Computer Security Tutorial

Computer Security is the process of detecting and preventing any unauthorized use of your laptop/computer. It involves the process of safeguarding against trespassers from using your personal or office based computer resources with malicious intent or for their own gains, or even for gaining any access to them accidentally.

In this tutorial, we will treat the concept of computer security which can be a laptop, a workstation, a server or even a network device. This is an introductory tutorial that covers the basics of Computer Security and how to deal with its various components and sub-components.

Audience

This tutorial has been prepared mainly for those professionals who are within the IT industry, working as IT specialists, System administrators, and Security administrators.

This tutorial is intended to make you comfortable in getting started with Computer Security and its various functions.

Prerequisites

It is an elementary tutorial and you can easily understand the concepts explained here with a basic knowledge of how a company or an organization deals with its Computer Security. However, it will help if you have some prior exposure on how to carry out computer updates regularly, setting up firewalls, antiviruses, etc. In this tutorial, we will treat the concept of Computer Security which can be a laptop, a workstation, a server or a network device. This tutorial is done mainly for people

that are within the IT industry who are IT specialists, System administrators, Security administrators.

Outlines of Computer Security Tutorial

- **Computer Security - Overview**
- **Computer Security - Elements**
- **Computer Security - Terminologies**
- **Computer Security - Layers**
- **Computer Security - Securing OS**
- **Computer Security - Antiviruses**
- **Computer Security - Malwares**
- **Computer Security - Encryption**
- **Computer Security - Data Backup**
- **Disaster Recovery**
- **Computer Security - Network**
- **Computer Security - Policies**
- **Computer Security - Checklist**
- **Legal Compliance**

Why Security?

Cyberspace (internet, work environment, intranet) is becoming a dangerous place for all organizations and individuals to protect their sensitive data or reputation. This is because of the numerous people and machines accessing it. It is important to mention that the recent studies have shown a big danger is coming from internal threats or from disappointed employees like the Edward Snowden case, another internal threat is that information material can be easy accessible over the intranet.

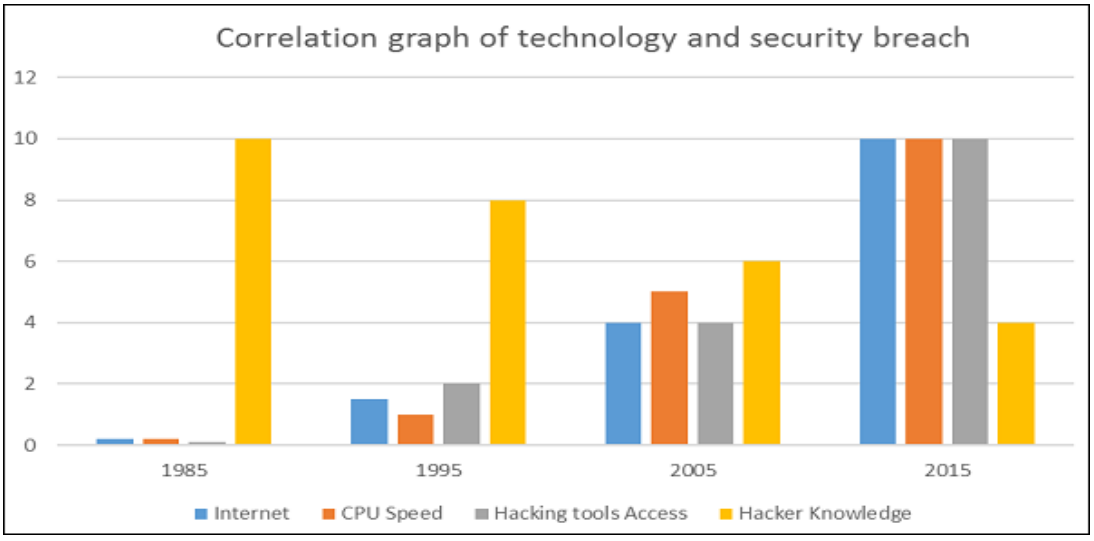
One important indicator is the IT skills of a person that wants to hack or to breach your security has decreased but the success rate of it has increased, this is because of three main factors −

- Hacking tools that can be found very easily by everyone just by googling and they are endless.
- Technology with the end-users has increased rapidly within these years, like internet bandwidth and computer processing speeds.
- Access to hacking information manuals.

