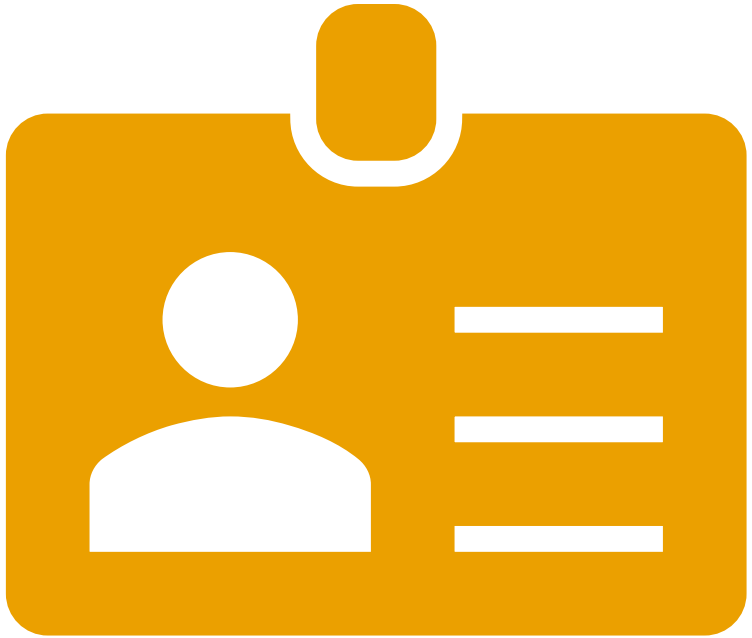
Lesson 10: Authentication and Identity Management



What is Access?

Access is the data flow between a subject and an object

Subject is a person, process or program

Object is a resource (server, printer, etc.)

ACL – Access Control List

Authentication terms

- *Security tokens* are similar to certificates. They contain the rights and access privileges of the token bearer as part of the token.
- *Smart cards* usually contains a small amount of memory that can be used to store permissions and access information.
- One type of smart card is the *Common Access Card (CAC)*. A picture appears on the front of the card with an integrated chip beneath and a barcode. On the back of the card, there is a magnetic strip and another barcode. This is used in the US Military.
- *Personal Identity Verification (PIV)* is used for federal employees and contractors, much as CAC is used for military

Authentication terms

A *Federation* is a collection of computer networks agreeing upon standards of operation.

Transitive access, one party (A) trusts another party (B). If the second party (B) trusts another party (C), then A trusts C.

Access Control Models

Subject—An active entity on an information system

Object—A passive data file

MAC Mandatory Access Control (MAC): Highest level of Control. Permissions are explicitly denied unless otherwise changed. The OS is in control of the data. This model is used with highly confidential data, such as military or government.

DAC Discretionary Access Control (DAC): Allows owners of data to specify what users can access data used most. Access control is based on discretion of data owners. Most common model. Users themselves can assign access to their own data.

Role Based Access Control (RBAC): (also called Non-discretionary access control) Centrally controlled model allows access based on the role the user holds in the organization; often hierarchical. Access is given to a group of users that perform a similar function. Based on the separation of duties.

Access Control Models (Continued)

- *Rule-Based Access Control (RBAC)* uses the settings in preconfigured security policies (i.e. rules) to make all access control decisions.
- Lattice Based Access Control: a security access methodology that assigns access permissions to both users and objects, creating a grid or lattice layout. A user cannot access an object with a security level greater that his/her own on the lattice.

ABAC

- NIST 800-162 Attributed Based Control Definition and Considerations
- "A logical access control methodology where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes."

