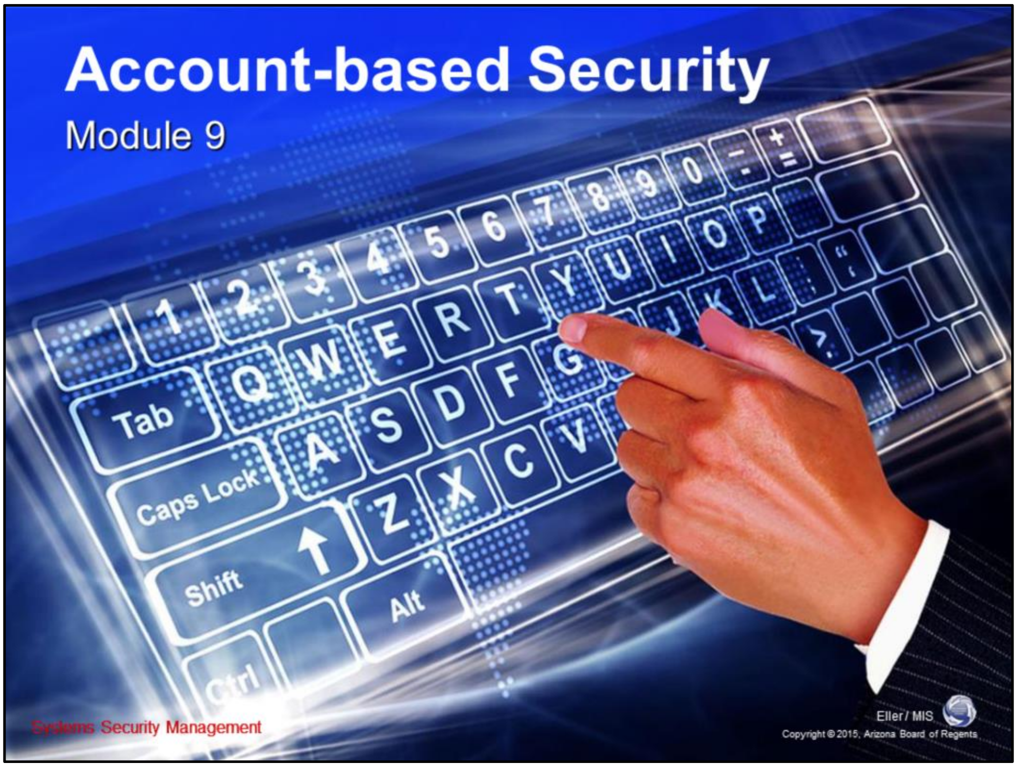
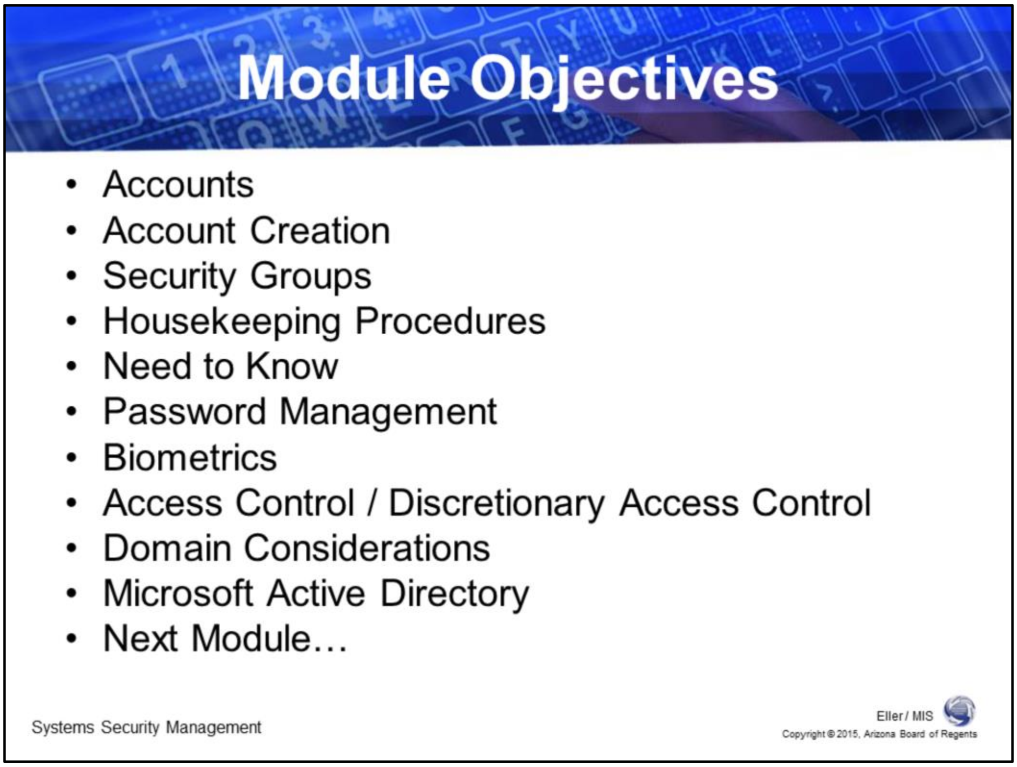


Account-based Security

Module 9

Systems Security Management

Eller / MIS



Module Objectives

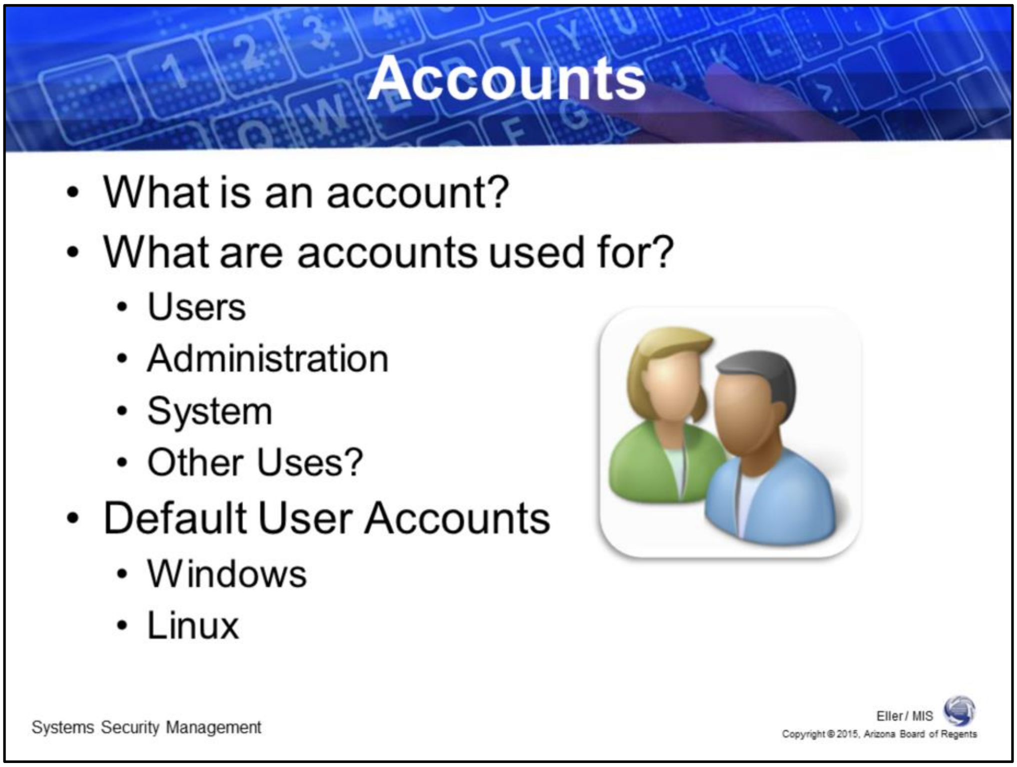
- Accounts
- Account Creation
- Security Groups
- Housekeeping Procedures
- Need to Know
- Password Management
- Biometrics
- Access Control / Discretionary Access Control
- Domain Considerations
- Microsoft Active Directory
- Next Module…

Systems Security Management

Eller / MIS

By the end of this module, you should have a clear understanding of:

•What accounts are and what they are used for.
•Naming conventions and policy creation.
•Security groups and the benefits of their use.
•The need for housekeeping procedures with user accounts.
•The creation of password management policies and their benefits.
•How biometrics can be used to increase account security.
•The difference between access control lists and discretionary access control lists.
•How the use of domains changes how security is handled.