All this can make even a school boy with the curiosity, a potential hacker for your organization.

Since locking down all networks is not an available option, the only response the security managers can give is to harden their networks, applications and operating systems to a reasonable level of safety, and conducting a business disaster recovery plan.

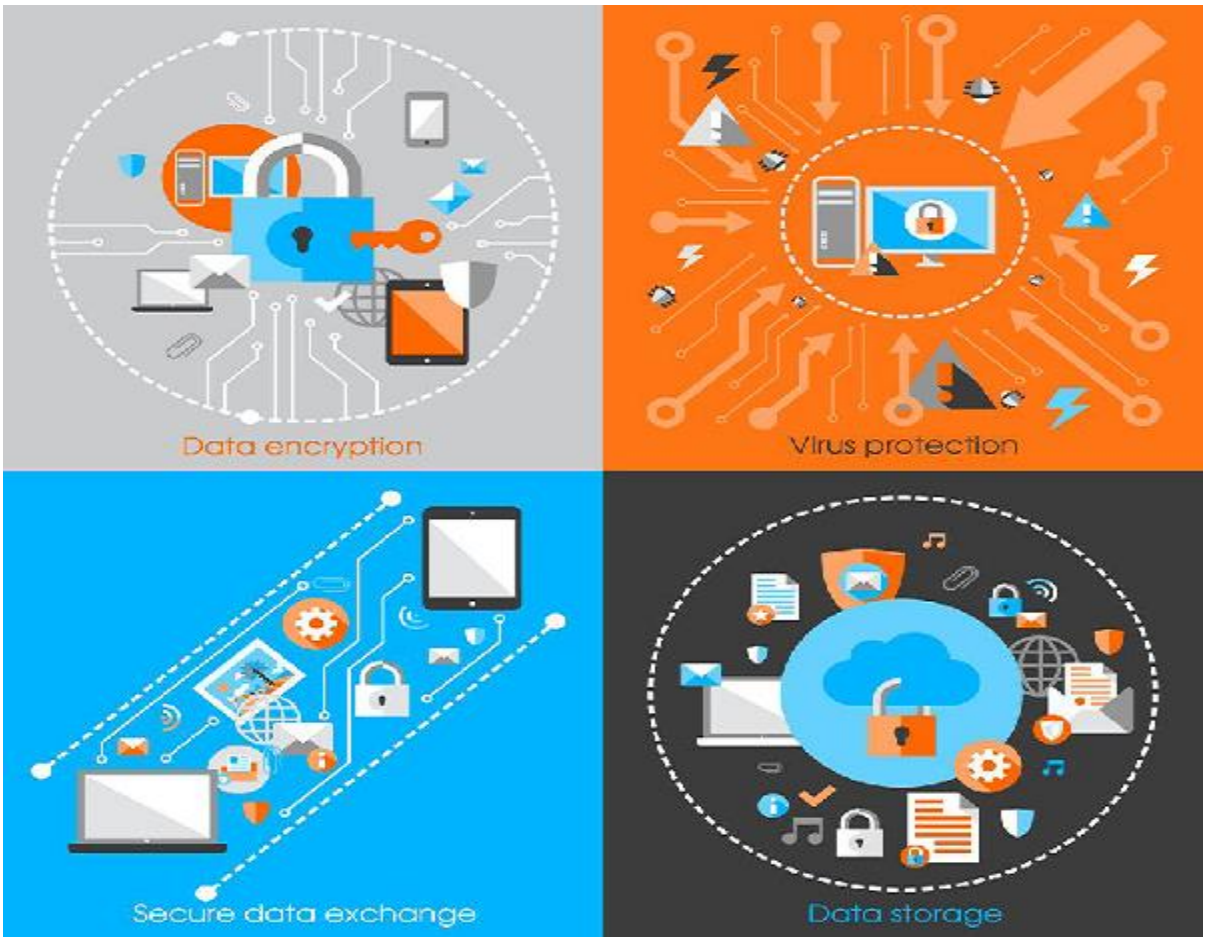
The following graph gives us a basic idea.



What to Secure?

Let's see this case, you are an IT administrator in a small company having two small servers staying in a corner and you are very good at your job. You are doing updates regularly, setting up firewalls, antiviruses, etc. One day, you see that the organization employees are not accessing the systems anymore. When you go and check, you see the cleaning lady doing her job and by mistake, she had removed the power cable and unplugged the server.

