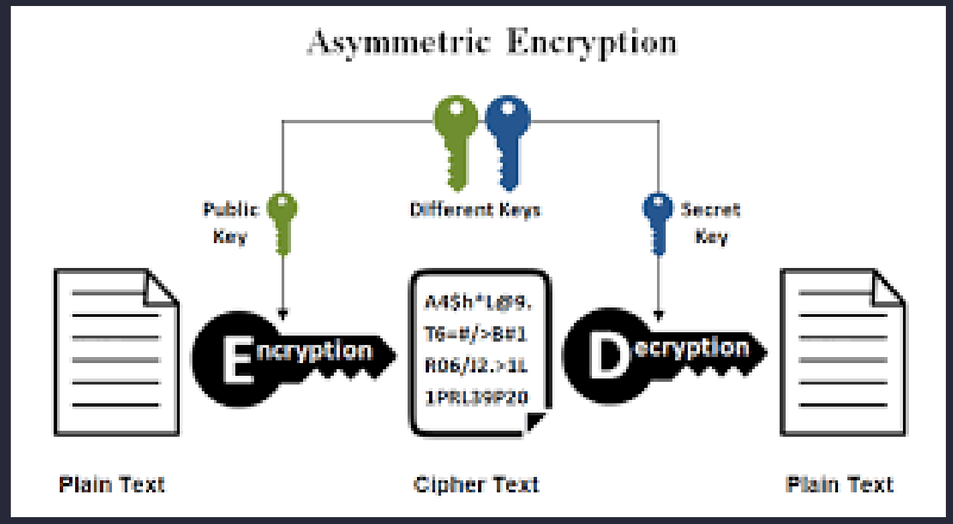
Symmetric Encryption Algorithm

It requires the use of a secret key known to both the sender and receiver. The sender encrypts the plaintext using the key. The receiver knowing the key, is easily able to reverse the process and decrypt the message.



Asymmetric Encryption Algorithm

It is also called public key encryption algorithm, the key for encryption and decryption are quite different. Although related, person A can make the encryption key public, and anyone can encrypt a message using A's public key and send it to A. Only A has the decryption key, however, so only A can decrypt the message.



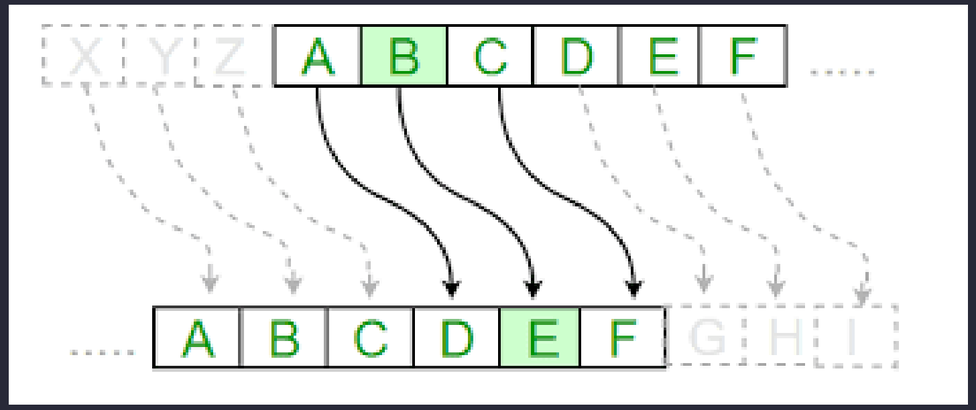
END OF DAY 1

KAKAPOY

Simple Encryption Algorithms

Caeser Cipher

Caeser Cipher also called shift cipher, involves shifting each character in the message to another some fixed distance farther along in the alphabet.
For example, if the shift value is 3, A would become D, B would become E, C would become F, and so on. Encrypt your message by replacing each letter with the corresponding shifted letter. For example, if the shift value is 3, the word “hello” would become “khoor”.



Block Cipher

Wapa mahuman

Web Transmission Security

TLS (Transport Layer Security) is one method for achieving secure transfer of information on the web. It encrypts data sent over the Internet to ensure that eavesdroppers and hackers are unable to see what you transmit which is particularly useful for private and sensitive information such as passwords, credit card numbers, and personal correspondence.

Embedded Computing

Embedded Computers are computational devices such as chips, processors, or computers that are embedded within another system. It usually performs one or two tasks as part of the system in which they occur, they are small devices that you never see. They can be found in cars, cellphones, video game console, home alarm system, watch, and many more.

Thanks!

Do you have any questions?