Accounts

- What is an account?
- What are accounts used for?
  - Users
  - Administration
  - System
  - Other Uses?
- Default User Accounts
  - Windows
  - Linux

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

What is an account?

Simply put, an account is a method for authenticating and authorizing a user, computer, or service to allow for access to client computers and network resources.

What are accounts used for?

User Accounts are created to allow a particular user to use a client computer system and to provide access to shared network resources.

Administrator Accounts are created to allow systems administrators to manage servers and client computers connected to the network.

System Accounts are created to provide automated services on the network to operate and perform various tasks automatically. For example, for running system services or backup operations.

Are there other uses for accounts?

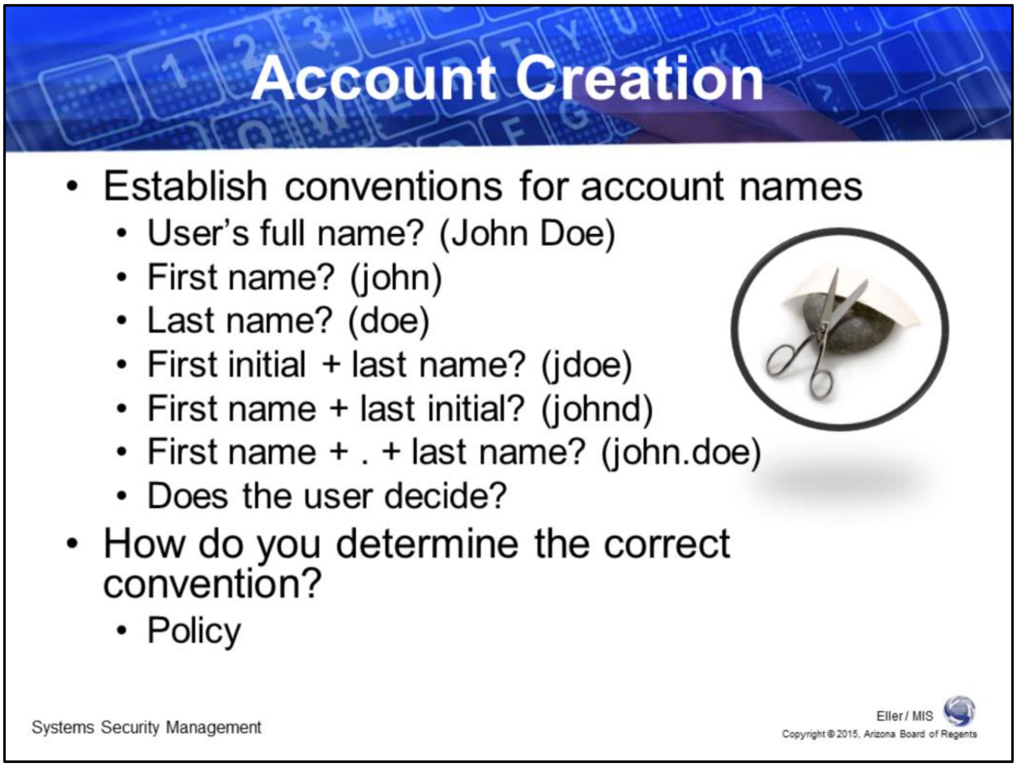
Windows Active Directory Services uses computer accounts to authorize specific network client computers access to systems resources.

Default User Accounts for Windows

Administrator
Guest
IUSR_SERVERNAME - For systems running Microsoft Internet Information Services (IIS).

Default User Accounts for Linux

Root



Account Creation

- Establish conventions for account names
  - User's full name? (John Doe)
  - First name? (john)
  - Last name? (doe)
  - First initial + last name? (jdoe)
  - First name + last initial? (johnd)
  - First name + . + last name? (john.doe)
  - Does the user decide?
- How do you determine the correct convention?
  - Policy

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

Prior to the creation of user accounts, it is important to establish an account naming convention. This should become the standard method for how user accounts are created on the network. There are a great many options available for creating a naming convention. Some of the typical conventions include:

User's full name
First name
Last name
First initial + last name
First name + last initial
First name + . + last name

An organization can also choose to allow the users to decide what their individual user account will be.

How do you determine the correct naming convention for user accounts?

There is no such thing as a "correct naming convention." Despite this, each organization should develop its own standard for naming conventions that takes into account the following four items:

Usability
Security
Administration
Audit

It is up to the organization to determine the priority of these four items.

Usability: Usability is concerned about the end user. An organization most concerned with keeping their customers happy will set usability as the top priority. The typical account naming convention in this scenario is your name-based convention such as "jdoe" or "doej".

Security: Security is concerned about unauthorized access. This concerns the ability of users to guess login names and therefore they have half of the authentication credential. The typical account naming convention in this scenario is a system generated account name that is not directly linked to identity data in any way.

Administration: Administration is concerned about ease of administration. The concern is the ability for "Help Desk" users to quickly and easily find user accounts. The typical account naming convention in this scenario is one based on full name such as "Doe, John" or "John Doe".

Audit: Audit is concerned about auditing and reporting system and application access. The concern is the ability to run reports to show the history of access for specific users. This requires a naming convention that doesn't change (such as a primary key in a database) since access logs normally only store user account names and not a globally unique identifier (GUID). The typical account naming convention in this scenario would be using a unique identifier from an authoritative data source such as employee ID for staff or student ID for students.

Depending on the structure of the organization, a policy for user account naming conventions can be created by the IT department, corporate leadership, or even the legal department. Regardless, a policy should be setup to guide systems administrators, and provide a logical expectation for users. The actual naming convention does not matter, but consistency is vital.

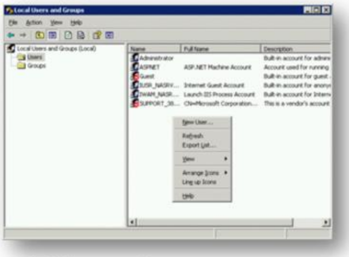
So what happens when a user account is already in use?

It is definitely conceivable that a user account could already exist within a company. For example, say James Jones was just hired to work for the company; however, the company already has an employee by the name of Jennifer Jones. If the naming convention policy was created so Jennifer was assigned the user id "jjones," how would the systems administrator create an account for James that adheres to the naming policy? Well, the answer here is the policy needs to be designed to account for these particular instances. So, for example, James could be assigned the user id "jonesj," or some other variation.

The bottom line is someone within the company should create a user account naming convention policy and the systems administrator should adhere to the policy.