What I mean by this case is that even physical security is important in computer security, as most of us think it is the last thing to take care of.



Now let's go directly to the point of what all to secure in a computer environment:

- First of all, is to check the physical security by setting control systems like motion alarms, door accessing systems, humidity sensors, temperature sensors. All these components decrease the possibility of a computer to be stolen or damaged by humans and environment itself.
- People having access to computer systems should have their own user id with password protection.
- Monitors should be screen saver protected to hide the information from being displayed when the user is away or inactive.
- Secure your network especially wireless, passwords should be used.
- Internet equipment as routers to be protected with password.
- Data that you use to store information which can be financial, or non-financial by encryption.
- Information should be protected in all types of its representation in transmission by encrypting it.

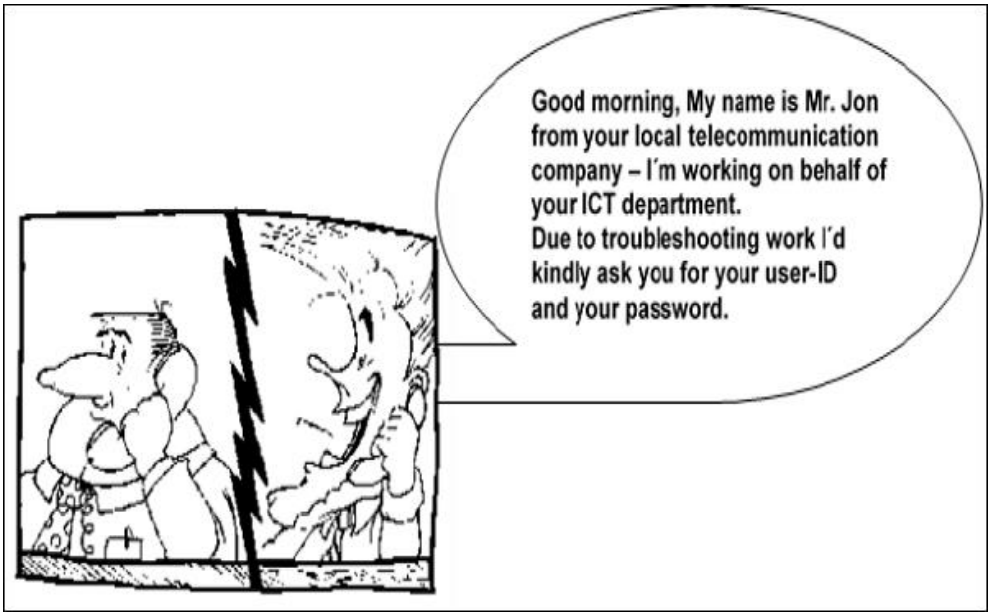
Benefits of Computer Security Awareness

Do you know in all this digital world, what is the biggest hole or the weakest point of the security?

Answer. It is us, humans.

Most of the security breaches come from uninformed and untrained persons which give information to a third party or publish data in Internet without knowing the consequences.

See the following scenario which tells us what employees might end up doing without computer security awareness −



So the benefits of computer security awareness are obvious as it directly minimizes the potential of you being hacked off your identity, your computer, your organization.

