Week 3 Portfolio

# Authentication:

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

Logically, authentication precedes [authorization](http://searchsoftwarequality.techtarget.com/definition/authorization) (although they may often seem to be combined). The two terms are often used synonymously but they are two different processes.

[User authentication](http://searchsecurity.techtarget.com/definition/user-authentication) occurs within most human-to-computer interactions other than guest accounts, automatically logged-in accounts and kiosk computer systems. Generally, a user must enter or choose an ID and provide their password to begin using a system. User authentication authorizes human-to-machine interactions in operating systems and applications as well as both wired and wireless networks to enable access to networked and Internet-connected systems, applications and resources.

# Encryption:

In computing, encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks. Unencrypted data, often referred to as [plaintext](http://searchsecurity.techtarget.com/definition/plaintext), is encrypted using an encryption [algorithm](http://whatis.techtarget.com/definition/algorithm) and an encryption [key](http://searchsecurity.techtarget.com/definition/key). This process generates [ciphertext](http://whatis.techtarget.com/definition/ciphertext) that can only be viewed in its original form if decrypted with the correct key. Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied. Today's most widely used encryption algorithms fall into two categories: symmetric and asymmetric.

# Hashing:

When a user sends a secure message, a hash of the intended message is generated and encrypted and is sent along with the message. When the message is received, the receiver decrypts the hash as well as the message. Then, the receiver creates another hash from the message. If the two hashes are identical when compared, then a secure transmission has occurred. This hashing process ensures that the message is not altered by an unauthorized end user.

Hashing is used to index and retrieve items in a database because it is easier to find the item using the shortened hashed key than using the original value.

Hash code typically is smaller of its original plain text. For this reason, to compare two large data volumes for equivalence it compares their checksums, which were calculated using same algorithm for both data arrays. It's a way much faster than comparing every character and every single bit in two data arrays.

# PKI (Public Key Infrastructure):

A public key infrastructure (PKI) supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over [networks](http://searchnetworking.techtarget.com/definition/network) such as the [Internet](http://searchwindevelopment.techtarget.com/definition/Internet) and verify the identity of the other party.

A typical PKI consists of hardware, software, policies and [standards](http://whatis.techtarget.com/definition/standard) to manage the creation, administration, distribution and revocation of keys and [digital certificates](http://searchsecurity.techtarget.com/definition/digital-certificate). Digital certificates are at the heart of PKI as they affirm the identity of the certificate subject and bind that identity to the [public key](http://searchsecurity.techtarget.com/definition/public-key) contained in the certificate.

PKI provides a chain of trust, so that identities on a network can be verified. However, like any chain, a PKI is only as strong as its weakest link. There are various standards that cover aspects of PKI -- such as the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC2527) -- but there is no predominant governing body enforcing these standards. Although a CA is often referred to as a “trusted third party,” shortcomings in the security procedures of various CAs in recent years has jeopardized trust in the entire PKI on which the Internet depends. If one CA is compromised, the security of the entire PKI is at risk. For example, in 2011, Web browser vendors were forced to [blacklist](http://searchexchange.techtarget.com/definition/blackhole-list) all certificates issued by the Dutch CA DigiNotar after more than 500 fake certificates were discovered.

# RADIUS (Remote Authentication Dial In User Service):

The Remote Authentication Dial-In User Service (RADIUS) protocol was developed by Livingston Enterprises, Inc., as an access server authentication and accounting protocol.

Communication between a network access server (NAS) and a RADIUS server is based on the User Datagram Protocol (UDP). Generally, the RADIUS protocol is considered a connectionless service. Issues related to server availability, retransmission, and timeouts are handled by the RADIUS-enabled devices rather than the transmission protocol.

RADIUS is a client/server protocol. The RADIUS client is typically a NAS and the RADIUS server is usually a daemon process running on a UNIX or Windows NT machine. The client passes user information to designated RADIUS servers and acts on the response that is returned. RADIUS servers receive user connection requests, authenticate the user, and then return the configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

This figure shows the interaction between a dial-in user and the RADIUS client and server.

# TACAS (Terminal Access Controller Access Control System):

TACACS (Terminal Access Controller Access Control System) is an older [authentication](http://searchsecurity.techtarget.com/definition/authentication)[protocol](http://searchnetworking.techtarget.com/definition/protocol) common to [UNIX](http://searchenterpriselinux.techtarget.com/definition/Unix) networks that allows a remote access server to forward a user's logon password to an authentication [server](http://whatis.techtarget.com/definition/server) to determine whether [access](http://whatis.techtarget.com/definition/access) can be allowed to a given system. TACACS is an [encryption](http://searchsecurity.techtarget.com/definition/encryption) protocol and therefore less secure than the later TACACS+ and [Remote Authentication Dial-In User Service](http://searchsecurity.techtarget.com/definition/RADIUS) protocols. A later version of TACACS is XTACACS (Extended TACACS). Both are described in [Request for Comments](http://whatis.techtarget.com/definition/Request-for-Comments-RFC) 1492.

# CHAP (Challenge Handshake Authentication Protocol):

CHAP (Challenge-Handshake Authentication Protocol) is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP). Here's how CHAP works:

After the link is made, the server sends a challenge message to the connection requestor. The requestor responds with a value obtained by using a one-way hash function.

The server checks the response by comparing it its own calculation of the expected hash value.

If the values match, the authentication is acknowledged; otherwise theconnection is usually terminated.

At any time, the server can request the connected party to send a new challenge message. Because CHAP identifiers are changed frequently and because authentication can be requested by the server at any time, CHAP provides more security than PAP. RFC1334 defines both CHAP and PAP.