Account Creation

- Windows Workstation or Server
  - Under Administrative Tools
    - Computer Management
    - Local Users & Groups
      - Users Folder
      - Click Action -> New User

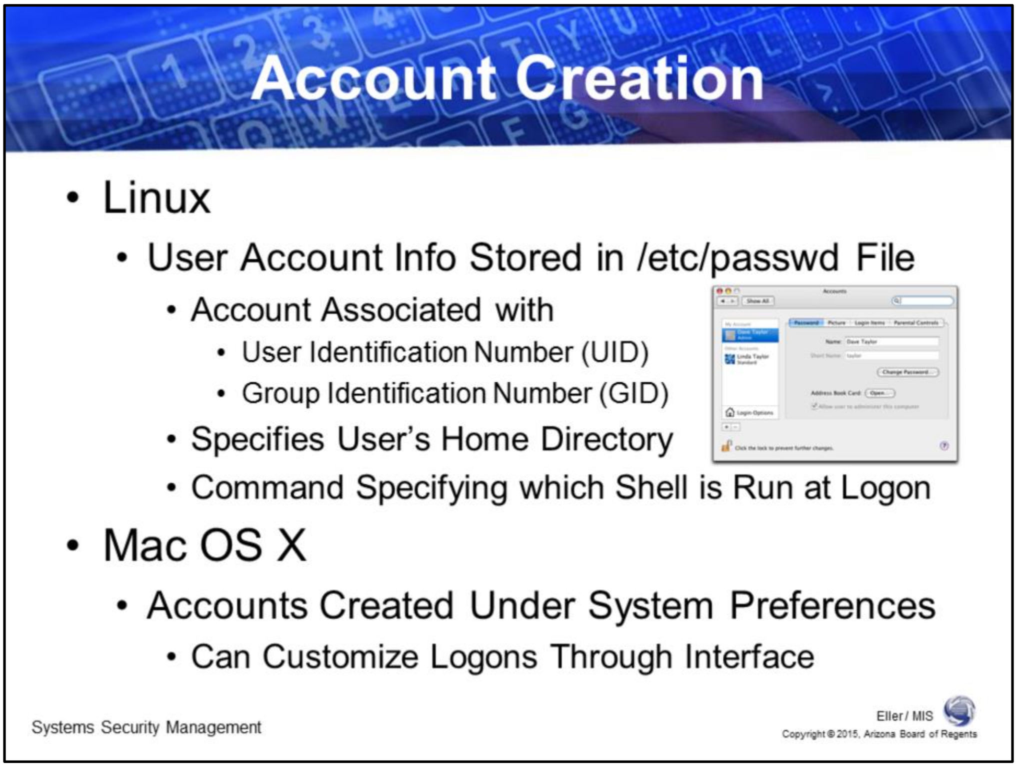


Name	Full Name	Description
Administrator		Built-in account for admin
ASPNET	ASP.NET Machine Account	Account used for running
Guest		Built-in account for guest
IUSR_NASRV...	Internet Guest Account	Built-in account for anony
IWAM_NASR...	Launch IIS Process Account	Built-in account for Intern
SUPPORT_38...	CN=Microsoft Corporation...	This is a vendor's account

- Windows Server with Active Directory
  - Under Administrative Tools
    - Active Directory Users & Computers
      - Create Accounts Under Users or an Organizational Unit

Accounts can be created rather easily in most operating systems. On a Windows-based workstation or server, user accounts can be created from the Administrative Tools folder found in the Control Panel. Run the Computer Management tool and open Local Users and Groups. Inside the Users Folder you can click on the Action Menu and select New User.

On a server running Microsoft's Windows Active Directory Services you will find the Active Directory Users and Computers tool inside the Administrative Tools folder. Within this tool you can create accounts under the Users folder or a custom Organizational Unit.



Account Creation

- Linux
  - User Account Info Stored in /etc/passwd File
    - Account Associated with
      - User Identification Number (UID)
      - Group Identification Number (GID)
    - Specifies User's Home Directory
    - Command Specifying which Shell is Run at Logon
- Mac OS X
  - Accounts Created Under System Preferences
    - Can Customize Logons Through Interface

Accounts

My Account: Dave Taylor, Admin

Other Accounts: Linda Taylor, Standard

Name: Dave Taylor

Short Name: taylor

Address Book Card:

☑ Allow user to administer this computer

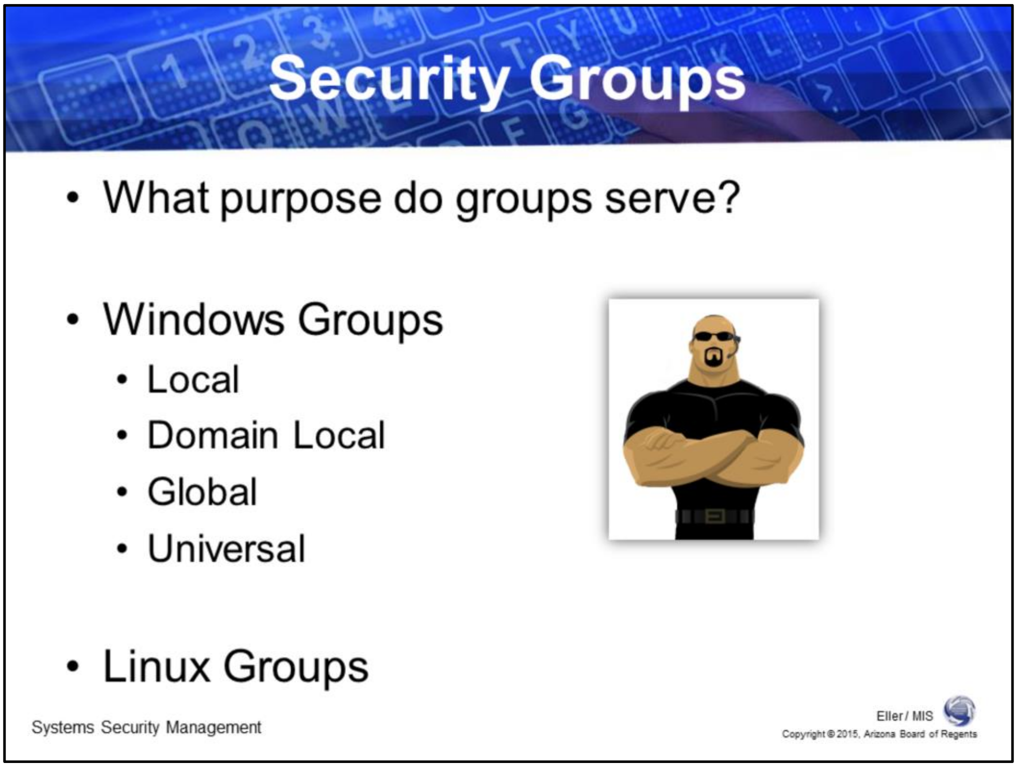
Click the lock to prevent further changes.

Systems Security Management

Eller / MIS

In Linux, user account information is stored in the /etc/passwd file. User accounts are associated with both a User Identification Number (UID) and a Group Identification Number (GID). In addition, the user account specifies the user's home directory, where that user's files are stored by default. Finally, the user account will specify which Linux shell is run at user logon.

In Apple's Mac OS X, accounts are created under system preferences. Through this interface, the system administrator can customize logons.



Security Groups

- What purpose do groups serve?
- Windows Groups
  - Local
  - Domain Local
  - Global
  - Universal
- Linux Groups

Systems Security Management

Eller / MIS

What are groups and what purpose do they serve?

Groups are objects which combine a collection of user or other accounts together in order to ultimately provide access to shared resources.

What types of groups are available in Microsoft Windows?

Local Groups: Local groups are security groups that exist only on the Windows client system (e.g. Windows 2000/XP/Vista/7). User accounts on the local computer and those from the network the computer is a member of can be added to these local groups. By default a Windows client system has the following groups: Administrators, Guests, Users, Power Users, and Backup Operators. Other groups may be created automatically when software is installed, or the system administrator can create custom groups as desired.