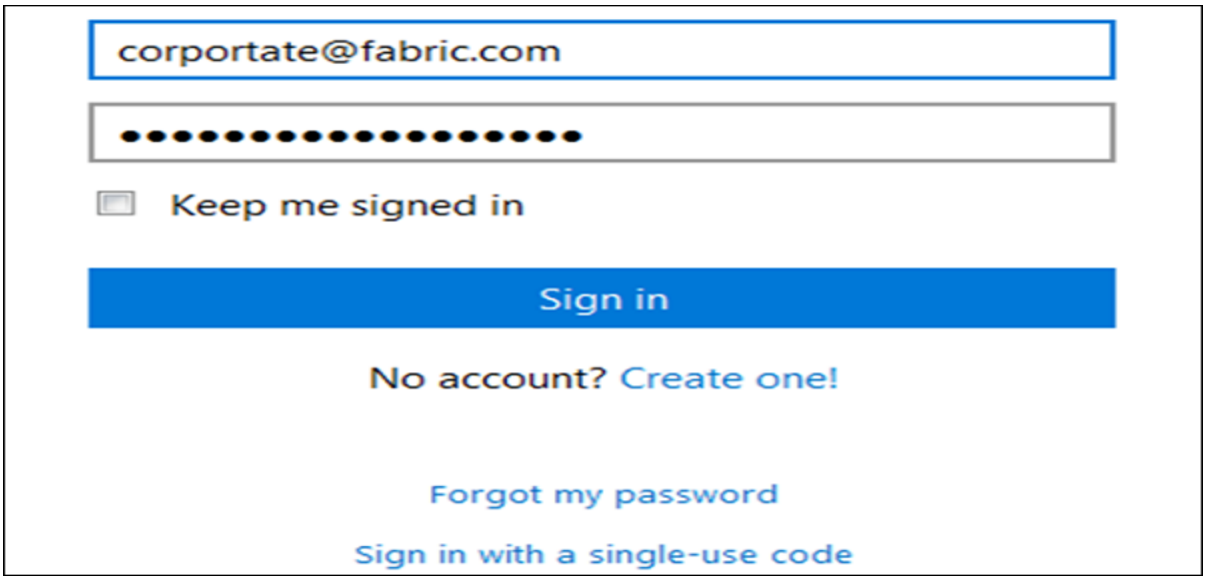
Potential Losses due to Security Attacks

The potential loses in this cyberspace are many even if you are using a single computer in your room. Here, I will be listing some examples that have a direct impact on you and on others −

- **Losing you data** − If your computer has been hacked or infected, there is a big chance that all your stored data might be taken by the attacker.
- **Bad usage of your computer resources** − This means that your network or computer can go in overload so you cannot access your genuine services or in a worst case scenario, it can be used by the hacker to attack another machine or network.
- **Reputation loss** − Just think if your Facebook account or business email has been owned by a social engineering attack and it sends fake information to

your friends, business partners. You will need time to gain back your reputation.

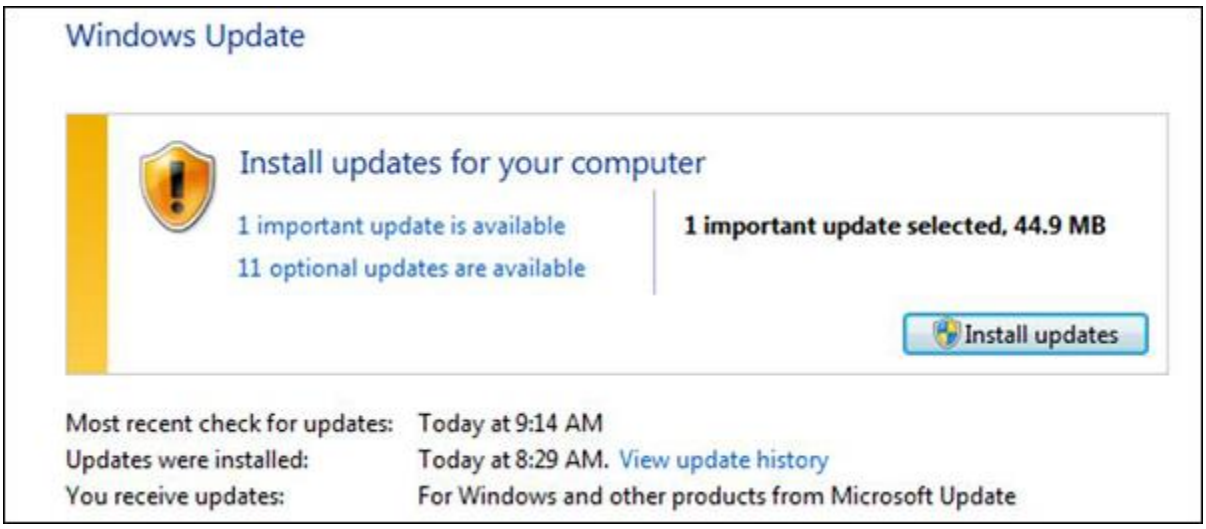
- **Identity theft** − This is a case where your identity is stolen (photo, name surname, address, and credit card) and can be used for a crime like making false identity documents.



