CSF 434/534: Advanced Network and System Security

Week 09 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes

AAA and Authentication

AAA and Authentication

AAA framework

- Identification
  - This is who you claim to be
  - Usually your username
- Authentication
  - Prove you are who you say you are
  - Password and other authentication factors
- Authorization
  - Based on your identification and authentication, what access do you have?
- Accounting
  - Resources used: Login time, data sent and received, logout time

AAA and Authentication

Multi-factor authentication

- More than one factor
  - Something you are
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do
- Can be expensive - Separate hardware tokens
- Can be inexpensive - Free smartphone applications

AAA and Authentication

Something you are

- Biometric authentication
  - Fingerprint, iris, voiceprint
- Usually stores a mathematical representation of your biometric
  - Your actual fingerprint isn't usually saved
- Difficult to change
  - You can change your password
  - You can't change your fingerprint
- Used in very specific situations
  - Not foolproof

AAA and Authentication

Something you have

- Smart card
  - Integrates with devices
  - May require a PIN
- USB token - Certificate is on the USB device
- Hardware or software tokens
  - Generates pseudo-random authentication codes
- Your phone
  - SMS a code to your phone

AAA and Authentication

Something you know

- Password
  - Secret word/phrase, string of characters
  - Very common authentication factor
- PIN
  - Personal identification number
  - Not typically contained anywhere on a smart card or ATM card
- Pattern
  - Complete a series of patterns
  - Only you know the right format

AAA and Authentication

Somewhere you are

- Provide a factor based on your location
  - The transaction only completes if you are in a particular geography
- IP address
  - Not perfect, but can help provide more info
  - Works with IPv4, not so much with IPv6
- Mobile device location services
  - Geolocation to a very specific area
  - Must be in a location that can receive GPS information or near an identified mobile or 802.11 network
  - Still not a perfect identifier of location

AAA and Authentication

Something you do

- A personal way of doing things
  - You're special
- Handwriting analysis
  - Signature comparison
  - Writing technique
- Typing technique
  - Personal typing pattern
- Very similar to biometrics
  - Close to something you are

AAA and Authentication

Federation

- Provide network access to others
  - Not just employees
  - Partners, suppliers, customers, etc.
- Third-parties can establish a federated network
  - Authenticate and authorize between the two organizations
  - Login with your Facebook credentials
- The third-parties must establish a trust relationship
  - And the degree of the trust

AAA and Authentication

Single sign-on (SSO)

- Authenticate one time
  - Gain access to everything!
- Saves time
  - A seamless process
  - End-user doesn't see any of the complexities under the surface
- Many different methods
  - Kerberos authentication and authorization
  - 3rd-party options

AAA and Authentication

Transitive trust

- Trust relationships need to be established early
  - Difficult to change once in place
- One-way trust
  - Domain B trusts Domain A, Domain A doesn't trust Domain B
- Two-way trust
  - Both domains are peers, both trust each other equally
- Non-transitive trust
  - A trust is specifically created and applies only to that domain
- Transitive trust
  - Domain A trusts Domain B, Domain B trusts Domain C, therefore Domain A trusts Domain C
  - Think math! If a = b and b = c then a = c

Identity and Access Services

Identity and Access Services

TACACS

- Terminal Access Controller Access-Control System
  - Remote authentication protocol
  - Created to control access to dial-up lines to ARPANET
- XTACACS (Extended TACACS)
  - A Cisco-created (proprietary) version of TACACS
  - Additional support for accounting and auditing
- TACACS+
  - The latest version of TACACS, not backwards compatible
  - More authentication requests and response codes
  - Released as an open standard in 1993

Identity and Access Services

RADIUS (Remote Authentication Dial-in User Service)

- One of the more common AAA protocols
  - Supported on a wide variety of platforms and devices
  - Not just for dial-in
- Centralize authentication for users
  - Routers, switches, firewalls
  - Server authentication
  - Remote VPN access
  - 802.1X network access
- RADIUS services available on almost any server operating system

Identity and Access Services

LDAP (Lightweight Directory Access Protocol)

- Protocol for reading and writing directories
  - An organized set of records, like a phone directory
- X.500 specification was written by the International Telecommunications Union (ITU)
- DAP ran on the OSI protocol stack
  - LDAP is lightweight, and uses TCP/IP (tcp/389 and udp/389)
- LDAP is the protocol used to query and update an X.500 directory
  - Used in Windows Active Directory, Apple OpenDirectory, Novell eDirectory, etc.

