Security +
Access Controls

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

General Concepts

Identification

- Users claim who they are
- Users may claim an identity with a username, or smart-card
- When using biometric identification systems the use a device such as fingerprint scanner or facial recognition

Authentication

- Users prove their identity (passwords, PIN number, OTP, biometric scan)

Authorization

- Access is granted to a specific resource based on the identity that has been authenticated

Accounting

- Access and usage is logged
- Accounting data can be used for controlling, monitoring, non-repudiation, statistics, and billing

AAA authentication, authorization, accounting (auditing)

- The elements of a comprehensive access management system
- Common AAA authentication protocols include:
  - RADIUS / DIAMETER
  - XTACACS / TACACS+
  - Kerberos
  - CHAP
  - PPP
  - LDAP

Authentication Factors

Multi-Factor

- Using more than one factor in the authentication process

Context Aware Authentication

- Incorporates extra information such as geolocation, time of day, device MAC address, etc, to improve security
- Factors include:

    - Something you know (password, PIN)
    - Something you have (smart-card, phone, USB token, 2nd factor)
    - Something you are (fingerprint, biometric, 3rd factor)
    - Somewhere you are (geolocation, MAC address of computer)
    - Something you do (touch gestures on a touch screen, keyboard dynamics, aka behaviour biometrics)

Password complexity

- Uppercase (26 A-Z)
- Lowercase (26 a-z)
- Numbers (10 0-9)
- Special characters (32 printable characters)

Password Policy

- A password policy may enforce min/max password age, min/max password length, complexity requirements, and whether to use reversible encryption, or not depending on whether the passwords needs to be determined from it's stored encrypted state
- **Key-space = C^N**
    - **C** is the number of **possible characters**, **N** is the **length of the password**
    - Key-space is the number of possible combinations of passwords/keys
- **Password expiry**
    - Changing the password prevents breached passwords from being used
- **Password recovery**
    - Changing the password to a temporary password which will then require being changed prevents the admin from knowing the password
- **Password history / reuse**
    - Because passwords should not be reused, a password history can **prevent password reuse** by a user
- **Account lockout threshold** and **account lockout duration** can prevent brute forcing passwords
- **Change default passwords**
    - All hardware appliance / software default passwords should be changed

Group Policy

- Allows creation of an access policy for a group and applying it to several users
- **Group Policy Object (GPO)**
    - Controls what users can and cannot do on a computer system
    - For example, to enforce a password complexity policy that prevents users from choosing an overly simple password, to allow or prevent unidentified users from remote computers to connect to a network share, to block access or restrict access to certain folders

Domain Controller

- A domain controller is a server that responds to authentication requests and verifies users on computer networks

- A domain is a concept introduced in **Windows NT** whereby a user may be granted access to a number of computer resources with the use of a single username and password combination
- In Windows NT 4, one DC serves as the primary domain controller (PDC)
- Others, if they exist, are usually a backup domain controller (BDC)

Active Directory Domain Services (AD DS)

- Is a **directory service** Microsoft has developed for **Windows networks**
- Included in **Windows Server OS**
- Windows 2000 and later versions introduced Active Directory
- Active Directory makes it easier for administrators to **manage and deploy network changes** and policies such as password changes, and group permissions
- Active Directory Server
- Active Directory Service
- Organizational Units (OU)
- Active Directory Users and Computers (ADUC)
- **Security principal** is used to authenticate an identity and is what handles what permissions an identity has

Access Security Hardware

- Smart-card (ISO/IEC 14443) - Use embedded certificates
- Proximity card (two types "A" and "B", with different communications protocols)
- CAC Common access card (Used by US Department of Defence ID cards)
- PIV Personal Identity Verification Card (Used by US federal agencies)
- Hardware token / Key FOB
- Fingerprint scanner
- Retina scanner
- Iris scanner - More common then a retina scanner
- Voice recognition - Does not provide good accuracy
- Facial recognition

Access Security Software Open Standards

- **HOTP HMAC based one time password**
    - Client token device or application and server both use a **secret key** and **incrementing counter** which are hashed together
    - The hashed result is then further reduced to a few characters and displayed to the user to be entered as authentication code
    - The counter values are incremented on the device / application when a hash is created, and on the server after a valid authentication has been submitted
    - The **validation window** is a range of counter values for which the server will accept a response from a client and consider it a valid authentication
- **TOTP time based one time password**
    - Uses **timestamp** as a factor to generate the **OTP**
    - **Google Authenticator** is an example of **TOTP**

    - The TOTP changes often and each one has a limited lifespan sometimes only a few seconds

False rejection rate (FRR or type I error) / False acceptance rate (FAR or type II error)

- Both are percentages of failure
- Devices can be adjusted for sensitivity / threshold of error
- **Cross-over Error Rate (CER)** is the point where FAR and FRR cross
- Lower CER means that a system is more accurate
- CER is often used to calibrate biometric systems to acceptable levels of error

Accounts

Credential Management

- All the processes and technologies involved in provisioning, maintaining, and managing user accounts and credentials

Types of Accounts

- **End-user accounts**
    - Regular user accounts
- **Administrator / Root**
    - Super privileged account
- **Privileged accounts**
    - Additional rights such as admin accounts
- **Guest accounts**
    - Limited temporary access accounts
- **Service accounts**
    - Accounts for application services such as Apache, MySQL, etc.

