**What is Information Security?**

**Information Security** is not all about securing information from unauthorized access. Information security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

Information can be physical or electrical one. Information can be anything like Your details or we can say profile on social media etc.

Information Security programs are build around 3 objectives, commonly known as **CIA – Confidentiality, Integrity, Availability.**

1. **Confidentiality –** means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.
2. **Integrity –** means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an employee leaves an organization then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.
3. **Availability –** means information must be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstand the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management. Denial of service attack is one of the factor that can hamper the availability of information.

Apart from this there is one more principal that governs information security **i.e. Non Repudiation**

* **Non repudiation –**means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction. For example in cryptography it is sufficient to show that message matches the digital signature signed with sender’s private key and that sender could have a sent a message and nobody else could have altered it in transit. Data Integrity and Authenticity are pre-requisites for Non repudiation.
* **Authenticity –**means verifying that users are who they say they are and that each input arriving at destination is from a trusted source. This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission. For example if take above example sender sends the message along with digital signature which was generated using the hash value of message and private key. Now at the receiver side this digital signature is decrypted using the public key generating a hash value and message is again hashed to generate the hash value. If the 2 value matches then it is known as valid transmission with the authentic or we say genuine message received at the recipient side

**(Definition:** [**https://hitachi-id.com/resource/iam-concepts/authentication.html**](https://hitachi-id.com/resource/iam-concepts/authentication.html) **)**

* **Accountability –**means that it should be possible to trace actions of an entity uniquely to that entity. For example as we discussed in Integrity section Not every employee should be allowed to do changes in other employees data. For this there is a separate department in an organization that is responsible for making such changes and when they receive request for a change then that letter must be signed by higher authority for example Director of college and person that is allotted that change will be able to do change after verifying his bio metrics, thus timestamp with the user (doing changes) details get recorded. Thus we can say if a change goes like this then it will be possible to trace the actions uniquely to an entity.

**Need for Information Security**

Information Security is needed for the following reasons-

1. Protecting the functionality of the organization
2. Enabling the safe operation of applications
3. Protecting the data that the organization collect and use
4. Safeguarding technology assets in organizations (source: <https://www.geeksforgeeks.org/need-of-information-security/?ref=rp> )

**Why do we need Information Security?**

As we know from the previous section, information security is all about protecting the confidentiality, integrity, and availability of information.

**Answer these questions:**

Do you have information that needs to be kept confidential (secret)?

Do you have information that needs to be accurate?

Do you have information that must be available when you need i?

If you have answered any of these questions, then you have a need for information security.

We need information security to reduce the risk of unauthorized information disclosure, modification, and destruction. We need information security to reduce the risk to a level that is acceptable to the business (management). We need information security to improve the way we do business.

(Source: <https://frsecure.com/blog/the-5-ws-of-information-security/> )

**Threats to Information Security**

In Information security threats can be many like Software attacks, theft of intellectual property, identify theft, theft of equipment or information, sabotage, and information extortion.

**Threat** can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm, object or objects if interest.

**Software attack** means attack by Viruses, Worms, and Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behaves differently.

**Malware** is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:

1. Infection Methods (Source: <https://www.geeksforgeeks.org/threats-to-information-security/> )
2. Malware Actions (Source: <https://www.geeksforgeeks.org/threats-to-information-security/> )

**Note-** According to the syllabus we just have to focus on Viruses and Worms, but if anyone wants to get more knowledge click on (Source) in the Document.

Viruses and Worms both are the Malware which uses the **Infection Method.**

**Virus-** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The **Creeper Virus** was first on ARPANET. Example include file Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.

**Worms-** Worms are also self replicating in nature but they don’t hook themselves to a the program on the host computer. Biggest difference between virus and worms is that worms are network aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will for example consume the hard disk space thus slowing down the computer.

**Top 10 Threats to Information Security:** [**https://scsonline.georgetown.edu/programs/masters-technology-management/resources/top-threats-to-information-technology**](https://scsonline.georgetown.edu/programs/masters-technology-management/resources/top-threats-to-information-technology)

**Intruders:**

One of the most publicized threats to security is the intruder (the other is viruses), often referred to as a hacker or a cracker. In an important early study of intrusion, Anderson [ANDE80] indentified three classes of intruders:

* **Masquerader:** An individual who is not authorized to use the computer and who penetrates a system’s access control to exploit a legitimate user’s account.
* **Misfeasor:** A legitimate user who accesses data, program, or resources for which such access is not authorized, or who is authorized for such accesses but misuses his or her privileges.
* **Clandestine user (done secretively, especially because illicit):** An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