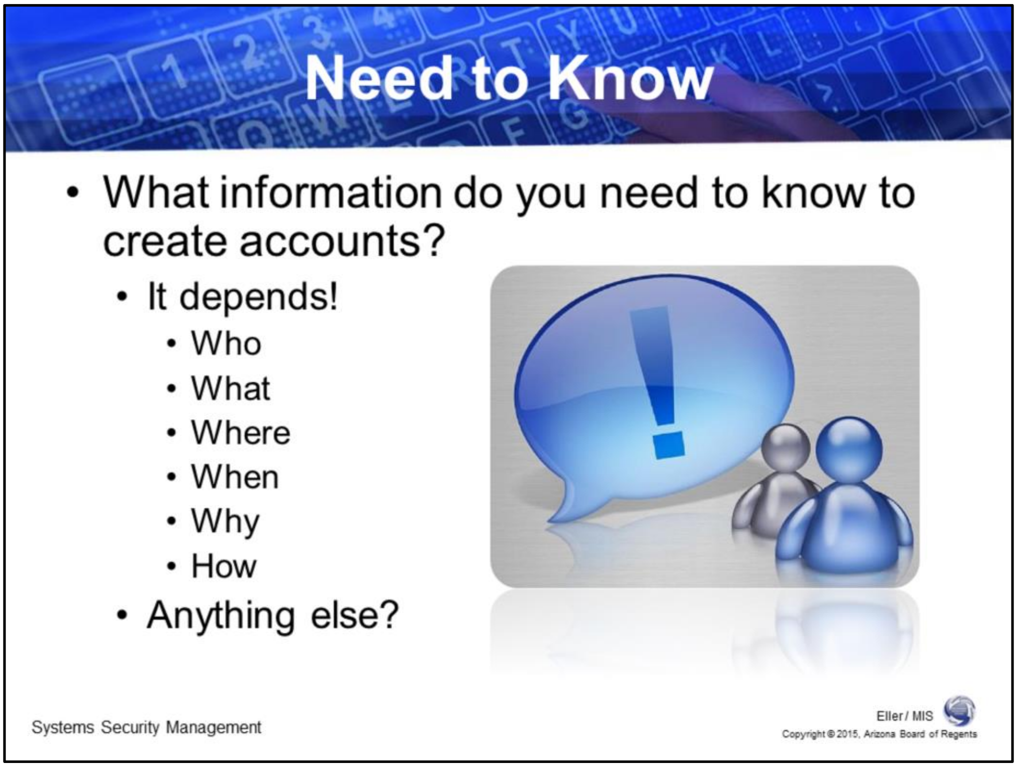
Domain Local Groups: Domain local groups are security groups that exist on a Windows Active Directory domain. These groups are used only within the domain environment and can only contain users or other domain local groups within the same domain. This means child domains or other domains within the same forest or within a trust relationship will not be able to be placed in these groups.

Global Groups: Global groups are security groups that exist on a Windows Active Directory domain. These groups are used only within the domain environment; however, they can contain users and global/domain local groups from the same domain and/or child domains. Users from other non-child domains in the same forest, or those formed from a manual trust relationship cannot be added to these groups.

Universal Groups: Universal groups are security groups that exist on a Windows Active Directory domain. These groups are used within the domain and forest environments, allowing users and groups from any domain within the same forest or from a trust relationship to be granted access to resources.

What types of groups are available in Linux?

Linux systems also use groups as a means of assigning security permissions to the system. The groupadd command allows Linux admins to create custom groups and assign users to the groups. Linux typically manages its own default groups.



Need to Know

- What information do you need to know to create accounts?
  - It depends!
    - Who
    - What
    - Where
    - When
    - Why
    - How
  - Anything else?

Systems Security Management

Eller / MIS

When creating user accounts there should be a definitive list of information that the systems administrator needs to know in order to create the account. The level of information necessary for the account creation process is something that should be defined in the user account policy, so specifically what information is required to create the account depends on the adopted policy. This information can include:

Who: Who is the user account for? The systems administrator should be provided with full contact information for the person who needs the user account. This should include full name, email address (unless the account being created is for that purpose), office location, office phone number, and office address (assuming the company has multiple locations).

What: What does the new user account need access to? Creating a user account is fine; however, the systems administrator needs to know what resources the user will need access to. In some cases, just granting access to the user's specific department resources will be enough; however, this is not true in all cases, and this information needs to be provided so the user will have access to everything they need for their position within the company.

Where: What department does the user work for? Should a user in the Accounting department be given access to the Human Resources servers and printers? Knowing this information will guide the systems administrator so the account is created with the appropriate access rights.

When: Does the user's position require they have access only during certain times of the day or week? This is something that is typically reserved for those companies who have a higher interest in security and want to monitor the time their employees are actively logged into the system.

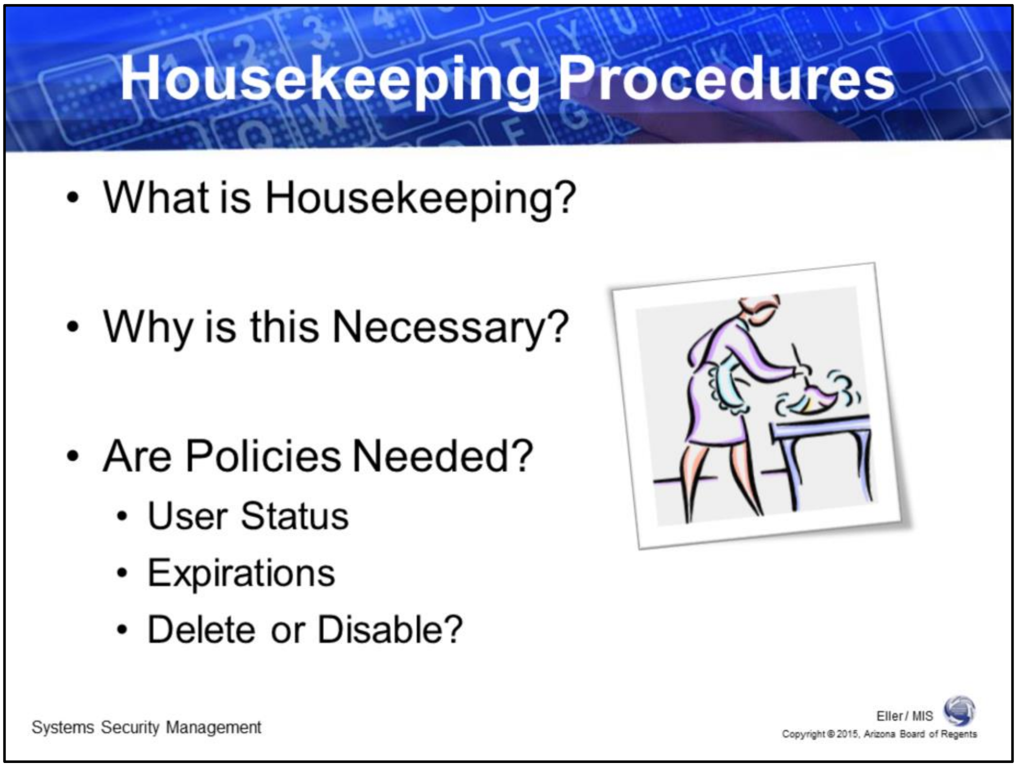
Why: Why does the user need an account? This is typically not the concern of the systems administrator. Leave the question of why to those who ask for the account to be created.

How: How will the user access the network? Will this be through a wired or wireless connection? Depending on how your network is configured, this may be a valid concern for securing resources.

Can you think of any other questions the systems administrator might need to know when creating user accounts?

What about system accounts?

With system accounts, the systems administrator needs to know specifically what purpose the system account will serve and should take steps to secure the account as much as possible to prevent its use by anyone other than the server or service which needs it.



Housekeeping Procedures

- What is Housekeeping?
- Why is this Necessary?
- Are Policies Needed?
  - User Status
  - Expirations
  - Delete or Disable?

Systems Security Management

Eller / MIS

What is housekeeping?

Occasionally it is important for you to perform some kind of maintenance on your own computer system. This maintenance can include removing programs you no longer need, defragmenting your computer, or just reorganizing your personal files. This is generally referred to as housekeeping, and the term is also applied to other areas of systems administration, including user account security.