Common Account Policies

- **Standardized account names**
    - Use a common standard for account names such as for email addresses, workstation accounts, etc.
    - For example firstname.lastname@domain.com
- **Limit admin account usage**
    - Don’t use admin accounts for day-to-day business functions. Require admins to escalate their privileges when needed
- **Prohibit shared accounts / mingling accounts**
    - Sharing accounts should only be allowed if absolutely necessary such as when systems can never be logged off/on
- **Multiple accounts**
    - Administrators and privileged users may have more than one account to prevent using an account with high level privileges all the time
- **Disablement policies**
    - Have policies in place to disable and backup, archive, and delete accounts for employees ASAP (termination, vacation)
    - It’s a good idea to automate and schedule disablement policies

whenever possible to avoid account sprawl

- **Account recovery**
  - Maintain the ability to enable disabled accounts and recover deleted / archived accounts
- **Time of day restrictions**
  - Limit times when users can logon
- **Location based policies**
  - Limit the user logins by geolocation such as GPS / GeoIP
- **Account maintenance**
  - Manual or automated account maintenance can report user’s logins and automatically delete unused accounts
- **Credential management**
  - Browsers, operating systems, and password managers can store and automatically supply credentials for websites, services or resources
- **Least privilege**
  - Never give more permissions to a user account than is necessary for them to do their job
- **Time-of-day restrictions**
  - Make sure that access is only available during the time that users should be doing their job

Access Control Models

Confidentiality Model

- Emphasizes the need to protect against unauthorized access

Integrity Model

- Emphasizes the need to protect all data from unauthorized modification

RoleBAC Role-based Access Control

- Uses **employee roles** to manage authorization to resources such as by adding users to groups (group based access control)
- These can be assigned based on job function, department and hierarchy (executive, manager, team member, administrator, etc.)

RuleBAC Rule-based Access Control

- Most common example is for **routers and firewalls**
- Use ACL (access control list) to block traffic or route VLAN traffic based on the physical port on the router
- ruleBAC can be dynamic (Fail2ban)
- **Account lockout** can block users who **fail login attempts** too many times

DAC Discretionary Access Control

- Most common example is file permissions on Windows (NTFS) and Linux systems. File/folder *owners can set permissions for groups and general users*
- Microsoft systems use SID (security identifiers) to identify users and groups
- All files/folders have DACL (discretionary access control list) specifying who

can access it
- The DACL is a list of ACE (access control entities) that include permission levels such as read, modify, full-control, etc.

MAC Mandatory Access Control

- **Security labels / sensitivity labels** on both **subjects (users)** and **objects (files/folders)**
- When labels match, the system can grant a user access to an object
- Labels are in lattice and can be complex relationships
- Generally, these labels include **hierarchal levels** and **dataset classifications**
- Users can be granted access to resources based primarily on their security level, but must be granted access to each dataset individually
- Administrators assign **access levels** based on **security professionals** and **security auditing**
- **SELinux** uses MAC for access control

ABAC Attribute-based Access Control

- Uses **attributes included in policies** to grant access when the system detects match in policy
- Common in **SDN (software defined networks)**
- ABAC uses **policy statements** that include **subject**, **object**, **action**, and **environment**
- ABAC can enforce both **DAC** and **MAC** models simultaneously
- The environment is everything outside the context of subject, and object attributes
- See **NIST SP 800-162 Guide to Attribute Based Access Control**

Physical Access Control

Mantrap

- Prevent people from tailgating by forcing people to go one at a time
- These can be turnstiles, or other physical infrastructure
- Can also include cards/scanners or embedded services

Bollards

- Prevents attackers from driving a vehicle through a window or entry point in order to gain access

Security Guards

Locks / cages / safes

Account Policies

- **Provisioning and Deprovisioning**
  - Creating and assigning accounts, and then removing access, disabling, archiving and eventually deleting
- **Account Policies**
  - Credential management, group policy, password policies

- **Account Lockout**
    - Process to lock an account that is being compromised, attacked or violates policies
- **On-boarding / Off-boarding**
    - May include many accounts, certificates, and devices
- During **off-boarding** these things should be disabled, archived or deleted
- **User audits and reviews**
    - Periodically audit the access to systems and resources to avoid **permission** bloat / privilege creep, etc.
- **Recertification**
    - An audit of permissions to sensitive systems and data
- **Continuous monitoring**
    - A form of auditing that tracks **logs** and other **documentation** to ensure user actions are not in violation of access control policies
    - This ensure that systems and data are being accessed properly and by authorized personnel
    - The monitoring can be **automated** or **manual**