ABAC

- Attributes are characteristics that define specific aspects of the subject, object, environment conditions, and/or requested actions that are predefined and pre-assigned by an authority.
- A subject is an active entity (generally an individual, process, or device)
- An object is a passive information system-related entity
- An operation is the execution of a function at the request of a subject upon an object. Operations include read, write, edit, delete, author, copy, execute, and modify

ABAC

- Access Control Mechanism Assesses:

a)Rules

b)Subject Attributes

c)Object Attributes

d)Environmental Conditions

The 4 A’s of Access Control

- Authentication
- Authorization
- Access Control
- Auditing

- Note some sources refer to triple AAA security meaning Authentication, Access Control, and Auditing.
- The term “AAA” is often used, describing cornerstone concepts Authentication, Authorization, and Accountability. The Access Control is left out or considered part of Authorization

Content Dependent Access Controls

- Access is determined by the type of data.
  - Example, email filters that look for specific things like “confidential”, “SSN”, images.
  - Web Proxy servers may be content based.

Context Dependent Access Control

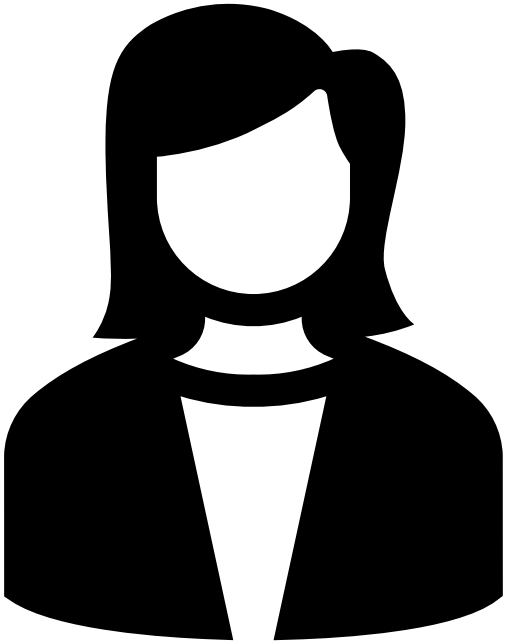
- System reviews a situation then makes a decision on access.
  - A firewall is a great example of this, if session is established, then allow
  - Another example, allow access to certain body imagery if previous web sessions are referencing medical data.

Access Control Categories

LOGICAL (TECHNICAL) ACCESS CONTROLS ARE USED THINGS LIKE SMART CARDS AND BIOMETRICS, AND PASSWORDS, AND AUDIT SYSTEMS.

ADMINISTRATIVE ACCESS CONTROLS

PHYSICAL ACCESS CONTROLS



Identification

- Identifies a user uniquely
- UID, SID, Username, email, employee ID (there are reasons why SSN is not a good choice)
- Should Uniquely identify a user for accountability
- Identifier should not indicate extra information about user such as job title or position

Authentication

1

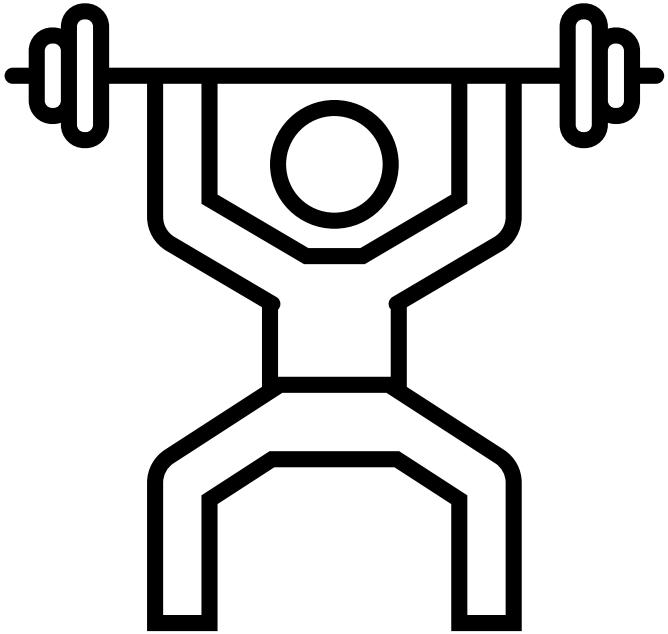
Type I
Something you know

2

Type II
Something you have

3

Type III
Something you are



Strong Authentication

- Strong Authentication is the combination of 2 or more of these (also called multi-factor authentication) Strong Authentication provides a higher level of *assurance*

Access Control Approaches

- Centralized Access Control - Centralized access control concentrates access control in one logical point for a system or organization.
- Decentralized Access Control – Locally controlled. Decentralized access control is also called distributed access control

Access Control Matrix

Access Control Matrix

Is a table of subjects and objects indicating what actions individual subjects can take upon individual objects.