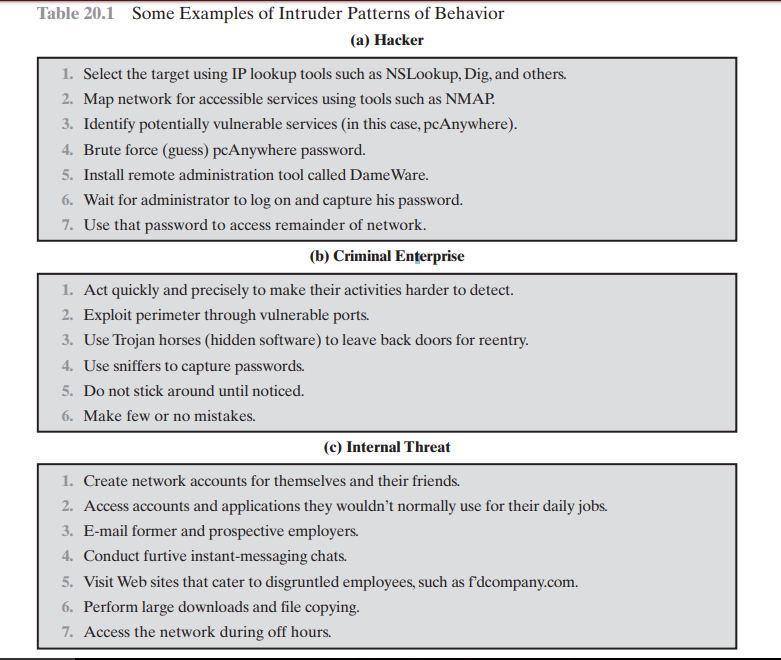
The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine users can be either an outsider or an insider.

Intruder attacks range from the kind to the serious. At the kind end of the scale, there are many people who simply wish to explore internets and see what is out there. At the serious end are individuals who are attempting to read privileged data, perform unauthorized modifications to data, or disrupt the system.

**Intruder Behavior Pattern:**

The techniques and behavior pattern of intruders are constantly shifting, to exploit newly discovered weaknesses and to evade detection and countermeasures. Even so, intruders typically follow one of a number of recognizable behavior patterns, and these patterns typically differ from those of ordinary users. In the following, we look at three broad examples of intruder behavior patterns

1. **Hacker**
2. **Criminal Enterprise**
3. **Internal Threat**



Source: <http://mercury.webster.edu/aleshunas/cosc%205130/chapter-20.pdf>

**What is IDS?**

An Intrusion Detection System (IDS) is a system that attempts to identify intrusions.

An intrusion detection system (IDS) is designed to monitor access points, hostile, and activities. These systems typically trigger on events by referencing network activity against an attack signature database or by monitoring network behavior. If an attack is detected (or believed to be detected), an alert takes place and the event is logged for future reference. Creating and maintaining the attack signature database is the most difficult part of working with IDS technology. It is important to always keep the IDS up to date with the latest signature database provided by the vendor as well as updating the database with the signatures found in testing.

Although intrusion detection system monitors networks for potentially malicious activities, they are also disposed to false alarms.

Intrusion prevention system also monitor network packets inbound the system to check the malicious activities involved in it and it once sends the warning notification.

**Classification of Intrusion Detection System (Source:** <https://www.geeksforgeeks.org/intrusion-detection-system-ids/> **):**

IDS are classified into 5 types:

1. **Network Intrusion Detection System (NIDS):** NIDS are set up to planned point within the network to examine traffic from all devices on the network.
2. **Host Intrusion Detection System (HIDS):** HIDS run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.
3. **Protocol-based Intrusion Detection System (PIDS):** PIDS is trying to secure the web servers by regularly monitoring the HTTPS protocol stream and accepts the related HTTP protocol.
4. **Application Protocol-based Intrusion detection System (APIDS):** APIDS is a system or agent that generally resides within a group of servers. It indentifies the intrusion by monitoring and interpreting the communication on application specific protocol.
5. **Hybrid Intrusion Detection System:** Hybrid Intrusion Detection System s made by the combination of two or more approaches of the intrusion detection system.

**Detection Method of IDS:**

**Signature-based Method:**

Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1’s or number of 0’s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

**Anomaly-based Method:**

Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Extra Source: <https://www.sciencedirect.com/topics/engineering/intrusion-detection-system>

**Insider Threat:** <https://www.imperva.com/learn/application-security/insider-threats/>

**Avenue of Attacks:**

There are mainly 4 avenues of attacks:

1. **Passwords:** The user may use the same password for different places and attacker by any how manage to find that one password and the username and user it for accessing you information over different platforms and there by miss use that information against you or for their interest. The best way to protect ourselves from this avenue we should either you different password for different accounts over different platforms or either use any password management/vault tool to safeguard our password or use two way authentication which means that cross checking if the logger is the authenticated user not the attacker. This can be done by using text message to put on the webpage for authentication or using other things like biometric etc. **There are three different factors of authentication: something you know, have, and are.**
2. **On the Web:** While using web we should be careful while share our information as the attacker can easily access you private information though internet, we should try not to send information on the website not using HTTPS protocol. On social media we should carefully choose our network and use the privacy according to the confidentiality of the information as if you choose public for you private account it is the worst idea while using the Social media.
3. **Email:** Using email is also a very risky for your personal information as they can contain any link that is not suitable for your information or for your computer. They may contain some links that look like some well known websites and actually they are phishing and by entering you username and password will put your information at huge risk, email with spam and the possibility of unsecure transmissions put at risk across all you accounts. You should always make sure that you email service provider provides encryption i.e encrypted data sending and encrypted connection as well.
4. **Mobile:** Mobile devices such as smart phones and tables are prime targets for cyber based attacks. The best way to secure is to download the updated software for the system and update the operating software time to time and also use PIN for security. We should always try not to download any application form an unknown developer as this application can hold with it some threats that can use your personal data or lock down your device. We should also try to use PIN to lock you device for the security.