# Authentication if the message is intercepted by

Authentication refers to the task of verifying the identity of aperson/software connecting to an application. The simplest form ofauthentication consists of a secret password that must be presented when a userconnects to the application. Unfortunately, passwords are easily compromised, for example, by guessing, or by sniffing of packets on the network if thepasswords are not sent encrypted.

More robust schemes are needed for criticalapplications, such as online bank accounts. Encryption is the basis for morerobust authentication schemes. Many applications use two-factor authentication, where two independentfactors (that is, pieces of information or processes) are used to identifya user. The two factors should not share acommon vulnerability; for example, if a system merely required two passwords, both could be vulnerable to leakage in the same manner. While biometrics suchas fingerprints or iris scanners can be used in situations where a user isphysically present at the point of authentication, theyarenot very meaningful across a network. Passwords are used as the first factor inmost such two-factor authentication schemes. Smart cards or other encryptiondevices connected through the USBinterface, which can be used for authentication based on encryption techniques are widelyused as second factors.

Encryption refers to the process oftransforming data into a form which cannot be readable. unless the reverseprocess of decryption is applied. Encryption algorithmsuse an encryption key to performencryption, and require a decryption key (whichcould be the same as the encryptionkey depending on the encryption algorithmused) to perform decryption.

Previouslyit was used for transmitting messages, using a secret key known only to thesender and the intended receiver. Even if the message is intercepted by anenemy, the enemy, not knowing the key, will not be able to decrypt andunderstand the message which was sent. Encryption is widely used today forprotecting data in transit in a variety of applications such as data transferon the Internet, and on cellular phone networks.

Encryption is also used tocarry out other tasks, such as authentication  After users are successfullyauthenticated against the selected data source, they are than authorized forspecific data or database or network resources. Authorization is basically whata user can and cannot do on the network after that user is authenticated. Authorization is typicallyimplemented using a AAA server-based solution. Authorization uses a created setof attributes that describes the user’s access to the specific data ordatabase. These attributes are compared to information contained within the AAAdatabase, and determination of restrictions for that user is made and deliveredto the local router where the user is connected.