Two types

Capability Table (bound to a subject)

Access Control List (bound to an object

Account Management

- Naming conventions: Never have a name the resembles a job position
- Limit Logon attempts
- Expiration Dates: Have your accounts expire
- Disable account when employee leaves company
- Time restrictions
- Machine restrictions
- Password policies
- Minimum password length
- Password rotation: systems remember old passwords, cannot reuse
- Password aging: Force users to change password regularly

Three steps to authorization

Identification: Who is the user?

Authentication: Is this user really who they claim to be?

Authorization: What resources does the user have permission to access?

TOTP & HOTP

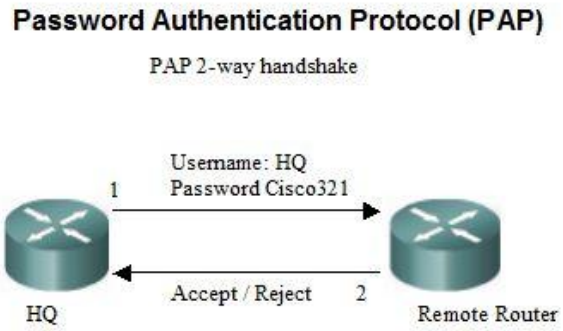
- Time-Based One-Time Password It is an algorithm that derives a one-time password from a shared secret key and the time. It is defined by RFC 6238. The current time stamp and a pre-shared key are combined using a cryptographic hash function to generate a one time password.
- HOTP or HMAC-based One-time Password Algorithm
- Is an HMAC one-time password

Authentication protocols

- The next few slides discuss authentication protocols. They are in chronological order starting with the oldest. You must know each of these for the test.

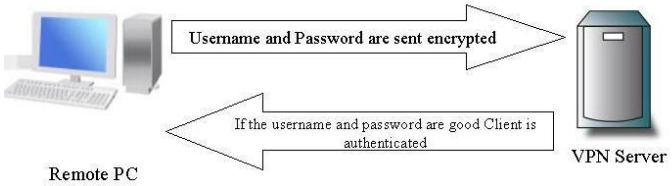
PAP

PAP is an acronym for *Password Authentication Protocol*. It is the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted, however the transmissions of the passwords are in clear text, unencrypted. This is the main weakness with PAP. The Basic Authentication feature built into the HTTP protocol uses PAP



