Secured Systems

Dr. Gaurav Londhe
Assistant Professor, Computer Engineering Department

System Security:

The objective of system security is the protection of information and property from theft, corruption and other types of damage, while allowing the information and property to remain accessible and productive. System security includes the development and implementation of security countermeasures. There are a number of different approaches to computer system security, including the use of a firewall, data encryption, passwords and biometrics.

Cyber Security:

It is a broad vision for today's security professionals to protect the system, with its online financial transactions. Since nowadays the computer systems are more prone to cybercrime. To overcome this, plethora of organizations are working on building and maintaining the more secured and concrete platform for their data privacy and security, in order to protect their precious data, by investing more amount in cyber security professionals with legitimate skillsets.

There are a lot of reasons to pursue a career in cyber security. Across the board, cyber security roles offer competitive pay, growth opportunity, job security, exciting day-to-day tasks and the chance to make a difference.

Cyber Security Course contents

Firewall
One widely used strategy to improve system security is to use a firewall. A firewall consists of software and hardware set up between an internal computer network and the Internet. A computer network manager sets up the rules for the firewall to filter out unwanted intrusions. These rules are set up in such a way that unauthorized access is much more difficult.

A system administrator can decide, for example, that only users within the firewall can access particular files, or that those outside the firewall have limited capabilities to modify the files. You can also set up a firewall for your own computer, and on many computer systems, this is built into the operating system.

Encryption

One way to keep files and data safe is to use encryption. This is often used when data is transferred over the Internet, where it could potentially be seen by others. Encryption is the process of encoding messages so that it can only be viewed by authorized individuals. An encryption key is used to make the message unreadable, and a secret decryption key is used to decipher the message.

Encryption is widely used in systems like e-commerce and Internet banking, where the databases contain very sensitive information. If you have made purchases online using a credit card, it is very likely that you've used encryption to do this.

Passwords

The most widely used method to prevent unauthorized access is to use passwords. A password is a string of characters used to authenticate a user to access a system. The password needs to be kept secret and is only intended for the specific user. In computer systems, each password is associated with a specific username since many individuals may be accessing the same system.

Cryptography

Cryptographic systems are generally classified along 3 independent dimensions: Type of operations used for transforming plain text to cipher text All the encryption algorithms are based on two general principles: substitution, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged.

Crypto analysis The process of attempting to discover X or K or both is known as cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst.

There are various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst. Cipher text only – A copy of cipher text alone is known to the cryptanalyst. Known plaintext – The cryptanalyst has a copy of the cipher text and the corresponding plaintext.

For More details check the following link:

https://gaurav6282.wixsite.com/talktosecure