Whose responsibility is it to secure your system?

(By Prof. Krishna Samdani, Assistant Professor, Computer Engineering Department)

Our society, economy, and critical infrastructures have become largely dependent on computer networks and other information technology solutions. As our dependence on information technology increases, cyber-attacks become more attractive and potentially more disastrous. Cyber-attacks are cheaper, more convenient, and less risky than physical attacks. As per the statistics, 95% of attacks were performed on three industries i.e. government, retail, and technology. Further with the development in the field of Internet of Things (IoT), there is a fivefold increase in the number of devices in the past ten years. Due to which these attacks are predicted to be surged by 300% in the coming years.

System security is the branch of security that deals with,

1. Protecting peripheral components.
2. Protecting distributed contents.
3. Trusted Computing platforms.
4. Detecting intrusion/ malware, protecting data/ access control, authentication.

Thus ensuring fundamental objectives (confidentiality, integrity and availability, authorization, authentication and nonrepudiation).

Challenges of System Security:

1. System security is not as simple as it appears. The requirements seem to be straightforward i.e. ensuring the fundamental objectives: confidentiality, integrity, availability, authorization, authentication and nonrepudiation. But the mechanisms used to meet those requirements can be quite complex.
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases attacks exploit an unexpected weakness in the mechanism.
3. Having designed various security mechanisms, it is necessary to decide where to use/place them. Security mechanisms require that participants have some secret information e.g. encryption key, which raises questions about the creation, distribution, and protection of that secret information.
4. There is a greater advantage to the attacker as he/she only have to find a single weakness and will succeed whereas the administrator needs to eliminate all weakness to achieve perfect security.
5. Lastly, it's a human tendency that people only invest in security mechanisms when a successful security attack is been performed.

Thus it's not only the responsibility of the network administrator or the service provider but also the user's to ensure security standards are met. To attain maximum security from such attacks users should have the knowledge and tools.

The B.Tech program in Cyber Security is defined to ensure that the student not only acquires knowledge of the encryption, program, operating system, database and network security but also meets the relevant industry standards allowing him/her to pursue entry-level roles security administrator, analyst, engineer or auditor.