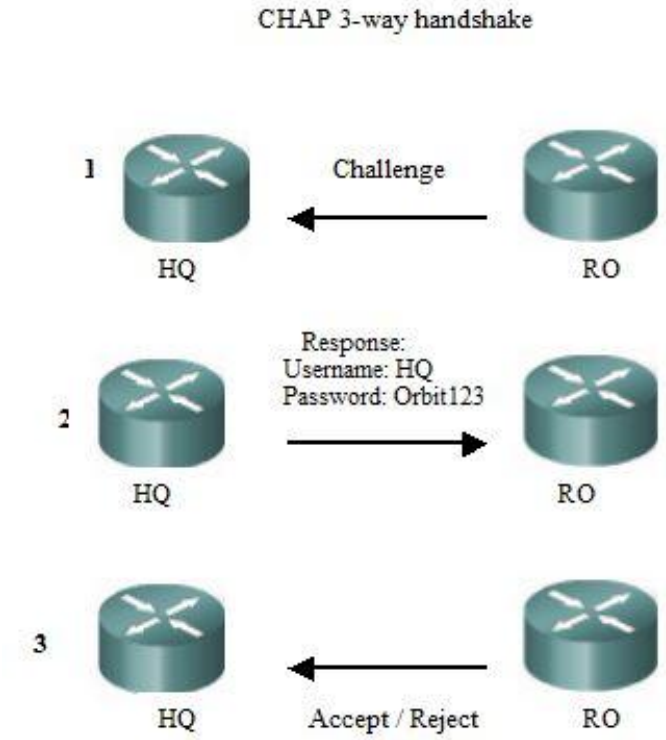
S-PAP

- SPAP is an acronym for Shiva Password Authentication Protocol. SPAP is a proprietary version of PAP. Most experts consider SPAP somewhat more secure than PAP. This is because the username and password are both encrypted when they are sent, unlike PAP which sends them in clear text



Authentication - CHAP

- **Challenge-Handshake Authentication Protocol**
- After the Link Establishment phase is complete, the authenticator sends a "challenge" message to the peer.
- The peer responds with a value calculated using a "one-way hash" function.
- The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise the connection SHOULD be terminated.
- At random intervals, the authenticator sends a new challenge to the peer, and repeats steps 1 to 3
- MS- CHAP is Microsoft version of CHAP.



EAP

- Extensible Authentication Protocol
- A framework frequently used in wireless networks and point-to-point connections. Originally defined in RFC 3748 but updated since then. It handles the transport of key's and related parameters. There are several versions of EAP.

EAP Variations

- LEAP - Lightweight Extensible Authentication protocol was developed by Cisco and has been used extensively in Wireless communications. LEAP is supported by many Microsoft operating systems including Windows 7. LEAP uses a modified version of MS-CHAP.
- Extensible Authentication Protocol - Transport Layer Security utilizes TLS in order to secure the authentication process. Most implementations of EAP-TLS utilize X.509 digital certificates to authenticate the users.
- Protected Extensible Authentication Protocol encrypts the authentication process with an authenticated TLS tunnel. PEAP was developed by a consortium including Cisco, Microsoft, and RSA Security. It was first included in Microsoft Windows XP.

Kerberos - Overview

Kerberos uses symmetric cryptography

Authentication is UDP port 88

AS generates a secret key by creating a hash of the user password then sends 2 messages to client

A) CLIENT/TGS Session Key encrypted with secret key of client

B) TGT includes client ID, client network address, validity period.

The messages are encrypted using the key the AS generated

Then the user attempts to decrypt message A with the a secret key generated by the client hashing the users entered password. If that entered password does not match the password the AS found in the database, then the hashes won't match, and the decryption won't work. If it does work, then message A contains the Client/TGS session key that can be used for communications with the TGS. Message B is encrypted with the TGS secret key and cannot be decrypted by the client.

Kerberos - Overview

- When requesting services, the client sends the following messages to the TGS:
  - Message C: Composed of the TGT from message B and the ID of the requested service.
  - Message D: Authenticator (which is composed of the client ID and the timestamp), encrypted using the *Client/TGS Session Key*.
- Upon receiving messages C and D, the TGS retrieves message B out of message C. It decrypts message B using the TGS secret key. This gives it the "client/TGS session key". Using this key, the TGS decrypts message D (Authenticator) and sends the following two messages to the client:
  - Message E: *Client-to-server ticket* (which includes the client ID, client network address, validity period and *Client/Server Session Key*) encrypted using the service's secret key.
  - Message F: *Client/Server Session Key* encrypted with the *Client/TGS Session Key*.

Kerberos - Overview

.

Upon receiving messages E and F from TGS, the client has enough information to authenticate itself to the Service Server (SS).
The client connects to the SS and sends the following two messages:

- Message E from the previous step (the client-to-server ticket, encrypted using service's secret key).
- Message G: a new Authenticator, which includes the client ID, timestamp and is encrypted using Client/Server Session Key.