Why is housekeeping necessary?

Housekeeping is a very important component of account security. If user accounts are kept active when an employee is no longer with the company, this provides a potential avenue for a breach of security. Keeping a user account active after an employee (temporary, contract, or otherwise) is no longer employed by the company is a major security risk. This is true regardless of the level of access the user had within the company (from basic employee to corporate executive). Continued access after termination can lead to basic security compromises, such as access to online file storage, to more serious compromises, such as corporate espionage. Keeping user status information current will prevent these types of security breaches.

Are policies needed?

Absolutely. As a systems administrator, how do you know when an account is no longer used or necessary? Creating and adopting a user account policy that specifically defines housekeeping procedures is incredibly important. The policy should cover what departments should do when an employee is hired and what to do when an employee is terminated. All companies have (or should have) a defined HR policy handling the hiring and termination of employees, and systems administrator notification should be included as part of these policies.

Some housekeeping options include:

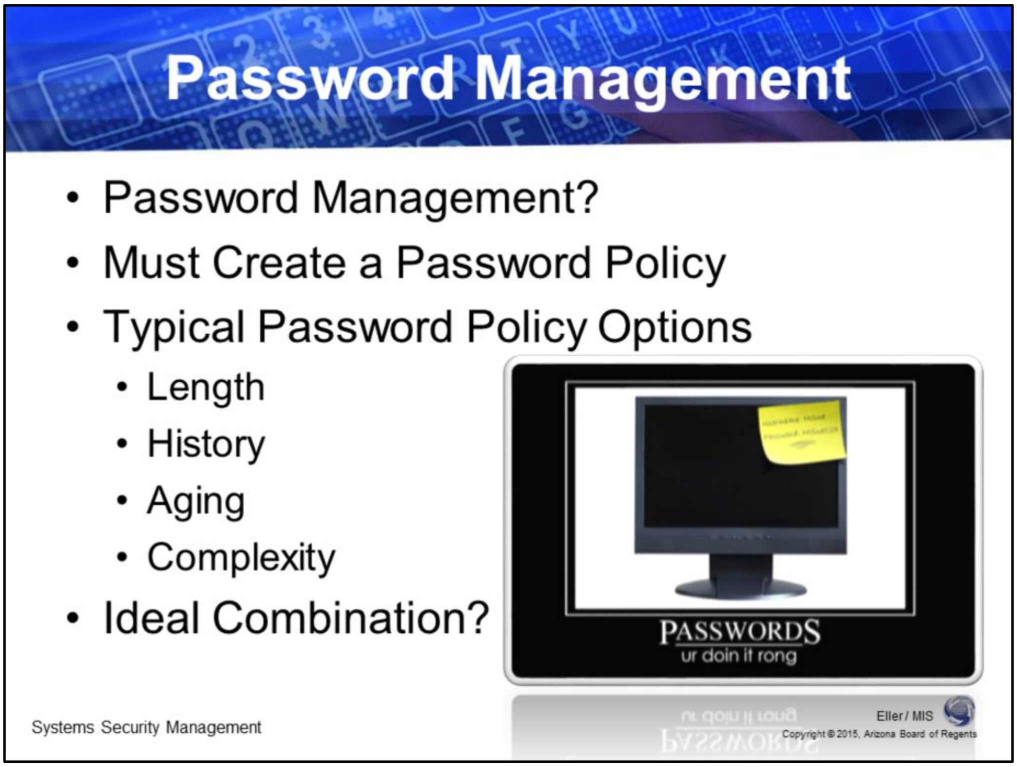
User Status: Is the user in question still employed with the organization? Are they a temporary or contract worker currently not working for the company or the contract was terminated? If the answer to these questions is yes, then the user account should be deleted or disabled to prevent this person from attempting to access company resources they no longer have a right to access.

Expirations: One way to prevent security breaches, especially with temporary or contract employees, is to use the ability to create an automatic account expiration when creating the user account. The user account can be set to disabled once the expected contract (or end of temp employment) date has been reached. In the event the contract or temp employment has been extended, it is a simple matter to reactivate the account and extend the expiration date.

Should you Delete or Disable?

The question of should you delete the account or simply disable the account is something that should be determined by the user account policy within the company. Deleting the account when it is no longer needed makes the process of housekeeping much simpler (and cleaner); however, this can cause other issues, especially in the event the account is needed again (either temporarily or permanently). For example, assuming a contract employee finishes their assigned contract and the account is deleted, if the same person is contracted again, the system administrator will need to recreate the account and reassign the necessary access rights. Had the systems administrator disabled the account instead, then they may have only needed to reactivate the account.

Depending on the level of security required by the company, deleting the user account after termination may be preferred or required. Sometimes this is a legal issue, other times it is simply a preference. Regardless, this issue should be addressed in the user account policy.



Password Management

- Password Management?
- Must Create a Password Policy
- Typical Password Policy Options
  - Length
  - History
  - Aging
  - Complexity
- Ideal Combination?

PASSWORDS
ur doin it rong

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

What is password management and is it necessary?

How do you ensure your users are helping keep your systems secure? This is typically a matter of educating the users on computer security; however, sometimes education is not enough, especially when the systems administrator has tools available to help enforce security requirements. Password management is the act of implementing rules governing how passwords are created and maintained for a company's acceptable level of risk.

Users in a large organization frequently have many passwords, each protecting their access to a different computer system. Users have some basic limitations, which limit what can be done in the context of secure password management. In particular, it is hard for most people to remember:

Complicated passwords.
Many different passwords.
Passwords that change frequently.
Passwords for systems that are used infrequently.

When people have trouble remembering their passwords, they do one or more of the following things:

Write down their passwords -- and reduce security to the protection afforded by a piece of paper.
Forget their passwords -- and require frequent assistance from a computer help desk organization to reset it.
Use very simple, easily compromised passwords.
Reuse old passwords as often as possible.

Clearly, sound password management practices must take into consideration human limitations, to limit the above problems. The creation of a password management policy is recommended to help keep passwords and the systems they are used to access secure ("Password Management Best Practices," 2009).

Some password management options typically used to help keep systems more secure:

Minimum Password Length: This is exactly what it sounds like. What is a minimum number of characters required in a user's password.

Password History: How many passwords should the authenticating system remember? In other words, when a user is required, or has a need, to change their password, will the system allow them to reuse their existing password, or will it require a new one?

Maximum/Minimum Password Age: The maximum age option is used to determine when a user will be required to change their password. For example, after six months the user will be forced to change their password. The minimum option is used to prevent a user from changing their password multiple times in a row to get around a password history requirement.