Identity and Access Services

X.500 Distinguished Names

- attribute=value pairs
- Most specific attribute is listed first
  - This may be similar to the way you already think

X.500 Directory Informational Tree

- Hierarchical structure
  - Builds a tree
- Container objects
  - Country, organization, organizational units
- Leaf objects
  - Users, computers, printers, files

Attribute	Field	Usage
CN	Common Name	Identifies the person or object.
OU	Organizational Unit	A unit or department within the organization.
O	Organization	The name of the organization.
L	Locality	Usually a city or area.
ST	State	A state, province, or county within a country.
C	Country	The country's 2-character ISO code (such as c=US or c=GB).
DC	Domain Component	Components of the object's domain.

Identity and Access Services

Microsoft NTLM

- Windows challenge/response
  - Domain name, username, password hash
- LAN Manager (LANMAN)
  - Microsoft and 3Com network operating system
- NT LAN Manager v2 (NTLM) challenge/response
  - Hash challenge, similar to CHAP
  - Somewhat insecure
    - MD4 password hash (same as NTLMv1)
    - HMAC-MD5 hash of username and server name
    - Variable-length challenge of timestamp, random data, domain name

Identity and Access Services

Microsoft NTLM vulnerabilities

- Some Windows password databases contain LM hash versions of the passwords
  - Compatibility with older systems
- NTLM vulnerable to a credentials forwarding attack
  - Use credentials of one computer to gain access to another
- Migrate to Kerberos
  - If you haven't already

Identity and Access Services

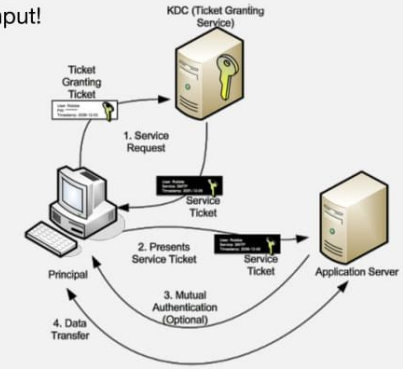
Kerberos

- Network authentication protocol
  - Authenticate once, trusted by the system
  - No need to re-authenticate to everything
  - Mutual authentication - the client and the server
    - Protect against man-in-the-middle or replay attacks
- Standard since the 1980s
  - Developed by the Massachusetts Institute of Technology (MIT)
  - RFC 4120
- Microsoft starting using Kerberos in Windows 2000
  - Based on Kerberos 5.0 open standard
  - Compatible with other operating systems and devices

Identity and Access Services

SSO with Kerberos

- Authenticate one time
  - Lots of backend ticketing
- No constant username and password input!
  - Save time
- Only works with Kerberos
  - Not everything is Kerberos-friendly



PAP, CHAP, and MS-CHAP

PAP, CHAP, and MS-CHAP

PPP authentication

- Point-to-Point Protocol
  - Analog dialup, ISDN
- And derivatives
  - PPTP (Point-to-Point Tunneling Protocol)
  - PPPoE (Point-to-Point Protocol over Ethernet)
- Need to authenticate through these non-Ethernet networks
  - PAP, CHAP, and MS-CHAP

PAP, CHAP, and MS-CHAP

PAP (Password Authentication Protocol)

- A basic authentication method
  - Used in legacy operating systems
  - Rare to see singularly used
- PAP is in the clear
  - Weak authentication scheme
  - Non-encrypted password exchange
  - We didn't require encryption on analog dialup lines

PAP, CHAP, and MS-CHAP

CHAP

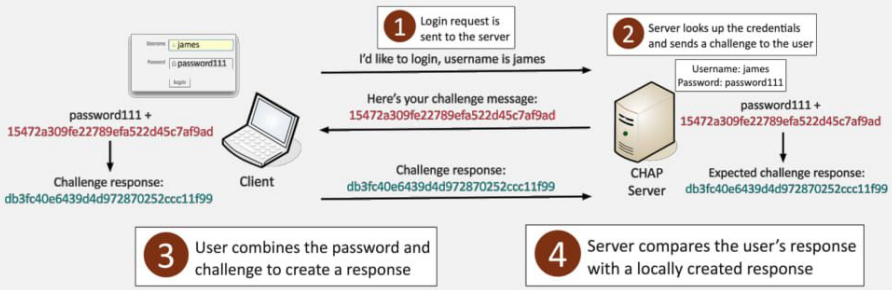
- Challenge-Handshake Authentication Protocol
  - Encrypted challenge sent over the network
- Three-way handshake
  - After link is established, server sends a challenge message
  - Client responds with a password hash calculated from the challenge and the password
  - Server compares received hash with stored hash
- Challenge-Response continues
  - Occurs periodically during the connection
  - User never knows it happens