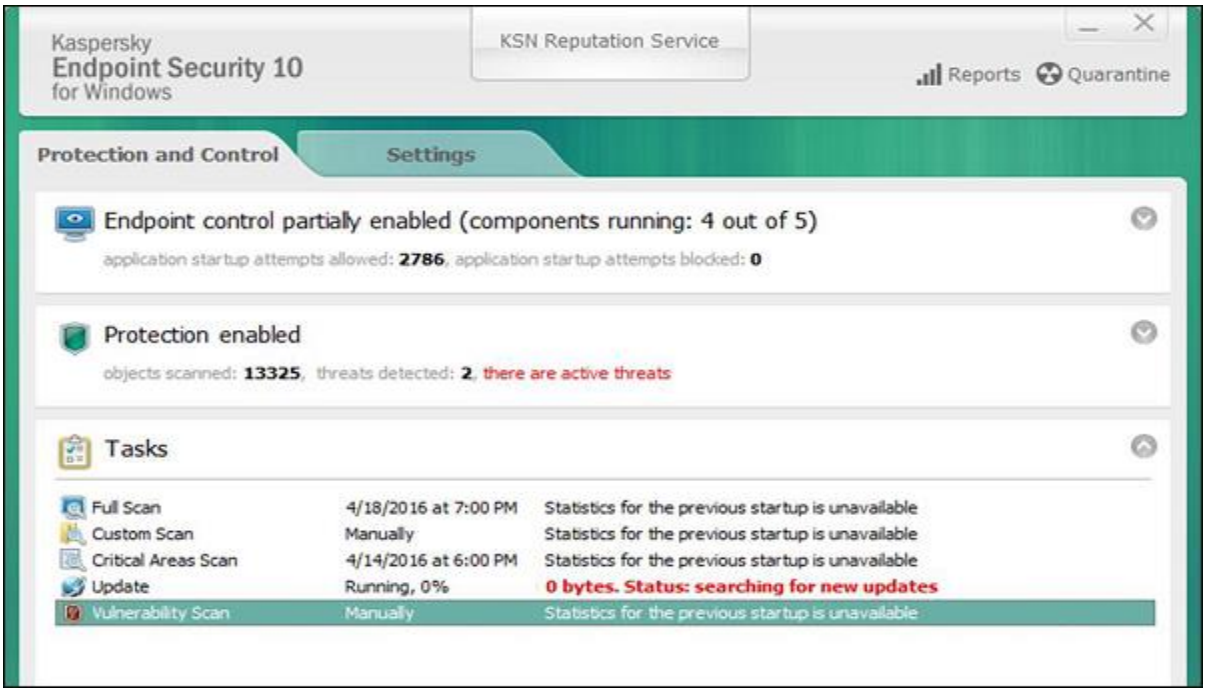
Basic Computer Security Checklist

There are some basic things that everyone of us in every operating system need to do −

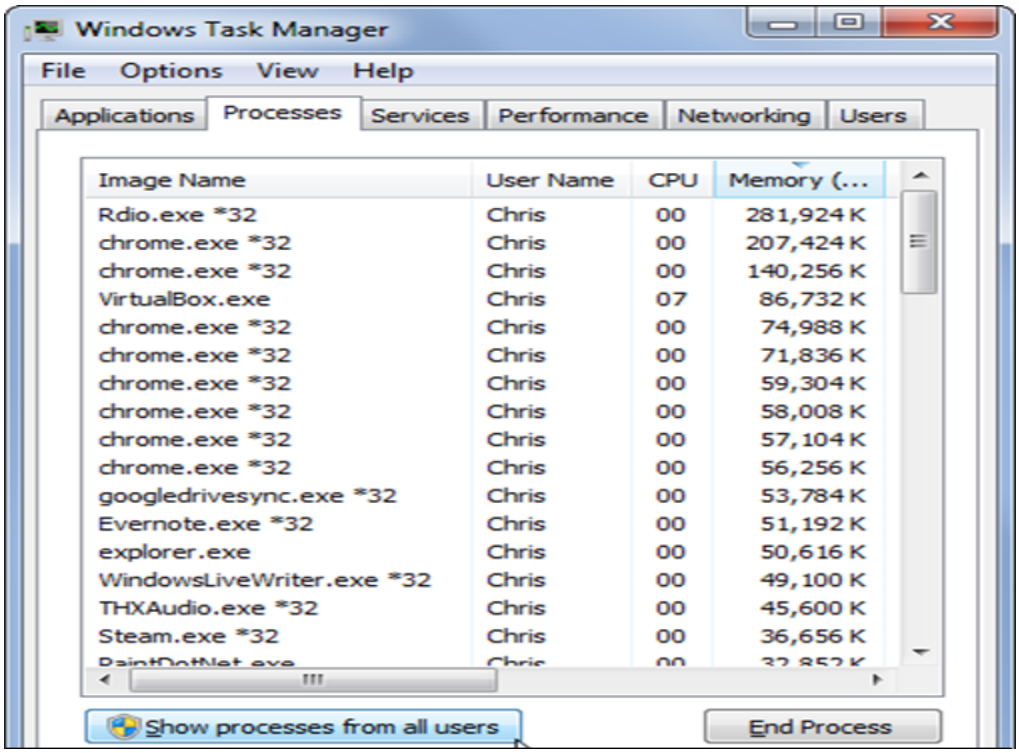
- Check if the user is password protected.
- Check if the operating system is being updated. In my case, I did a screenshot of my laptop which is a Windows 7.