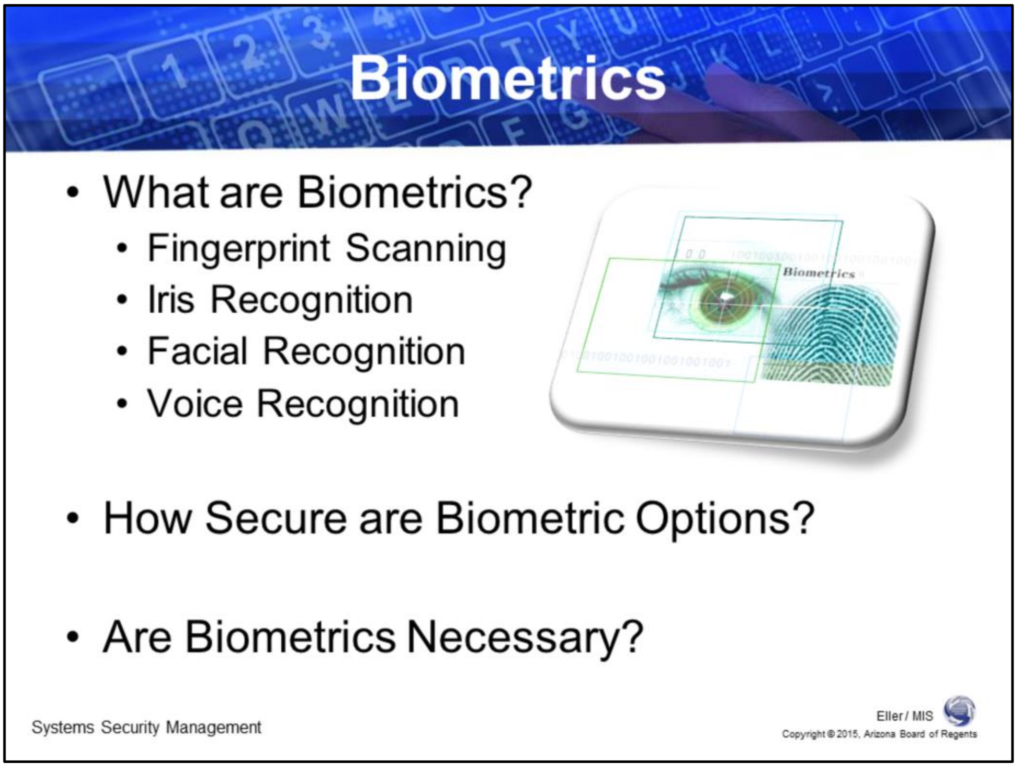
Password Complexity: The complexity requirement is one that states a password MUST have three of the following four items used within the password:

Lowercase letters
Uppercase letters
Numbers
Symbols

In addition to three of those options, the password may also not contain any personally identifiable information, such as the user's first or last name.

Is there an ideal combination for effective password management?

No, but many companies adopt some form of password management. A common combination is a one year maximum password age, with complexity rules, a minimum of 8 characters, and a history of five previous passwords. This should be defined in the company's user account policies.



Biometrics

- What are Biometrics?
  - Fingerprint Scanning
  - Iris Recognition
  - Facial Recognition
  - Voice Recognition
- How Secure are Biometric Options?
- Are Biometrics Necessary?

Systems Security Management

Eller / MIS

Biometrics

What are biometrics?

“Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristics. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent” (“An Introduction to Biometrics,” 2009).

“Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming socially acceptable and cost effective” (“An Introduction to Biometrics,” 2009).

There are a number of biometric options becoming available for increased systems security; however, the most common by-far at this time are fingerprint scanners. Other options, such as iris, facial, and voice recognition devices are beginning to enter the market; however, many are cost prohibitive at this time.

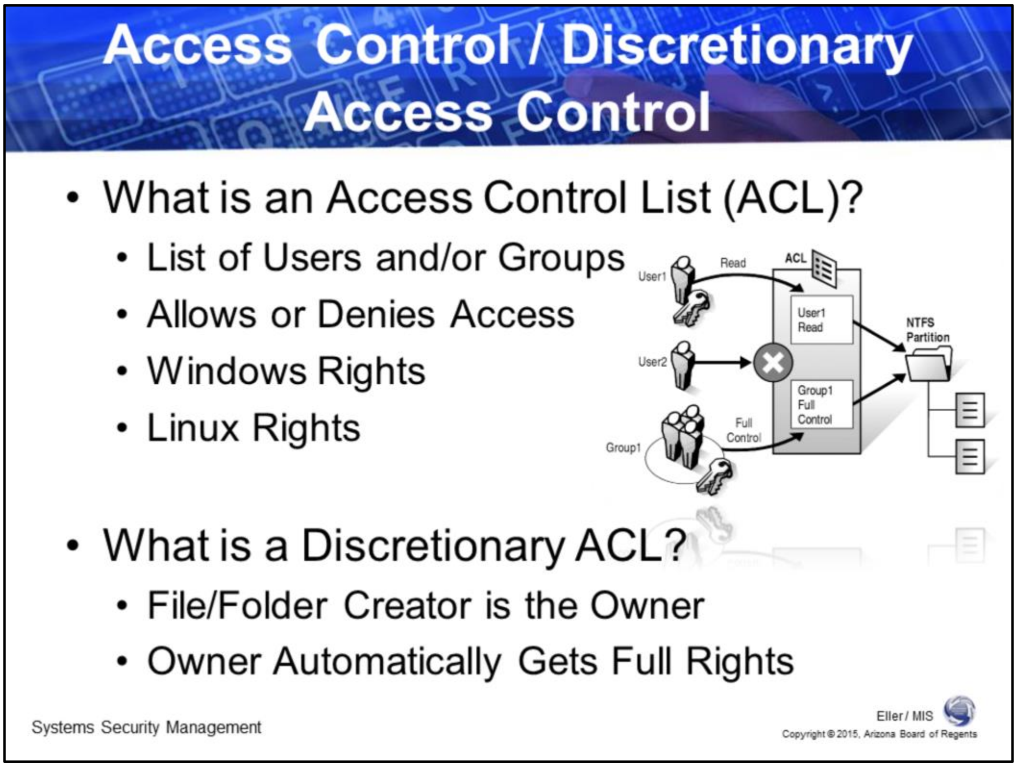
How secure are biometric options?

“There’s usually an inverse relationship between enterprise security and end user convenience. When you tighten security, it often means more hoops for users to jump through – more complex passwords to remember, more sign-ons to endure, more tokens or cards to carry. That’s when you end up with passwords on Post-its, completely defeating your attempts at stronger security” (Muathaler, 2007).

“The layers of security you can build around biometric authentication can help you secure a client device, your network, or an application or service. It’s important to note that the solutions can be designed to fit into what you already have in place, so there’s no “rip and replace” necessary. And the benefits are real. At the device level, you get simpler security procedures, theft deterrent, and protection of sensitive data. At the network level, there’s simplified VPN and Wi-Fi access, reduced help desk costs and a strong audit trail. And at the service or application level, you can eliminate phishing, provide transaction tracking and have hardware-based security” (Muathaler, 2007).

Are biometrics necessary?

It depends. If your company is very security conscience, biometrics provide a very secure method for authentication and systems access. In other companies, the cost of the technology may prohibit its availability and use. In general, biometrics are not necessary; however, there are some significant security benefits with regard to their use.



Access Control / Discretionary Access Control

- What is an Access Control List (ACL)?
  - List of Users and/or Groups
  - Allows or Denies Access
  - Windows Rights
  - Linux Rights

- What is a Discretionary ACL?
  - File/Folder Creator is the Owner
  - Owner Automatically Gets Full Rights

Systems Security Management

Eller / MIS

What is an Access Control List (ACL)?

An Access Control List (ACL) is a list of users and/or groups which are granted or denied access to files, folders, or other network objects and resources, such as printers. ACLs are used by all major operating systems as a means of controlling who has access to a system and its resources.

Windows Rights

The following permissions are included with the Windows operating systems:

Full Control: Read, List Contents, Write, Delete, Take Ownership – basically you can do anything with this access right.
Modify: Read, List Contents, Write, Delete – cannot take ownership of files.
Write: Read, List Contents, Write.
Read: Read, List Contents.
Special Permissions: Any combination of the above, can get into very specific permissions.

Linux Rights

In Linux, permissions are treated somewhat differently; each file and directory has group permissions in addition to basic permission types.

