

## Computer Security Authentication by Kent Pinkerton

Computer security authentication means verifying the identity of a user logging onto a network. Passwords, digital certificates, smart cards and biometrics can be used to prove the identity of the user to the network. Computer security authentication includes verifying message integrity, e-mail authentication and MAC (Message Authentication Code), checking the integrity of a transmitted message. There are human authentication, challenge-response authentication, password, digital signature, IP spoofing and biometrics.

Human authentication is the verification that a person initiated the transaction, not the computer. Challenge-response authentication is an authentication method used to prove the identity of a user logging onto the network. When a user logs on, the network access server (NAS), wireless access point or authentication server creates a challenge, typically a random number sent to the client machine. The client software uses its password to encrypt the challenge through an encryption algorithm or a one-way hash function and sends the result back to the network. This is the response.

Two-factor authentication requires two independent ways to establish identity and privileges. The method of using more than one factor of authentication is also called strong authentication. This contrasts with traditional password authentication, requiring only one factor in order to gain access to a system. Password is a secret word or code used to serve as a security measure against unauthorized access to data. It is normally managed by the operating system or DBMS. However, a computer can only verify the legality of the password, not the legality of the user.

The two major applications of digital signatures are for setting up a secure connection to a website and verifying the integrity of files transmitted. IP spoofing refers to inserting the IP address of an authorized user into the transmission of an unauthorized user in order to gain illegal access to a computer system.

Biometrics is a more secure form of authentication than typing passwords or even using smart cards that can be stolen. However, some ways have relatively high failure rates. For example, fingerprints can be captured from a water glass and fool scanners.