PAP, CHAP, and MS-CHAP

MS-CHAP

- Microsoft's implementation of CHAP
  - Used commonly on Microsoft's Point-to-Point Tunneling Protocol (PPTP)
  - MS-CHAP v2 is the more recent version
- Security issues related to the use of DES
  - Relatively easy to brute force the 256 possible keys to decrypt the NTLM hash
  - Don't use MS-CHAP!
  - Consider L2TP, IPsec, or some other secure VPN technology

PAP, CHAP, and MS-CHAP



Federated Identities

Federated Identities

Server-based authentication

- HTTP/web browser communication is stateless
  - Each request is unique and has no relationship to the previous request
- Traditionally, the server has kept track of logins
  - You are assigned a session ID when you login
  - The server checks each time you send a request
- Adds overhead to the server
  - Difficult to scale
  - Adds challenges with redundancy and cloud services
  - Difficult to manage across multiple devices

Federated Identities

Token-based authentication

- No session information is stored on the server
  - Stateless, just like HTTP
- After user authenticates, the application sends a token to the client
  - The client stores the token locally
- The token is provided with each request to the server
  - The server validates the token and the application continues to work normally

Federated Identities

Security Assertion Markup Language (SAML)

- Open standard for authentication and authorization
  - You can authenticate through a third-party
  - One standard does it all, sort of
- Shibboleth is open-source software that implements SAML to provide federated SSO
  - SAML defines the standard that Shibboleth uses
- Not originally designed for mobile apps
  - This has been SAML's largest roadblock

Federated Identities

OAuth

- Authorization framework
  - Determines what resources a user will be able to access
- Created by Twitter, Google, and many others
  - Significant industry support
- Not an authentication protocol
  - OpenID Connect handles the single sign-on authentication
  - OAuth provides authorization between applications
- Relatively popular
  - Used by Twitter, Google, Facebook, LinkedIn, etc.

Access Control Models

Access Control Models

Access control

- Authorization
  - The process of ensuring only authorized rights are exercised
    - Policy enforcement
- The process of determining rights
  - Policy definition
- Users receive rights based on Access Control models
  - Different business needs or mission requirements

Access Control Models

Mandatory Access Control (MAC)

- The operating system limits the operation on an object
  - Based on security clearance levels
- Every object gets a label
  - Confidential, secret, top secret, etc.
- Labeling of objects uses predefined rules
  - The administrator decides who gets access to what security level
- Users cannot change these settings

Access Control Models

Discretionary Access Control (DAC)

- Used in most operating systems
  - A familiar access control model
- You create a spreadsheet
  - As the owner, you control who has access
  - You can modify access at any time
- Very flexible access control
  - And very weak security

Access Control Models

Role based access control (RBAC)

- You have a role in your organization
  - Manager, director, team lead, project manager
- Administrators provide access based on the role of the user
  - Rights are gained implicitly instead of explicitly
- In Windows, use Groups to provide role-based access control
  - You are in shipping and receiving, so you can use the shipping software
  - You are the manager, so you can review shipping logs

Access Control Models

Attribute-based access control (ABAC)

- Users can have complex relationships to applications and data
  - Access may be based on many different criteria
- ABAC can consider many parameters
  - A “next generation” authorization model
  - Aware of context
- Combine and evaluate multiple parameters
  - Resource information, IP address, time of day, desired action, relationship to the data, etc.

