**Module 4 Identity & Access Management**

**4.2 Access Protocols**

**Directories/Directory Service Protocols**

* Repositories of organisation’s network resources & users
* Most follow hierarchical database format, based on X.500 standard
* Directory service manages entries & data in directory & enables access control & identity management
* Types – Microsoft Active Directory (AD) & LDAP

**Lightweight Directory Access Protocol (LDAP)**

* Standardised directory access protocol
* Main purpose is query the LDAP user database – pared-down X.500-based directories
* Supported by most major vendors including Microsoft AD & OpenLDAP
* Hierarchical structure

1. CN=Pitchers Name, OU=Pitchers, O=Baseball Team, DN=example.com, C=US

**LDAP Security**

* LDAP vulnerable to snooping
* Encrypt communications using SSL/TLS to secure LDAP transmissions
* Certificates can validate authentication requests
* LDAPv3 bind requests should use Simple Authentication & Security Layer (SASL)

**Kerberos**

* Symmetric key authentication protocol
* Kerberos v5 uses mutual authentication between requesting client & supporting server through Key Distribution Centre (KDC)
* Once authenticated with KDC, user given a *Ticket Granting Ticket (TGT)*

1. Tickets encrypted & have limited life span
2. Ticket lists user’s privileges

* Each time user wishes to access some resource on network, user’s computer presents KDC with TGT; TGT then sends user’s computer a *Service Ticket*, granting user access to that service

**Kerberos Authentication Process**

* Each time user wishes to access some resource on network, user’s computer presents KDC with the TGT
* TGT then sends user’s computer a *Service Ticket*, granting user access to that service
* User’s computer then sends service ticket to server user trying to access
* As final authentication check, server communicates with TGT to confirm & validate service ticket

**Remote Authentication Dial-In User Service (RADIUS)**

* IETF (Internet Engineering Task Force) standard
* Implemented by most major OS manufacturers
* Uses UDP transport to centralised server providing authentication & access control for networks

**Terminal Access Controller Access Control System Plus (TACACS+)**

* Handles authentication, authorisation & accounting (AAA) services
* Similar to RADIUS
* TCP rather than UDP as its transport method
* Client/server model
* TACACS+ advantages over RADIUS

1. TCP rather than UDP as transport method – more reliable
2. Encrypts entire packet, not just authentication
3. Controls authorisation of router commands

**Password Authentication Protocol (PAP)**

* Legacy
* User ID & password sent clear text
* No protection for playback/trial-and-error attack

**Challenge Handshake Authentication Protocol (CHAP)**

* Provides on-demand authentication over encrypted channels
* Server first authenticates client
* Client generates one-way hashing function (MD5 algorithm) & send to service
* Client hash compared against service’s hash by *authenticator service*
* Process repeated at random intervals to prevent replay attacks

**MSCHAP (Microsoft CHAP) & PEAP (Protected Extensible Authentication Protocol)**

* MSCHAPv2 – Microsoft proprietary version

1. Uses new string each time for authentication
2. Client & server mutually authenticate & use 2 encryption keys

* Should not be used alone
* Use MS-CHAP with Protected Extensible Authentication Protocol (PEAP) or L2TP/IPSec
* PEAP

1. Provides TLS/SSL tunnel
2. Protects authentication traffic
3. Uses certificate on authentication server

**NTLM (NT LAN Manager)**

* Legacy authentication form Microsoft
* Replaced by Kerberos
* Similar to CHAP & MSCHAP
* All NTLM versions use relatively weak cryptographic scheme
* Lacks MFA (Multi-Factor Authentication) support

**Federated Services**

* Security Assertion Markup Language (SAML)
* OAuth
* Simple Web Tokens & JSON Web Tokens
* OpenID Connect

**Security Assertion Markup Language (SAML)**

* Extensible Markup Language (XML) framework for creating & exchanging security information between online systems
* Main purpose is SSO (Single Sign-On) for enterprise users over web
* 3 main functions

1. User seeking to verify identity is principal
2. Entity that can verify identity of end-user is Identity Provider
3. Entity that uses Identity Provider to verify identity of end-user is Service Provider

* Shibboleth system (Single sign-on log-in system for computer networks) uses SAML

**Open Authorisation (OAuth)**

* Framework used for internet token-based authorisation
* Purpose is API authorisation between apps
* Current version is 2.0
* Allows access tokens to be issued to 3rd-party clients (resource consumers) with approval of resource owner, such as social media site
* OAuth2.0 uses JSON & HTTP protocols
* Use SSL/TLS to prevent eavesdropping

**OpenID & OpenID Connect**

* Identity layer based on OAuth 2.0 specifications
* Used for consumer single sign-on
* OpenID Connect implements authentication as extension to OAuth 2.0 authorisation process
* Provides additional security – signing, encryption of identity data & session management
* Uses ID token structure including authentication of end-user via JSON Web Token (JWT)
* JWT used to prove that authentic source created originating data