- Check if the antivirus or antimalware is installed and updated. In my case, I have a Kaspersky antivirus being updated.



- Check for the unusual services running that consumes resources.

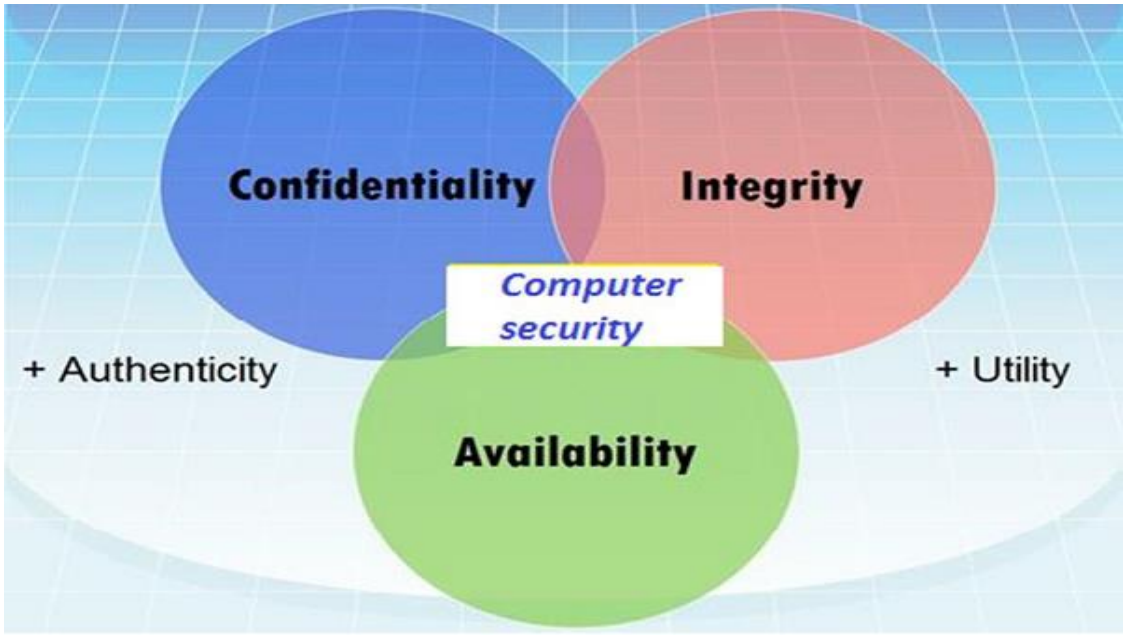


- Check if your monitor is using a screen saver.
- Check if the computer firewall is on or not.
- Check if you are doing backups regularly.
- Check if there are shares that are not useful.
- Check if your account has full rights or is restricted.
- Update other third party software's.

The general state in Computer Security has the ability to detect and prevent attacks and to be able to recover. If these attacks are successful as such then it has to contain the disruption of information and services and check if they are kept low or tolerable.