The group rights are:

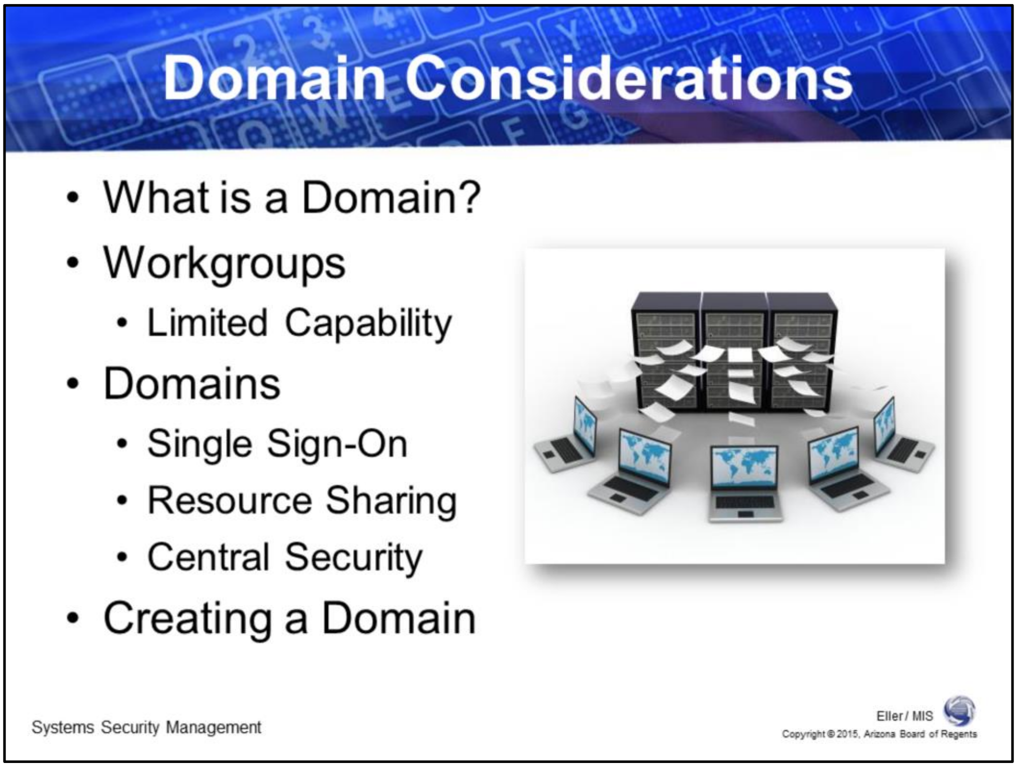
Owner: These permissions apply to the owner of the file or directory.
Group: These permissions apply to the group that has been assigned to the file or directory.
Others: These permissions apply to everyone else.

Permission Types:
[r] Read: Allows the user or group to read a file.
[w] Write: Allows the user or group to write to a file.
[x] Execute: Allows the user or group to execute a file.

We'll cover these permissions more in-depth in Module 11 – File, Directory, and Shared Resource Security.

What is a Discretionary Access List?

"In layman's terms, discretionary access control means that each object has an owner and the owner of the object gets to choose its access control policy. There are loads of objects in Windows that use this security model, including printers, services, and file shares. All secure kernel objects also use this model, including processes, threads, memory sections, synchronization objects such as mutexes and events, and named pipes" (Tavares, 2004).



Domain Considerations

- What is a Domain?
- Workgroups
  - Limited Capability
- Domains
  - Single Sign-On
  - Resource Sharing
  - Central Security
- Creating a Domain

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

What is a domain?

“The term domain can refer either to a local subnetwork or to descriptors for sites on the Internet. On a local area network (LAN), a domain is a subnetwork made up of a group of clients and servers under the control of one central security database. Within a domain, users authenticate once to a centralized server known as a domain controller, rather than repeatedly authenticating to individual servers and services. Individual servers and services accept the user based on the approval of the domain controller” (“What is a Domain?,” 2009).

Workgroups

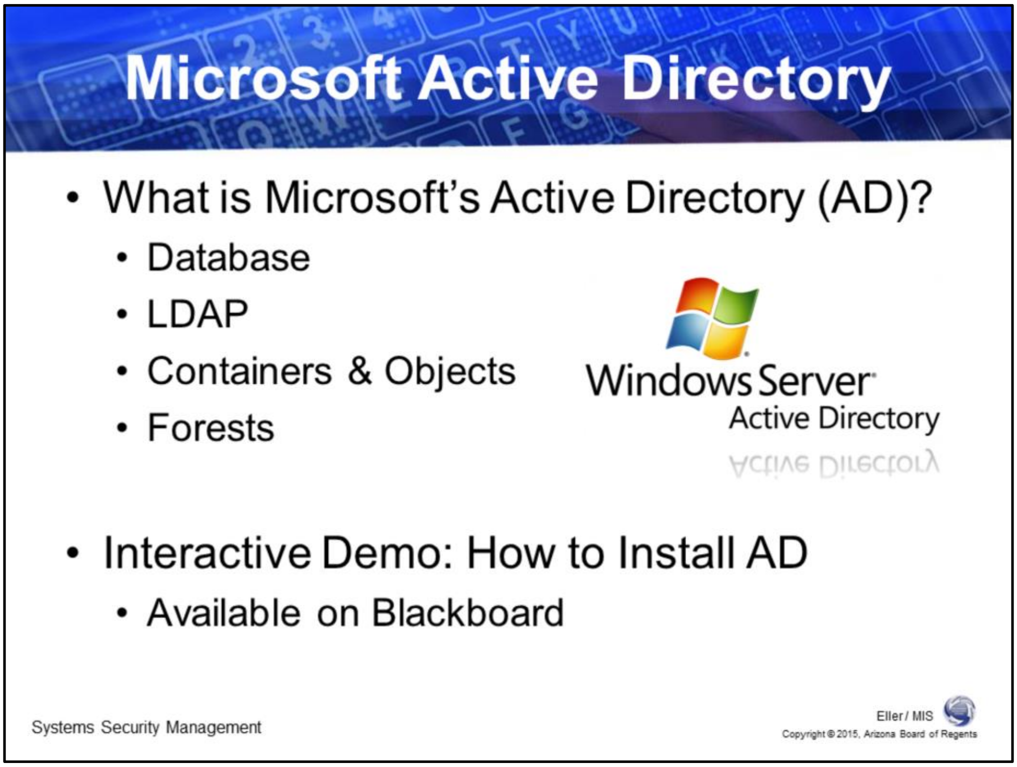
Workgroups are a means of grouping computers logically on a network that is not serviced by a Windows domain. While workgroups allow multiple computers to be grouped together, they do not provide any centralization of services. In addition, workgroups are limited in capabilities, including a hard limit of 10 different users accessing a shared resource at one time. In addition, with no centralized authentication method, workgroups require user accounts with the exact same username/password combination (or providing multiple accounts for each user) on every system sharing a resource on the network. Assuming the system administrator has a very small network of computers, for example in a small office of 10 or fewer computers, then a workgroup might make the most sense.

The Benefits of a Domain

A domain network provides a large number of benefits that are unavailable in a workgroup environment. First and foremost is the benefit of centralized authentication and authorization. The flexibility to assign a single user account access to multiple resources across the domain makes resource sharing efficient and effective. In addition, a single sign-on provides users with fewer username and password combinations to remember, making network access simpler. Domains also allow the systems administrator to create system-wide security policies, where changes can be made in one location on the network and propagated automatically to every computer or user connected to the domain.

How do you create a domain?

In Windows 2003 Server through Windows Server 2012 R2, a domain is created through the installation and configuration of Microsoft’s Windows Active Directory Services.



Microsoft Active Directory

- What is Microsoft's Active Directory (AD)?
  - Database
  - LDAP
  - Containers & Objects
  - Forests
- Interactive Demo: How to Install AD
  - Available on Blackboard

Windows Server
Active Directory

Systems Security Management

Eller / MIS

What is Microsoft's Windows Server Active Directory (AD) Services?