The SS decrypts the ticket (message E) using its own secret key to retrieve the Client/Server Session Key. Using the sessions key, SS decrypts the Authenticator and sends the following message to the client to confirm its true identity and willingness to serve the client:

- Message H: the timestamp found in client's Authenticator

The client decrypts the confirmation (message H) using the Client/Server Session Key and checks whether the timestamp is correct. If so, then the client can trust the server and can start issuing service requests to the server.
The server provides the requested services to the client

Kerberos - BASIC

User

KDC

Key Distribution Center

AS

(Authentication Service)

TGS

(Ticket Granting Service)

Step 1: User is authenticated by AS

Step 2:AS directs TGS to create TGT

Step 3: TGT is sent back to user.
Encrypted with symmetric key known only to KDC

Step 4: User requests service ticket, sends TGT to KDC

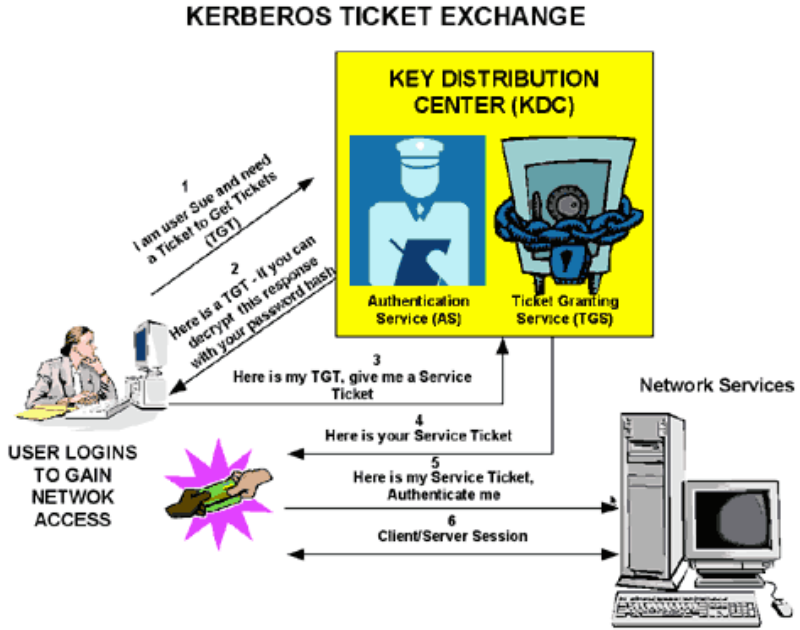
Step 5: KDC sends service ticket to user.
Good for <5 min symmetric key known to KDC and Service

Service (some server/service the user wants to access)

Step 6: User sends service ticket to service

Kerberos Continued

The following image is from Microsoft MSDN description of Kerberos at https://msdn.microsoft.com/en-us/library/bb742516.aspx



Kerberos - Continued

- Kerberos components
  - Principal – a server or client that Kerberos can assign tickets to
  - Authentication Service (AS)– Server that gives authorizes the principal and connects them to the Ticket Granting Service
  - Ticket Granting Service (TGS)– provides tickets
  - Key Distribution Center (KDC) –A server that provides the initial ticket and handles TGS requests. Often it runs both AS and TGS services
  - Ticket Granting Ticket (TGT) the ticket that is granted during the authentication process
  - Ticket – used to authenticate to the server. Contains identity of client, session key, timestamp, and checksum. Encrypted with servers key.
  - Session key- temporary encryption key
  - Authenticator = proves session key was recently created. Often expires within 5 minutes
  - Realm: a boundary within an organization. Each realm has its own AS and TGS
  - Remote Ticket Granting Server (RTGS) – A TGS in a remote realm

NOTE: The test has heavy emphasis on Kerberos. Make sure you know it well.

SPNEGO

Simple and Protected GSS-API Negotiation Mechanism (pronounced “spenay-go”). GSS-API stands for Generic Security Service Application Program Interface.

SPNEGO is used when a client application wants to authenticate to a remote server, but neither end is sure what authentication protocols the other supports.

