System Security - Precautions & Measures

Computer System face a variety of security threats. All these threats can be broadly classified into 3 categories-

- The first category is **data loss** which means that some data or information can no longer be retrieved. This is generally caused by physical damage or hardware failure of the storage medium.
- The second category is **unauthorized access**. Getting unauthorized access to a system is called hacking.
- The third category of threats consists of **viruses and other harmful programs**. These programs can cause critical damage to a system.

The security of a system can be compromised through following breaches -

1. *Breach of confidentiality*
2. *Breach of integrity*
3. *Breach of availability*
4. *Theft of service*
5. *Denial of service*

The primer of system security is protection of data from theft, corruption and other damages, while allowing the same to remain accessible. Hence primary goals of system security is ***integrity, secrecy*** and ***availability***. System administrators are responsible for ensuring system security. This can be accomplished by following simple practices and precautions discussed below -

- **Firewall** - A system administrator can set up firewall to allow access to legit users and provide limited capabilities to those outside the firewall.
- **Encryption** - Data transferred over the internet is susceptible to potential theft. Encryption is the process of encoding information so that only authorized individuals can view it. Hence, using encryption files and data can be secured.
- **Passwords** - Using passwords or digital signatures is the most commonly used method to prevent unauthorized access. Every password is associated with an authenticated user. Hence **authentication** and **authorization** together make a key component of system security.
- **Physical Security** - Physical protection for the system is crucial. System must be installed in a secured location and its access must be granted to only authorized personnel.
- **System/Console Timeout** - System administrator terminals are high risk if not secured properly. System timeouts ensure that system will be logged out and multiple sessions will be expired if administrator forgets to log out of system.
- **Lean Systems** - Configure your system with minimum essential components, services and packages required for running an application. Using larger number of services increase the risk of system exploitation. Hence any extra service running must be removed. Also unused TCP/UDP ports must be closed.
- **Superuser/User Password** - Administrator password must be set with utmost caution. The password must be lengthy and hard to guess. Use shadow password feature if the system is LINUX based.
- **Delegation of superuser tasks** - If needed, the users must not be given complete privileged access to system and instead Mandatory access control must be implement by propagating privileges appropriately.
- **Securing User Terminals** - Unattended user terminals can be misused. Hence timeout and screen lock out features must be implemented.
- **Restricting Users** - If users of the system are not logging in directly to system you have to configure the system to accept connections from only known IP addresses. Hence user environment must be controlled.
- **Updating Systems** - Security patches or security pack can close most of the known security holes. System pack must be updated and new patches must be installed from time to time as per requirement of system

infrastructure.

- **Vulnerability Testing** - Prevention is better than cure. System must be thoroughly test time to time to assess the security risks and system vulnerabilities.
- **Configuration Documentation** - Any change in the system configuration must be documented and audit trails must be done to monitor the security of system.
- **Backup & Disaster Recovery** - In spite of all the security measures, there are times when system crashes or fails. Hence data must be be backed up from time to time in case of any emergency.
- **Using Change Management Procedures** - whenever changes are made to system, change management methodologies must be used to eliminate unexpected issues and loop holes.