Information Classification

- **Public data**
    - Available to anyone, press release, web-sites, product information, brochures
- **Confidential data**
    - Is to be secret to a specific group of people. Salary data, contract data, etc.
- **Proprietary data**
    - Trade secrets, patents, trademarks, copyrights
- **Private data**
    - PII and PHI of employees or customers are both examples of private data

Network Authentication Services

Centralized authentication

- Uses a unified system for authentication between different networks, or applications

Decentralized authentication

- Do not trust each other’s credential database or authentication mechanisms

Kerberos

- Network authentication mechanism for **Windows Active Directory** and some Unix environments known as **realms**
- Developed at MIT, Kerberos provides mutual authentication to prevent MITM and uses **tickets** to **help prevent** replay attacks
- Kerberos uses a **Key Distribution Center (KDC)** to issue **Ticket Granting Tickets (TGT)** which are used **by clients** to generate **session tokens**

which are used to **access services** or resources
- Tickets are used for authentication when accessing system resources
- **Kerberos v5** requires all systems to be time synchronized within **5 minutes** of each other and timestamps tickets to ensure they expire at the correct time as specified
- Kerberos uses a database of users such as **Active Directory** in the authentication / authorization process
- Kerberos uses **symmetric key cryptography** to prevent unauthorized access and ensure confidentiality

NTLM New Technology LAN Manager

- A suite of protocols that provide **authentication, integrity, and confidentiality** within Windows
- NTLM uses message digest hashing to verify identity
- **NTLM v1** uses MD4 and is not recommended
- **NTLM v2** is a challenge response protocol
- Creates an HMAC-MD5 of username, logon hostname, the user’s password, current time, and more
- **NTLM2 Session** improves **NTLM v2** by adding mutual identification between the client and server
- Although **NTLM** does not send passwords in cleartext in transit, it is not considered very secure and **Kerberos** is more secure form of authentication

LDAP / LDAPS Lightweight Directory Access Protocol

- Is an extension of **X.500** standard used in Novell and MS Exchange Server
- **Active Directory** is based on and uses the LDAP format and **Unix realms** use LDAP
- **LDAPS** is **LDAP Secure** and uses SSL/TLS on **port 686** instead of **389**
- LDAP string: LDAP://CN=Name,CN=Users,DC=Domain,DC=com
  - CN=Name -> CN is short for common name
  - CN=Users -> CN is short for container
  - DC=Domain -> domain component
  - DC=com -> second domain component

SSO Single Sign On

- Allows logon to multiple systems / resources simultaneously
- Has the potential to increase security by giving the user only one password to remember instead of possibly hundreds
- Can reduce the burden of multiple account management systems
- Requires a **SSO policy server** to authenticate credentials
- Can be used with hardware token such as smart-card
- Can use 2FA or MFA to increase security
- Some SSO protocols include:
  - **OAuth** - Facebook login, Google Login, and other social network logins
  - **Kerberos -** Once authenticated can get tickets for network services
  - **SAML -** Protocol for web portal SSO
- Some SSO implementations include:

  - Accounts & SSO (Nokia, Intel, Canonical) since
  - Active Directory Federation Services (Microsoft) since 2003 in Windows Server 2003
  - Bitium (Google) since 2012

Transitive Trust / Circle of trust

- Creates an indirect trust relationship between systems
- If **A** trusts **B** and **B** trusts **C**, then **A** will also trust **C**
- Reduces the number of trusts that are needed for authentication interoperability between different domains
- **Non-transitive** trust is a trust that will not extend past the domains it was created with
- With LDAP domains use transitive trust for SSO

Federation / FIM Federated Identity Management

- Subscribers use the **same authentication credentials** between **multiple enterprises** to obtain access to network resources
- Prevents forcing users to create separate accounts for multiple domains
- Allows enterprises to share resources such as **community cloud**
- Is a **multi-environment** authentication system with a **centralized identity management database**
- Used for access to different network resources, operating systems on a network, or websites
- **Windows Active Directory** supports federated login system
- Common **FIM** protocols include **SAML**, **OpenID**, **OAuth**, and **Shibboleth**

Shibboleth

- Is an example of a **federated identity management system** with **SSO**
- Uses **SAML**
- Is an Open Source software project that began in 2000

SAML Security Assertion Markup Language

- Is an XML data format used for SSO on web-browsers
- If organizations have transitive trust, SAML can be used to enable federated identity management
- SAML has three roles (principal, identity provider, service provider)
- **Principal**
  - Typically a user who is either logging on or registering
- **Identity provider**
  - Maintains the central identity data
- **Service provider**
  - Provides the login / access services to principals
- SAML does not provide identical authorization across federations or systems

Oauth and OpenID Connect

- An open standard for authorization to provide secure access to protected resources
- Used for cross-site login of websites (Facebook login, etc.) and also for

payment systems such as between PayPal and vendor

- OpenID Connect works with Oauth 2.0 and provides 3rd party authentication services