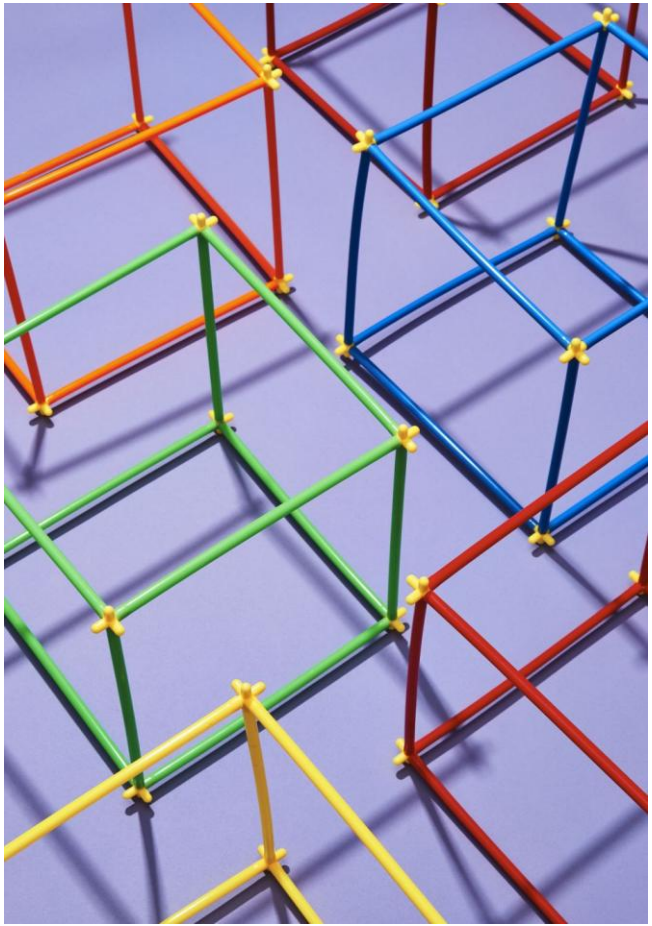
This is used in Microsoft’s HTTP Negotiate authentication extension.

https://www.ibm.com/docs/en/was/8.5.5?topic=SSEQTP_8.5.5/com.ibm.websphere.nd.multiplatform.doc/ae/csec_SPNEGO_explain.htm

OATH

Open Standard for Authorization (OATH) is a common method for authorizing websites or applications to access information. It allows users to share information with third party applications.

It is designed to work with HTTP and allows access tokens to be issued to third-party clients with the approval of the resource owner. Thus a resource owner, such as a social media website user, can authorize a third party to access his or her data.



SESAME

Secure European System for Applications in a Multi-vendor Environment

European technology, developed to extend Kerberos and improve on it’s weaknesses

Sesame uses both symmetric and asymmetric cryptography.

Uses “Privileged Attribute Certificates” rather than tickets, PACS are digitally signed and contain the subjects identity, access capabilities for the object, access time period and lifetime of the PAC.

PACS come from the Privileged Attribute Server.

KRYPTOKNIGHT

Developed by IBM Zurich and Yorktown Research Laboratories

Three types of principles: users, programs(services), and authentication servers.

Four service classes: SSO, Two Party Authentication, Key Distribution, Authentication of origin and contents of data.

https://www.zurich.ibm.com/security/past-projects/kryptoknight/

Remote access

- The next few slides discuss remote access protocols. They are in chronological order

RADIUS

Remote Authentication Dial In User Service , used for authentication.

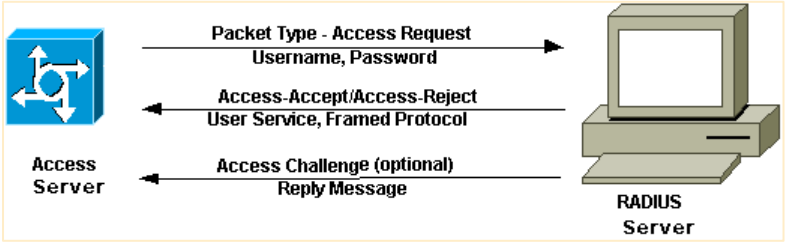
Provides AAA

It was developed in 1991, but is still used frequently. RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP as transport.

