Cyber Safety is the branch of technology that educates users about the security and safety of the technology they use in their day-to day lives. Users of technology must be aware of the best practices when they use the cloud. Any threat to security is directly making the computer system susceptible to the threat and risking safety of the system. Security of the network and technology is thus very essential for protection from vulnerable risks.

One such significant role in security is played by Trusted Systems. Trusted Systems are special systems designed to serve the purpose of providing security. Safety is ensured by trusted system in a manner by protecting the system against malicious software's and third party intruders. Trusted system allow only verified users to access the computer system. Trusted system are responsible for providing security at different levels and based on different parameters.

Trusted Systems are based on different level of security. They are mentioned as below:

- **Multilevel Security:** This type of Trusted system ensures that security is maintained at different levels of the computer system. It ensures that the information is prevented from being at risk. The different security levels of computer systems are :
    - Top Secret Level
    - Secret Level
    - Confidential Level
    - Unclassified Level
- The order of security level is also given by top level security having the highest priority followed by secret Level priority, confidential Level priority and then least priority is assigned to unclassified level priority. If security is not cleared at one particular level, flow of information is restricted. Also, one important point that must be kept in mind is that 'Read Up' and 'Write Down' are not permitted in multilevel security.
- **Data Access Control:** This type of Trusted system provides additional security to the verified process of log-in. It helps in setting permissions for different users, giving them

limited access and restricting any additional accesses granted. There are three basic models of Data Access Control:

- **Access Matrix:** They are composed of three parts
  - Subject
  - Object
  - Access right
- **Access Control List:** They are composed of different entries of objects depicting user access and the level of access granted (public or private). Access control list demonstrate column-wise split.
- **Capability List:** They are composed of authorized users and the granted operations for them. Users can have multiple capability tickets. Capability list demonstrate row-wise split.

- **Reference Monitor:** This type of trusted system provides hardware level security by limiting the access to objects. Reference monitor maintain security rules ensuring that 'Read Up' and 'Write Down' operations are not performed. Reference monitor ensure that the entire security maintaining process that is carried out is verified and safe.

Importance of Trusted System:

- **Identity Verification:** Trusted systems ensure that only verified users are given access. The verification process takes place that each user is identified uniquely.
- **Safety Maintained:** Trusted system ensures that safety is maintained by preventing direct access to confidential information.
- **Limiting Access:** Permissions and access that are absolutely necessary are granted for users. Unwanted rules and permissions are avoided.
- **Preventing Malicious Activities:** Trusted systems have a mechanism in place to detect and prevent malicious activities such as hacking attempts and unauthorized access.
- **Ensuring Compliance:** Trusted systems help organizations to comply with various regulations and standards such as HIPAA, PCI-DSS, and SOX by providing a secure environment for sensitive information.

Examples of Trusted Systems:

Windows BitLocker: Windows BitLocker is a trusted system that provides encryption for the entire hard drive. It prevents unauthorized access to the data stored on the hard drive by requiring a password or a smart card to unlock the drive.

TPM (Trusted Platform Module): A TPM is a hardware-based security chip that is built into a computer. It provides secure storage for encryption keys and can be used to verify the integrity of the system at boot time.

Trusted Boot: Trusted Boot is a feature that ensures that the system is running a trusted version of the operating system. It works by verifying the integrity of the boot process and ensuring that only signed and trusted software is executed.

Trusted systems are essential for maintaining the security of computer systems and networks. They provide a secure environment for sensitive information and prevent unauthorized access to the system. By implementing trusted systems, organizations can comply with various regulations and standards, and prevent malicious activities such as hacking attempts and unauthorized access.

Trusted systems in cryptography and network security include:

- **Secure identities**: These are essential to protect communication between people, devices, and applications.
- **Trusted computing**: This is a technical systems security initiative.
- **Credit or identity scoring systems**: These are used in financial and anti-fraud applications.
- **Secure operating systems**: These can help secure against Trojan horse attacks.
- **Public-key cryptography**: This allows the creator of keys to have complete control over who has access to them.
- **Trusted systems in the military**: These protect data and resources based on security levels. For example, users can be granted clearances to access certain categories of data.

Here are some other elements of trusted systems:

- **Binding**: Encrypting using a public key
- **Signing**: Using a private key
- **Sealing**: Binding a message with a set of platform metrics
- **Sealed-signing**: Having a signature that is contingent on PCR values