Access Control Models

Rule-based access control

- Generic term for following rules
  - Conditions other than who you are
- Access is determined through system-enforced rules
  - System administrators, not users
- The rule is associated with the object
  - System checks the ACLs for that object
- Rule examples
  - Lab network access is only available between 9-5
  - Only Chrome browsers may complete this web form

Access Control Models

File system security

- Store files and access them
  - Hard drive, SSDs, flash drives, DVDs
  - Part of most operating systems
- Accessing information
  - Access control list
  - Group/user rights and permissions
  - Can be centrally administered and/or users can manage files they own
- Encryption can be built-in
  - The file system handles encryption and decryption

Access Control Models

Database security

- Databases have their own access control
  - Username, password, permissions
- Encryption may be an option
  - Most databases support data encryption
- Data integrity is usually an option
  - No data is lost because of a fault
  - Part of the database server operation
- Applications can provide a secure front-end
  - Prevent SQL injections and inappropriate access to data

Access Control Technologies

Access Control Technologies

Proximity cards

- Close range card - Contactless smart card
- Passive device - No power in the card
  - Powered from the reader
- Not a large data storage device
  - Often used as an identifier
  - Keycard door access, library cards, payment systems
  - The identifier is linked to data stored elsewhere

Access Control Technologies

Smart cards

- Integrated circuit card
  - Contact or contactless
- Common on credit cards
  - Also used for access control
- Must have physical card to provide digital access
  - A digital certificate
- Multiple factors
  - Card with PIN or fingerprint

Access Control Technologies

Biometric factors

- Fingerprint scanner
  - Phones, laptops, door access
- Retinal scanner
  - Unique capillary structure in the back of the eye
- Iris scanner
  - Texture, color
- Voice recognition
  - Talk for access
- Facial recognition
  - Shape of the face and features

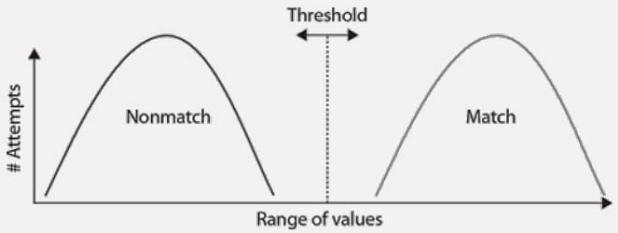
Access Control Technologies

Biometric acceptance rates

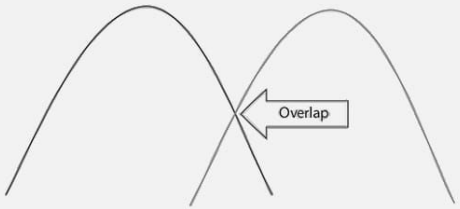
- False acceptance rate (FAR)
  - Likelihood that an unauthorized user will be accepted
  - This would be bad
- False rejection rate (FRR)
  - Likelihood that an authorized user will be rejected
  - No, it's really me
  - Let's try again
- Crossover error rate (CER)
  - The rate at which FAR and FRR are equal
  - Adjust sensitivity to equalize both values
  - Used to quantitatively compare biometric systems

Access Control Technologies

Ideal probabilities



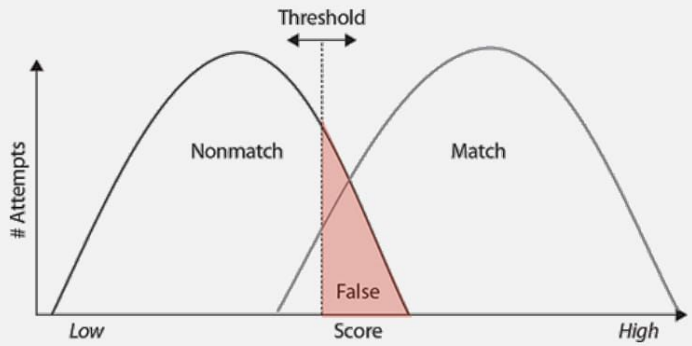
Realistic probabilities



Access Control Technologies

False Acceptance Rate (FaR)

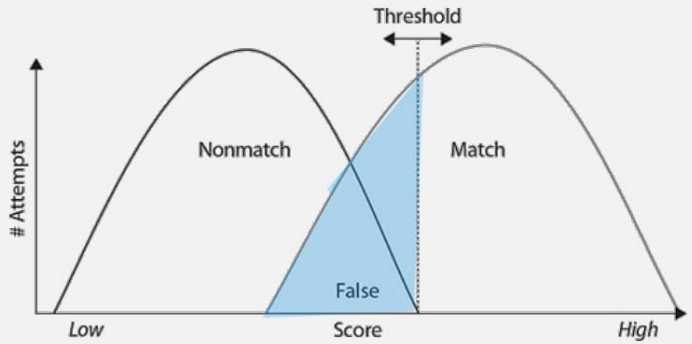
- Level of false positives that are allowed in the system