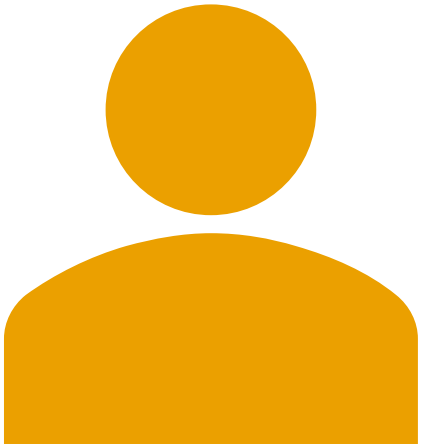
Once authenticated, RADIUS also determines what rights or privileges the user or computer is authorized to perform and maintains a record of this access (i.e. Auditing)

RADIUS authentication

1. User credentials are past to the Remote Access Server (RAS) using PPP (Point to Point Protocol)
2. The RAS sends a Radius Access Request message to the RADIUS Server.
3. That request includes username/password or certificate. It may also contain other information such as IP address.
4. RADIUS server checks the information using some authentication protocol such as CHAP or EAP or even Kerberos.
5. RADIUS Server then sends one of three responses to the RAS
6. a) Access rejected
7. b) Access accepted
8. c) Access challenged (i.e. more information needed perhaps a token, card, PIN, etc.)



Realms (used in RADIUS and other protocols)



- A realm is commonly appended to a user's user name and delimited with an '@' sign, resembling an email address domain name. This is known as postfix notation for the realm. Another common usage is prefix notation, which involves prepending the realm to the username and using '\' as a delimiter. Modern RADIUS servers allow any character to be used as a realm delimiter, although in practice '@' and '\' are usually used.

Diameter

- Successor to RADIUS
- Backwards compatible
- RFC 3588
- AAA services
- Uses EAP
- TCP instead of UDP (like RADIUS)
- Uses port 3868

Diameter

- Diameter Applications extend the base protocol by adding new commands and/or attributes, such as those for use with the Extensible Authentication Protocol (EAP).
- Diameter protocol was initially developed by Pat R. Calhoun, Glen Zorn, and Ping Pan in 1998 to provide a framework for authentication, authorization and accounting (AAA) that could overcome the limitations of RADIUS. RADIUS had issues with reliability, scalability, security and flexibility. RADIUS cannot deal effectively with remote access, IP mobility and policy control. The Diameter protocol defines a policy protocol used by clients to perform policy, AAA, and resource control. This allows a single server to handle policies for many service

TACACS

- Family of protocols including TAXACS+
- Terminal Access Controller Access Control System defined in RFC 1492, and uses (either TCP or UDP) port 49 by default
- The most current method or level of TACACS is TACACS+, and this replaces the previous two incarnations. TACACS+ allows credentials to be accepted from multiple methods, including Kerberos. TACACS+ is not backward compatible.
- TACACS+ and RADIUS have generally replaced TACACS and XTACACS in more recently built or updated networks. TACACS+ is an entirely new protocol and is not compatible with its predecessors, TACACS and XTACACS. TACACS+ uses TCP (while RADIUS operates over UDP).

TACACS extensions

Extended TACACS (XTACACS) is a proprietary extension to TACACS introduced by Cisco Systems in 1990 without backwards compatibility to the original protocol. TACACS and XTACACS both allow a remote access server to communicate with an authentication server in order to determine if the user has access to the network.

Terminal Access Controller Access-Control System Plus (TACACS+) is a protocol developed by Cisco and released as an open standard beginning in 1993. Although derived from TACACS, TACACS+ is a separate protocol that handles authentication, authorization, and accounting (AAA) services. TACACS+ and other flexible AAA protocols have largely replaced their predecessors.