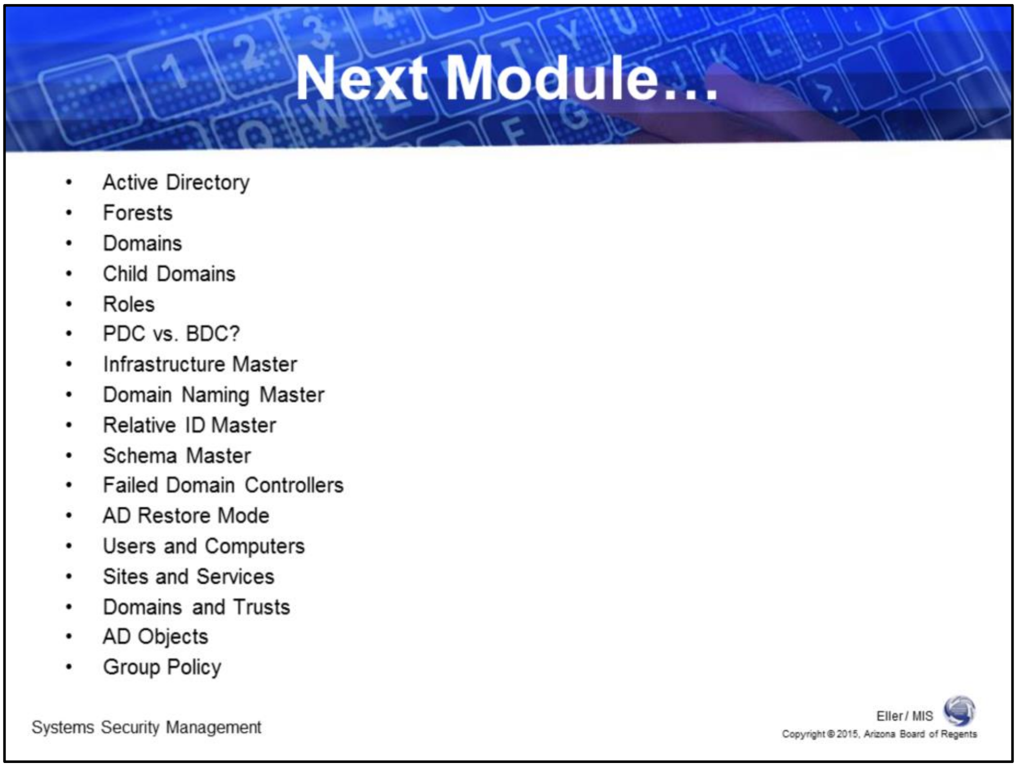
At its most basic level, Microsoft's AD Services is simply a database containing a variety of objects defining resources and access rights to the network. Built on the lightweight directory access protocol (LDAP), AD allows systems administrators, and those whom the SysAdmin has delegated responsibility, to create user accounts, groups, policies, computer accounts, organizational units (OUs), shared folders, printers, among other objects.

When creating an AD domain, some thought needs to go into the design. There are multiple levels to a Windows AD domain environment, beginning with a Forest. The Forest is an overarching schema shared by multiple domains (or trees) within the Forest. Each domain, when initially configured, must be setup as members of the same Forest in order to share resources between the domains. When these domains are created, an automatic trust relationship is established between them, making resource sharing simple and secure. Resources within the individual domains can then be configured to allow other forest-member domains access if necessary.

More Information on AD

For more information on Microsoft AD Services, check out the interactive Flash demo in Blackboard detailing how to install and configure Microsoft AD Services.

For your AD Design Lab, you will be responsible for designing the AD for the Fortune Automotive corporation. Check the Assignments section for detailed instructions on how to complete this individual lab assignment.

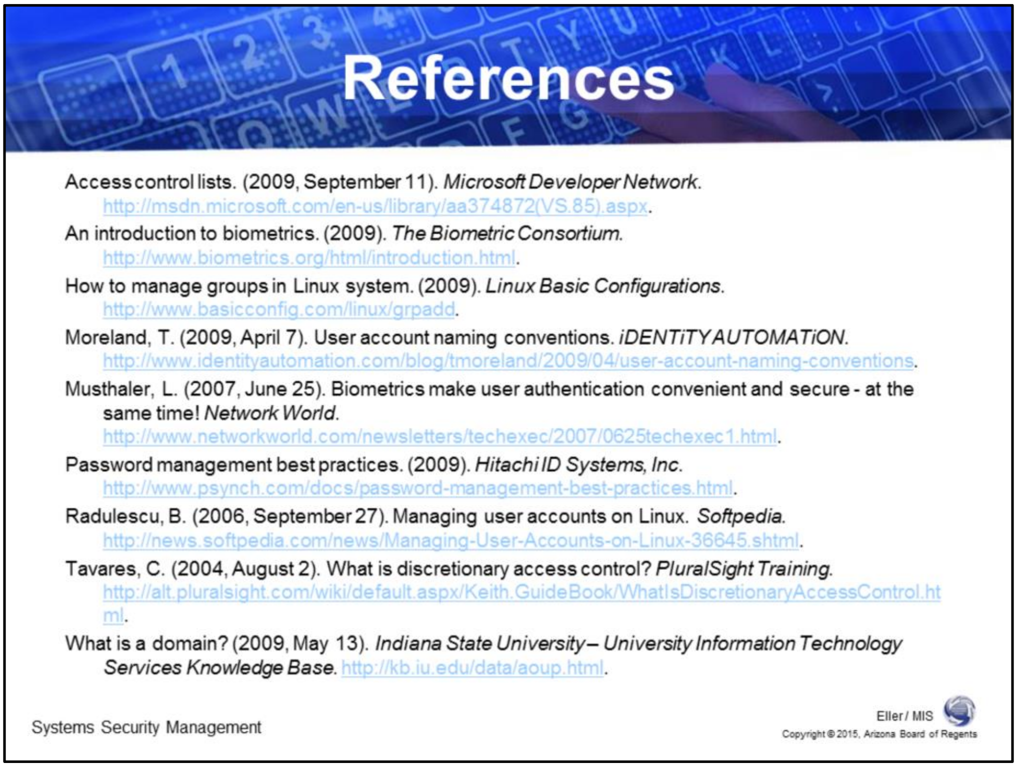


Next Module…

- Active Directory
- Forests
- Domains
- Child Domains
- Roles
- PDC vs. BDC?
- Infrastructure Master
- Domain Naming Master
- Relative ID Master
- Schema Master
- Failed Domain Controllers
- AD Restore Mode
- Users and Computers
- Sites and Services
- Domains and Trusts
- AD Objects
- Group Policy

Systems Security Management

Eller / MIS



References

Access control lists. (2009, September 11). *Microsoft Developer Network*. http://msdn.microsoft.com/en-us/library/aa374872(VS.85).aspx.

An introduction to biometrics. (2009). *The Biometric Consortium*. http://www.biometrics.org/html/introduction.html.

How to manage groups in Linux system. (2009). *Linux Basic Configurations*. http://www.basicconfig.com/linux/grpadd.

Moreland, T. (2009, April 7). User account naming conventions. *iDENTiTY AUTOMATiON*. http://www.identityautomation.com/blog/tmoreland/2009/04/user-account-naming-conventions.

Musthaler, L. (2007, June 25). Biometrics make user authentication convenient and secure - at the same time! *Network World*. http://www.networkworld.com/newsletters/techexec/2007/0625techexec1.html.

Password management best practices. (2009). *Hitachi ID Systems, Inc*. http://www.psynch.com/docs/password-management-best-practices.html.

Radulescu, B. (2006, September 27). Managing user accounts on Linux. *Softpedia*. http://news.softpedia.com/news/Managing-User-Accounts-on-Linux-36645.shtml.

Tavares, C. (2004, August 2). What is discretionary access control? *PluralSight Training*. http://alt.pluralsight.com/wiki/default.aspx/Keith.GuideBook/WhatIsDiscretionaryAccessControl.html.

What is a domain? (2009, May 13). *Indiana State University – University Information Technology Services Knowledge Base*. http://kb.iu.edu/data/aoup.html.