The Concepts of Authentication, Authorization and Encryption

Authentication

Attackers can try to gain access to sensitive data and services. Access control limits is one of the way to secure the sensitive data. It give limitations to users who or what can use specific resources as well as the services or options available once access is granted.

The simplest and easiest form of authentication is passwords. This method is easy to implement but also the weakest and least secure. Password-only logins are very vulnerable to brute force attacks and provides no accountability. Anyone with the password can gain entry to the device and alter the configuration.

There are many types of authentication methods which are better than passwords.

- Certificate-Based Authentication: -This type uses an x.509 certificate for public/private key technology.
- Token-Based Authentication: - A token, such as SecurID, is a hardware device that displays an authentication code for 60 seconds; a user uses this code to log into a network.
- Biometric Authentication: - This type uses a physical characteristic such as fingerprint, eye iris, or handprint to authenticate the user.

graduatefixer.com

Authorization

After users are successfully authenticated against the selected data source, they are than authorized for specific data or database or network resources. Authorization is basically what a user can and cannot do on the network after that user is authenticated.

Authorization is typically implemented using a AAA server-based solution. Authorization uses a created set of attributes that describes the user's access to the specific data or database. These attributes are compared to information contained within the AAA database, and determination of restrictions for that user is made and delivered to the local router where the user is connected.

Encryption

Need help with the assignment?

Our professionals are ready to assist with any writing!

GET HELP

Encryption can be used to encrypt data while it is in transit or while it's stored on a hard drive. Cryptography is the study of protecting information by mathematically scrambling the data, so it cannot be deciphered without knowledge of the mathematical formula used to encrypt it. This mathematical formula is known as the encryption algorithm. Cryptography is composed of two words: crypt (meaning secret or hidden) and graphy (meaning writing). Cryptography literally means secret or hidden writing. Cleartext is the plan text which can be read by everyone and understandable data, and cipher text is the scrambled text as a result of the encryption process. Cipher text should be unreadable and show no repeatable pattern to ensure the confidentiality of the data.

There are three critical elements to data security. Confidentiality, integrity, and authentication are known as the CIA triad. Data encryption provides confidentiality, meaning the data can only be read by authorized users. Message hashing provides integrity, which ensures the data sent is the same data received and the information was not modified in transit. Message digital signatures provide authentication (ensuring users are who they say they are) as well as integrity. Message encrypting, and digital signatures together provide confidentiality, authentication, and integrity.

gradesfixer.com

Need help with the assignment?

Our professionals are ready to assist with any writing!

GET HELP