TACACS+ versus RADIUS

- TCP rather than UDP
- Message body fully encrypted
- AAA services provided independently
- Flexible Authentication
- Multiprotocol

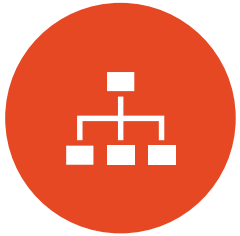
Control types

- Deterrent – intended to discourage attacks
- Preventative – intended to prevent incidents
- Detective – intended to detect incidents
- Corrective – intended to correct incidents
- Recovery – intended to bring controls back up to normal operation
- Compensative – provides alternative controls to other controls

Note: you must be able to identify and differentiate these for the test

Administrative Controls

PERSONNEL



SUPERVISORY

TRAINING

TESTING

Physical Controls

- Physical Network Segregation
- Perimeter Security – CCTV, fences, security guards, badges
- Computer Controls – physical locks on computer equipment, restrict USB access, etc.
- Work Area Separation
- Cabling – shielding, Fiber, TEMPEST
- Control Zone – break up office into logical areas (lobby – public, R&D- Top Secret, Offices – secret)

Technical or Logical controls

Using technology to protect

System Access – Kerberos, 2-Factor authentication, TACACS+

Network Architecture – IP subnets, VLANS , DMZ

Network Access – Routers, Gateways, and Firewalls that control access

Encryption – protect confidentiality, integrity

Auditing

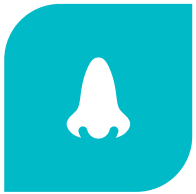
Single Sign On

Log in one time, and access resources many places

Not the same as password synchronization

SSO software handles the authorization to multiple systems

Attacks on Password



SNIFFING (ELECTRONIC MONITORING)

BRUTE FORCE ATTACKS

DICTIONARY ATTACK

SOCIAL ENGINEERING (WHAT IS SOCIAL ENGINEERING?)

RAINBOW TABLES – A TABLE THAT CONTAINS PASSWORDS IN HASH FORMAT FOR EASY/QUICK COMPARISON

Cognitive passwords

- Not really passwords, but facts that only a user would know. Can be used to verify who you are talking to without giving out password, or for password reset challenges. Also called ‘out of band authentication’

One Time Password

- Password is good only once then no longer valid
- Used in high security environments
- VERY secure
- Not vulnerable to electronic eavesdropping, but vulnerable to loss of token, (though must have pin)
- Require a token device to generate passwords. (RSA SecureID key is an example)

Other types

Digital signatures

Passphrases

Smart cards

Biometrics

Biometrics verifies (authenticates) an individuals identity by analyzing unique personal attribute (something they ARE)

Systems can be calibrated, for example of you adjust the sensitivity to decrease fall positives, you probably will INCREASE false negatives, this is where the CER come in.

CER

- Crossover Error Rate (CER)* is an important metric that is stated as a percentage that represents the point at which the false rejection rate equals the false positive rate.
- Lower number CER is better/more accurate*. (3 is better than an 4)
- Also called Equal Error Rate
- Use CER to compare vendors products objectively

Biometric Types Overview

- Fingerprint
- Palm Scan
- Hand Geometry
- Retina Scan
- Iris Scan
- Keyboard Dynamics
- Voice Print
- Facial Scan
- Hand Topography

Emanation Countermeasures

Faraday cage – a metal mesh cage around an object, it negates a lot of electrical/magnetic fields.

White Noise – a device that emits uniform spectrum of random electronics signals. You can buy sounds frequency white noise machines. (call centers, doctors)

Control Zones – protect sensitive devices in special areas with special walls etc.

Other Technology

SAML (Security Assertion Mark-up Language) defines a standard protocol to exchange authentication and authorization assertions. It uses WS-Security standard to protect assertions while their transmission.

OAUTH allows an end user's account information to be used by third-party services, without exposing the user's password.

Shibboleth is a single sign on system, but it works with federated systems. Shibboleth is a middleware solution for authentication and identity management that uses SAML and works over the internet.

OpenID connect works with the Oauth 2.0 protocol and supports multiple clients including web based and mobile clients. OpenID connect also supports REST