Different Elements in Computer Security

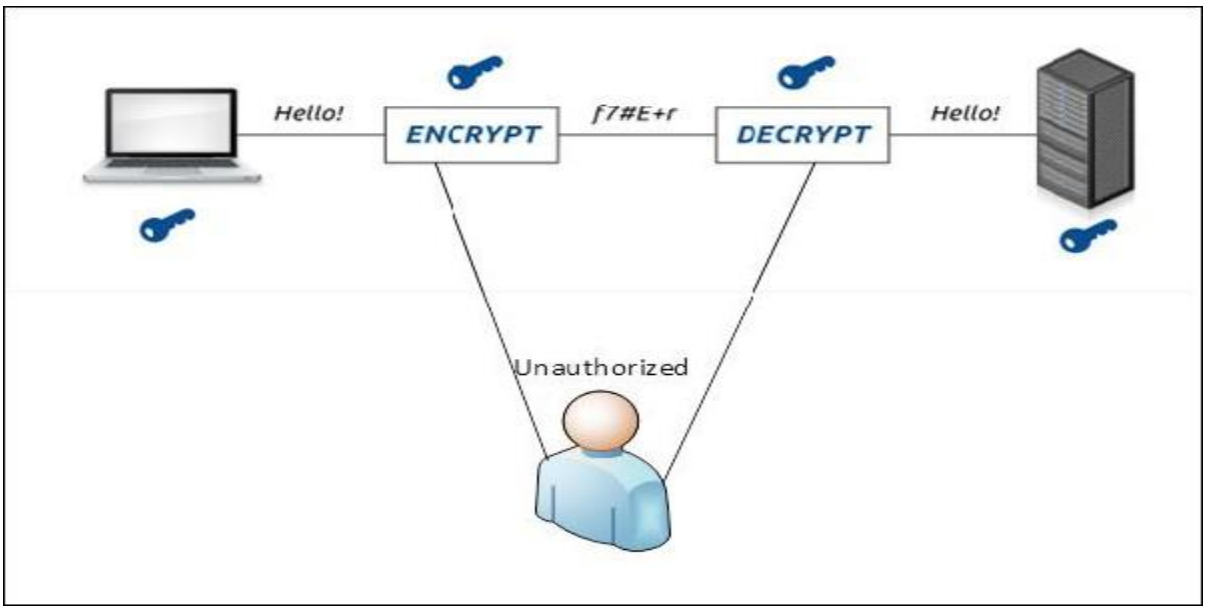
In order to fulfil these requirements, we come to the three main elements which are **confidentiality, integrity**, and **availability** and the recently added **authenticity and utility**.



Confidentiality

Confidentiality is the concealment of information or resources. Also, there is a need to keep information secret from other third parties that want to have access to it, so just the right people can access it.

Example in real life − Let's say there are two people communicating via an encrypted email they know the decryption keys of each other and they read the email by entering these keys into the email program. If someone else can read these decryption keys when they are entered into the program, then the confidentiality of that email is compromised.



Integrity

Integrity is the trustworthiness of data in the systems or resources by the point of view of preventing unauthorized and improper changes. Generally, Integrity is composed of two sub-elements – data-integrity, which it has to do with the content of the data and authentication which has to do with the origin of the data as such information has values only if it is correct.

Example in real life − Let's say you are doing an online payment of 5 USD, but your information is tampered without your knowledge in a way by sending to the seller 500 USD, this would cost you too much.

In this case cryptography plays a very major role in ensuring data integrity. Commonly used methods to protect data integrity includes hashing the data you receive and comparing it with the hash of the original message. However, this means that the hash of the original data must be provided in a secure way.

Availability

Availability refers to the ability to access data of a resource when it is needed, as such the information has value only if the authorized people can access at right time. Denying access to data nowadays has become a common attack. Imagine a downtime of a live server how costly it can be.

Example in real life − Let's say a hacker has compromised a webserver of a bank and put it down. You as an authenticated user want to do an e-banking transfer but it is impossible to access it, the undone transfer is a money lost for the bank.

In this chapter, we will discuss about the different terminology used in Computer Security.

- **Unauthorized access** − An unauthorized access is when someone gains access to a server, website, or other sensitive data using someone else's account details.
- **Hacker** − Is a Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc.
- **Threat** − Is an action or event that might compromise the security.
- **Vulnerability** − It is a weakness, a design problem or implementation error in a system that can lead to an unexpected and undesirable event regarding security system.
- **Attack** − Is an assault on the system security that is delivered by a person or a machine to a system. It violates security.

- **Antivirus or Antimalware** − Is a software that operates on different OS which is used to prevent from malicious software.
- **Social Engineering** − Is a technique that a hacker uses to stole data by a person for different for purposes by psychological manipulation combined with social scenes.
- **Virus** − It is a malicious software that installs on your computer without your consent for a bad purpose.
- **Firewall** − It is a software or hardware which is used to filter network traffic based on rules.