Access Control Technologies

False Rejection Rate (FrR)

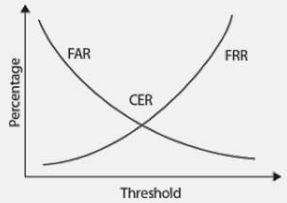
- Level of false negatives, or rejections, are going to be allowed in the system



Access Control Technologies

Crossover Error Rate (CeR)

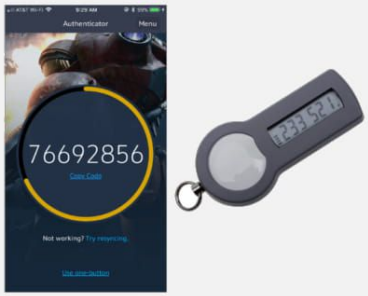
- Both the FaR and the FrR are set by choosing a threshold value
- Decrease chance of false positive? Cause failed authorizations of legitimate users
- Decrease chance of false negative? Some unauthorized users will get accepted
- The crossover error rate (CeR) is the rate where both accept and reject error rates are equal



Access Control Technologies

Token generators

- Pseudo-random token generators
  - A useful authentication factor
- Carry around a physical hardware token generator
  - Where are my keys again?



- Use software-based token generator on your phone
  - Powerful and convenient

Access Control Technologies

HOTP

- One-time passwords
  - Use them once, and never again
  - Once a session, once each authentication attempt
- HMAC-based One-Time Password algorithm
  - Keyed-hash message authentication code (HMAC)
  - The keys are based on a secret key and a counter
- Token-based authentication
  - The hash is different every time
- Hardware and software tokens available
  - You'll need additional technology to make this work

Access Control Technologies

TOTP

- Time-based One-Time Password algorithm
  - Use a secret key and the time of day
  - No incremental counter
- Secret key is configured ahead of time
  - Timestamps are synchronized via NTP
- Timestamp usually increments every 30 seconds
  - Put in your username, password, and TOTP code
- One of the more common OTP methods
  - Used by Google, Facebook, Microsoft, etc.

Access Control Technologies

Certificate-based authentication

- Smart card
  - Private key is on the card
- PIV (Personal Identity Verification) card
  - US Federal Government smart card
  - Picture and identification information
- CAC (Common Access Card)
  - US Department of Defense smart card
  - Picture and identification
- IEEE 802.1X
  - Gain access to the network using a certificate
  - On device storage or separate physical device

Access Control Technologies

TOTP - Time-based One-time Password Algorithm

- Hardware and software token generator

Google Authenticator

Account Types

Account Types

User accounts

- An account on a computer associated with a specific person
  - The computer associates the user with a specific identification number
- Storage and files can be private to that user
  - Even if another person is using the same computer
- No privileged access to the operating system
  - Specifically not allowed on a user account
- This is the account type most people will use
  - Your user community

Account Types

Shared and generic accounts

- Shared account
  - Used by more than one person
  - Guest login, anonymous login
- Very difficult to create an audit trail
  - No way to know exactly who was working
  - Difficult to determine the proper privileges
- Password management becomes difficult
  - Password changes require notifying everyone
  - Difficult to remember so many password changes
  - Just write it down on this yellow sticky paper
- Best practice: Don't use these accounts

Account Types

Service accounts

- Used exclusively by services running on a computer
  - No interactive/user access (ideally)
  - Web server, database server, etc.
- Access can be defined for a specific service
  - Web server rights and permissions will be different than a database server
- Commonly use usernames and passwords
  - You'll need to determine the best policy for password updates

Account Types

Privileged accounts

- Elevated access to one or more systems
  - Administrator, Root
- Complete access to the system
  - Often used to manage hardware, drivers, and software installation
- This account should not be used for normal administration
  - User accounts should be used
- Needs to be highly secured
  - Strong passwords, 2FA
  - Scheduled password changes

Account Management

Account Management

Least privilege

- Rights and permissions should be set to the bare minimum
  - You only get exactly what's needed to complete your objective
- All user accounts must be limited
  - Applications should run with minimal privileges
- Don't allow users to run with administrative privileges
  - Limits the scope of malicious behavior

Account Management

On-boarding

- Bring a new person into the organization
  - New hires or transfers
- Technical agreements need to be signed
  - May be part of the employee handbook or a separate AUP
- Create accounts
  - Associate the user with the proper groups and departments
- Provide required IT hardware
  - Laptops, tablets, etc.
  - Preconfigured and ready to go

Account Management

Off-boarding

- All good things...
  - But you knew this day would come
- This process should be pre-planned
  - You don't want to decide how to do things at this point
- What happens to the hardware and the data?
- Account information is usually deactivated
  - But not always deleted

Account Management

Perform routine audits

- Is everything running to policy?
  - You have to police yourself
- It's amazing how things change
  - Make sure the routine is scheduled
- Certain actions can be automatically identified
  - Consider a tool for log analysis

Account Management

Auditing

- Permission auditing
  - Does everyone have the correct permissions?
  - Some Administrators don't need to be there
  - Scheduled recertification
- Usage auditing
  - How are your resources used?
  - Are your systems and applications secure?
- Time-of-day restrictions
  - Nobody needs to access the lab at 3 AM

Account Management

Standard naming convention

- Unique
  - The username shouldn't conflict with another user
  - Use the same username across multiple systems
- Consistent
  - Usernames shouldn't describe a role or status
- Persistent
  - Use the same username for the duration of employment
- Memorable
  - This shouldn't be difficult. Make it easy to remember

Account Management

Account maintenance

- Account creation
  - Initial provisioning
  - Password management
  - Group and permission assignments
- Periodic updates
  - Password resets / forced updates
  - Permission audits
- Deprovisioning
  - Disable account
  - Archive user documents and encryption keys

Account Management

Group-based access control

- Set privileges based on what you do
  - Put many users into a single group
  - Set privileges on the group
  - Add/remove users from the group to assign privileges
- Users can be members of multiple groups
  - Group permissions can overlap
  - How do you determine the effective permissions?
    - Not as straightforward as you might think

Account Management

Location-based policies

- User access is based on location
  - GPS - mobile devices, very accurate
  - 802.11 wireless, less accurate
  - IP address, not very accurate
- Restrict application use
  - Don't allow this app to run unless you're near the office
- Apply security rules
  - Your IP address is associated with an IP block in China
  - We don't have an office in China
  - Permission not granted

Account Policy Enforcement

Account Policy Enforcement

Credential management

- All that stands between the outside world and all of the data
  - The data is everything
- Passwords must not be embedded in the application
  - Everything needs to reside on the server, not the client
- Communication across the network should be encrypted
  - Authentication traffic should be impossible to see

Account Policy Enforcement

Configuring settings

- Windows Group Policy Management
  - Apply security and admin settings across many computers
  - Thousands of settings
- Different than NTFS or Share permissions
  - Control the use of the operating system
- Linked to Active Directory administrative boundaries
  - Sites, domains, organization units (OUs)
  - Define by groups, locations, etc.

Account Policy Enforcement

Group Policy control

- Administrative policies
  - Remove Add or Remove Programs
  - Prohibit changing sounds
  - Allow font downloads
  - Only allow approved domains to use
  - ActiveX controls without prompt
- Security policies
  - Specify minimum password length
  - Maximum security log size
  - Enforce user login restrictions

Account Policy Enforcement

Password complexity and length

- Make your password strong
  - No single words
  - No obvious passwords
    - What's the name of your dog?
  - Mix upper and lower case
  - Use special characters
    - Don't replace a o with a 0, t with a 7
  - A strong password is at least 8 characters
    - Consider a phrase or set of words
  - Prevent password reuse
    - System remembers password history, requires unique passwords

Account Policy Enforcement

Password expiration and recovery

- All passwords should expire
  - Change every 30 days, 60 days, 90 days
- Critical systems might change more frequently
  - Every 15 days or every week
- The recovery process should not be trivial!
  - Some organizations have a very formal process

Account Policy Enforcement

Account lockout and disablement

- Too many bad passwords will cause a lockout
  - This should be normal for most users
  - This can cause big issues for service accounts
    - You might want this
- Disable accounts
  - Part of the normal change process
  - You don't want to delete accounts
    - At least not initially

CSF 434/534: Advanced Network and System Security

Week 09 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes