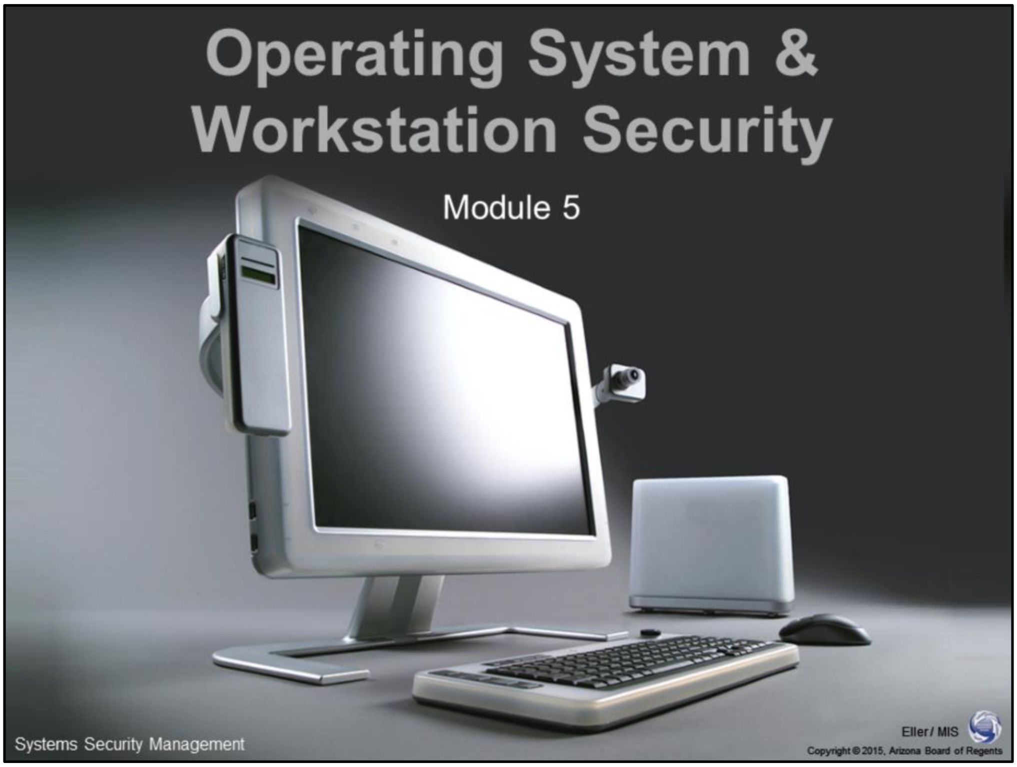
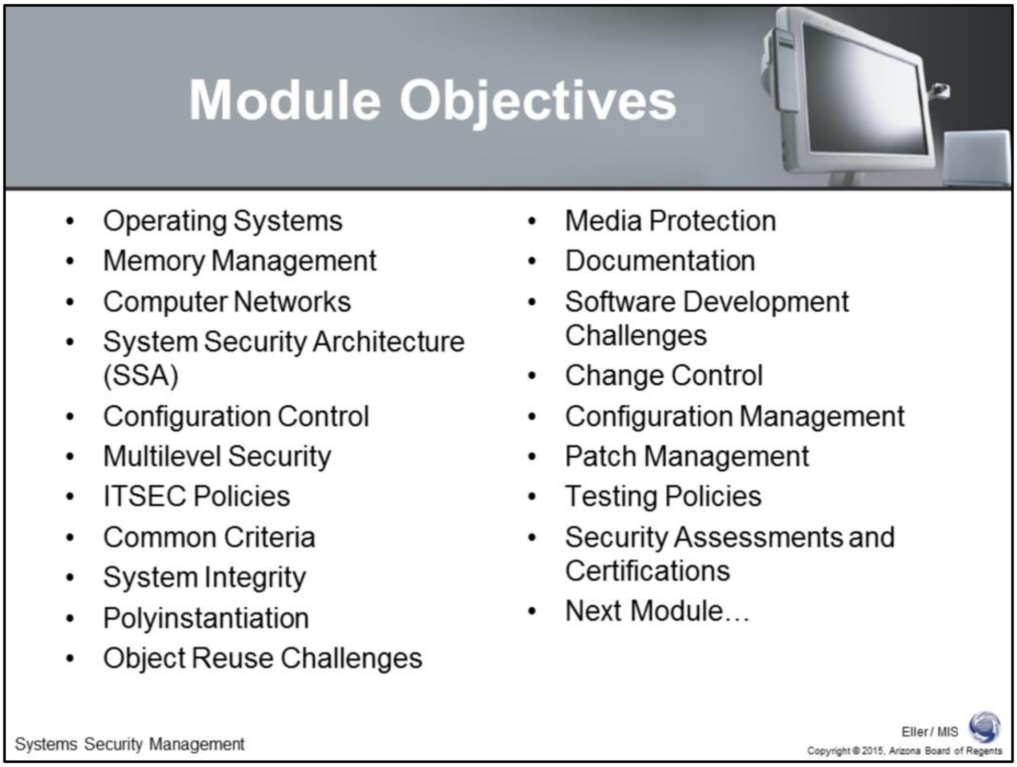


Operating System & Workstation Security

Module 5

Systems Security Management

Eller / MIS



Module Objectives

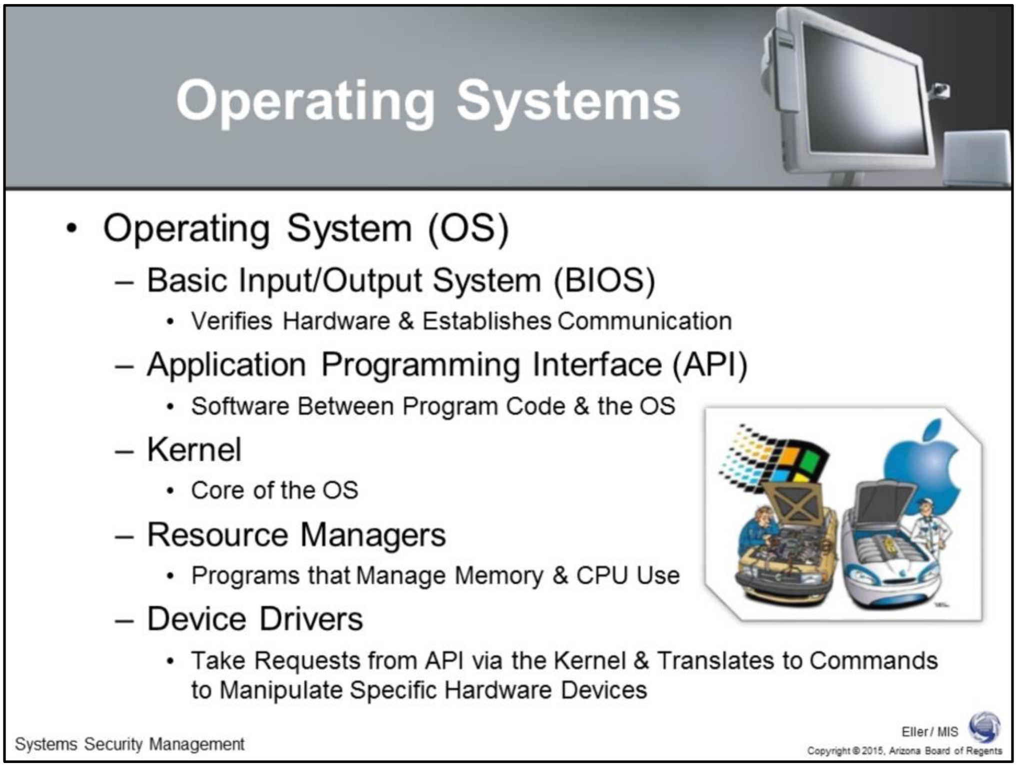
- Operating Systems
- Memory Management
- Computer Networks
- System Security Architecture (SSA)
- Configuration Control
- Multilevel Security
- ITSEC Policies
- Common Criteria
- System Integrity
- Polyinstantiation
- Object Reuse Challenges
- Media Protection
- Documentation
- Software Development Challenges
- Change Control
- Configuration Management
- Patch Management
- Testing Policies
- Security Assessments and Certifications
- Next Module…

Systems Security Management

Eller / MIS

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

- What an operating system is and how they are used.
- What memory management is and the basics of how it works.
- What a computer network is and the differences between different network types.
- How system security architecture helps with system design.
- Why configuration controls are used for improving security.
- What ITSEC policies and the Common Criteria are and why they are used.
- How system integrity can be ensured.
- What polyinstantiation is and how it is used for improving system security.
- What challenges arise when reusing objects and how to protect backup media.
- What system documentation is and why it is important.
- How software development challenges are overcome and how change controls improve this process.
- How patch management improves security and how testing policies help ensure system stability.
- Why security assessments and certifications are necessary in certain instances.



Operating Systems

- Operating System (OS)
  - Basic Input/Output System (BIOS)
    - Verifies Hardware & Establishes Communication
  - Application Programming Interface (API)
    - Software Between Program Code & the OS
  - Kernel
    - Core of the OS
  - Resource Managers
    - Programs that Manage Memory & CPU Use
  - Device Drivers
    - Take Requests from API via the Kernel & Translates to Commands to Manipulate Specific Hardware Devices

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

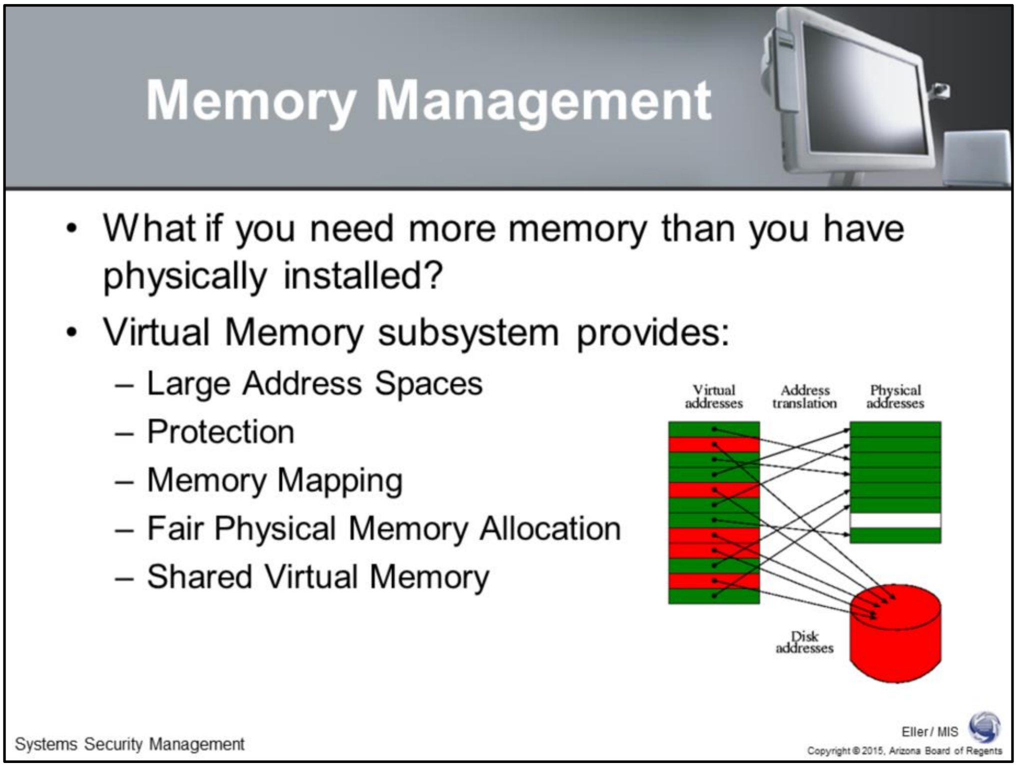
Operating Systems

What is an Operating System?

An operating system (OS) is computer software code that interfaces with user application software and the computer's basic input/output system (BIOS) to allow the application to interact with the computer's hardware. All of you should be familiar with an operating system, most likely with one or more versions of Windows. Other operating systems include Mac OS X and Linux.

An operating system typically consists of five primary areas: the BIOS, APIs, the kernel, resource managers, and device drivers.

- **The Basic Input/Output System (BIOS):** A computer program that conducts basic hardware and software communications inside the computer. Basically, a computer's BIOS resides between the computer hardware and the operating system, such as UNIX or Windows. Operating systems such as Mac OS X reside on computers which do not utilize a BIOS. These newer hardware systems use a different technology to accomplish the same tasks.
- **The Application Programming Interface (API):** APIs are functions of programming features in an operating system that programmers can use for network links, links to messaging services, or interfaces to other systems. Each OS provides its own API, used by software developers to allow for the creation of the applications we use every day, from Microsoft Office to custom applications in the workplace. It is important to note that APIs are not solely provided by an OS. APIs are also provided for specific development platforms and used for a variety of applications. This includes web-based applications as well as applications designed to run on a multitude of OS types (e.g. applications coded in a platform agnostic language such as Java).
- **The Kernel:** An essential set of programs and computer code built into a computer operating system to control processor, disk, memory, and other functions central to the basic operation of a computer. The kernel communicates with the BIOS, device drivers, and APIs to perform these functions. It also interfaces with the resource managers.
- **Resource Managers:** Programs that manage computer memory and CPU use. System administrators will use resource managers as a means of determining how well a server is performing given its use. The objective is to try and ensure the server is not overburdened with resource requests and performs as the organization requires. Should the resource manager reveal the server is unable to keep up with heavy loads, this is an indication the server hardware may need to be upgraded or additional servers need to be added to help spread the resource load.
- **Device Drivers:** Takes requests from the API via the Kernel and translates them into commands to manipulate specific hardware devices. For example, in order to send a document to your printer, the OS must use a device driver to convert the document into something the printer understands in order to provide the printed copy you expected.



Memory Management

- What if you need more memory than you have physically installed?
- Virtual Memory subsystem provides:
  - Large Address Spaces
  - Protection
  - Memory Mapping
  - Fair Physical Memory Allocation
  - Shared Virtual Memory

Virtual addresses
Address translation
Physical addresses
Disk addresses

Systems Security Management

Eller / MIS

Memory Management

What happens when you need more memory than you have physically installed? Since the early days of computers, there has been a need for more memory than can feasibly be installed in a computer, even with high-end servers having terabytes of RAM, and workstations having upwards of 32GB installed in them, there is sometimes still a need for more memory. This is where virtual memory management techniques come into play. Some virtual memory management techniques include large address spaces, protection, memory mapping, fair physical memory allocation, and shared virtual memory.

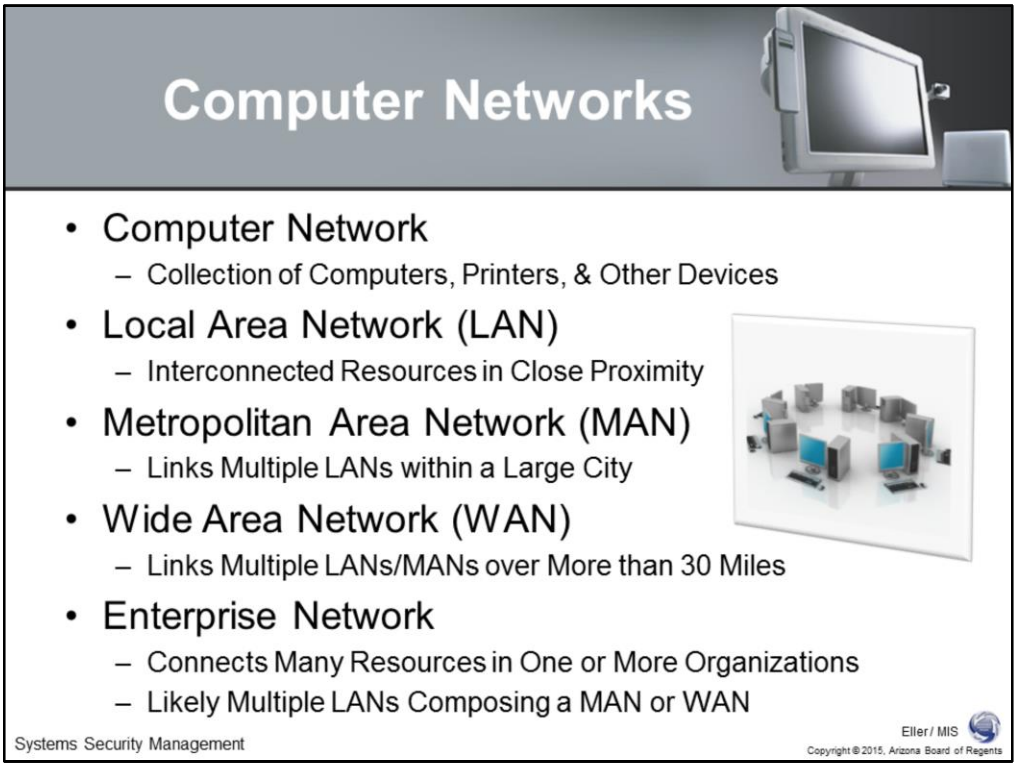
Large Address Spaces – The operating system will pretend that it has more memory than is actually installed in the system. This is the paging file in Windows, and Swap file in Linux, UNIX, and Mac OS X.

Protection – Each process has its own virtual memory space, like its own sandbox, that prevents other processes from interfering. This also allows areas of memory to be protected from writing to prevent malicious applications from overwriting data and code during runtime.

Memory Mapping – This is used to map data files into a process address space; in memory mapping the contents of a file are linked directly into the virtual address space of a process.

Fair Physical Memory Allocation – This ensures that each process is given a fair share of the physical memory in times that direct RAM access is necessary.

Shared Virtual Memory – Even though each process can have its own sandbox, sometimes it becomes necessary for multiple processes to share the same space, for example, if you're running several applications that call to the same Dynamic Link Library (DLL) files in Windows, it's more efficient to load the DLL into memory one time and call back to it, rather than loading the DLL multiple times, once for each process that may use it (Rusling, 1999).



Computer Networks

- Computer Network
  - Collection of Computers, Printers, & Other Devices
- Local Area Network (LAN)
  - Interconnected Resources in Close Proximity
- Metropolitan Area Network (MAN)
  - Links Multiple LANs within a Large City
- Wide Area Network (WAN)
  - Links Multiple LANs/MANs over More than 30 Miles
- Enterprise Network
  - Connects Many Resources in One or More Organizations
  - Likely Multiple LANs Composing a MAN or WAN

Systems Security Management

Eller / MIS

Computer Networks

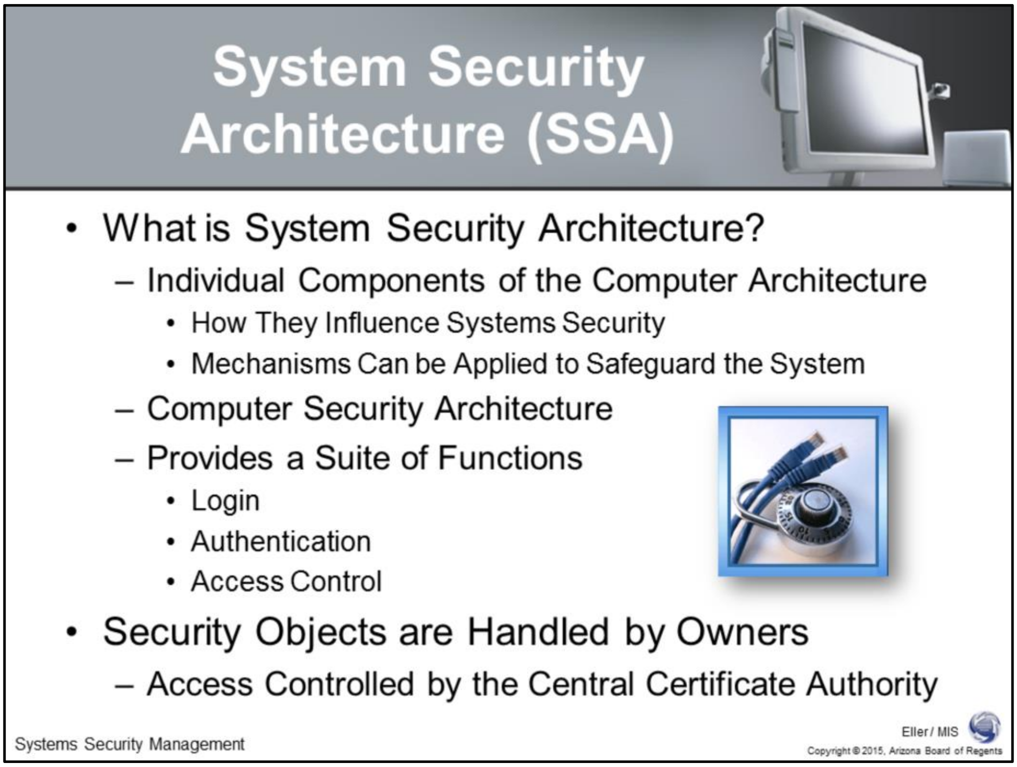
A computer network is a system of computers, print devices, network devices, and computer software linked by communications cabling or radio waves. There are four primary types of computer networks, including LANs, MANs, WANs, and Enterprise Networks.

Local Area Network (LAN) – A series of interconnected computers, printing devices, and other computer equipment that share hardware and software resources. Sound similar to the generic definition for a computer network? This is because a LAN is what everyone uses for a local network, in your home and your workplace.

Metropolitan Area Network (MAN) – A network that links multiple LANs in a large city or metropolitan region.

Wide Area Network (WAN) – A far-reaching system of networks that usualy extends over 30 miles (approximately) and often reaches across states and continents.

Enterprise Network – A combination of LANs, MANs, or WANs that provides computer users with an array of computer and network resources for completing different tasks. Enterprise networks are commonly used to connect many different resources in one or more organizations.



System Security Architecture (SSA)

- What is System Security Architecture?
  - Individual Components of the Computer Architecture
    - How They Influence Systems Security
    - Mechanisms Can be Applied to Safeguard the System
  - Computer Security Architecture
  - Provides a Suite of Functions
    - Login
    - Authentication
    - Access Control
- Security Objects are Handled by Owners
  - Access Controlled by the Central Certificate Authority

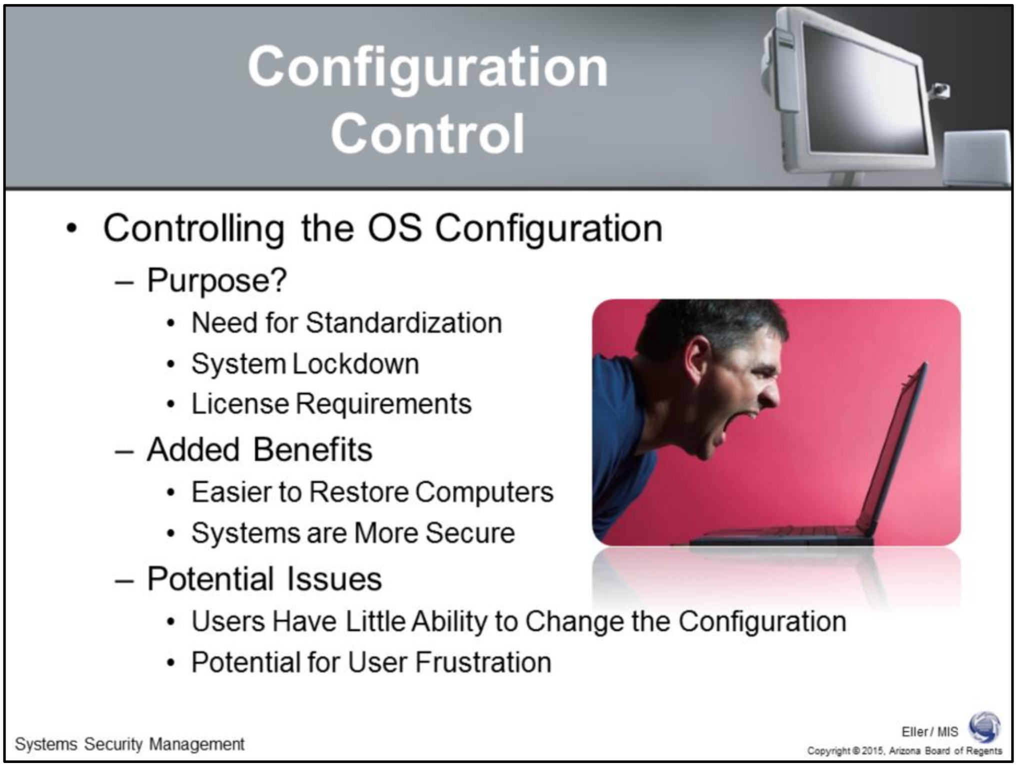
Systems Security Management

Eller / MIS

System Security Architecture (SSA)

System Security Architecture takes the individual components of the computer architecture in order to determine how the components influence the security of the system. Taking this information, the SSA will highlight different mechanisms that can be applied to help safeguard the system.

Computer Security Architecture is a similar concept to the System Security Architecture, providing a series of functions designed to help ensure the security of a computer system. These functions include the use of logins, authentication, and access controls. In general, the security objects associated with this architecture are handled by the object owners and access is typically controlled by a central certificate authority.



Configuration Control

- Controlling the OS Configuration
  - Purpose?
    - Need for Standardization
    - System Lockdown
    - License Requirements
  - Added Benefits
    - Easier to Restore Computers
    - Systems are More Secure
  - Potential Issues
    - Users Have Little Ability to Change the Configuration
    - Potential for User Frustration

Systems Security Management

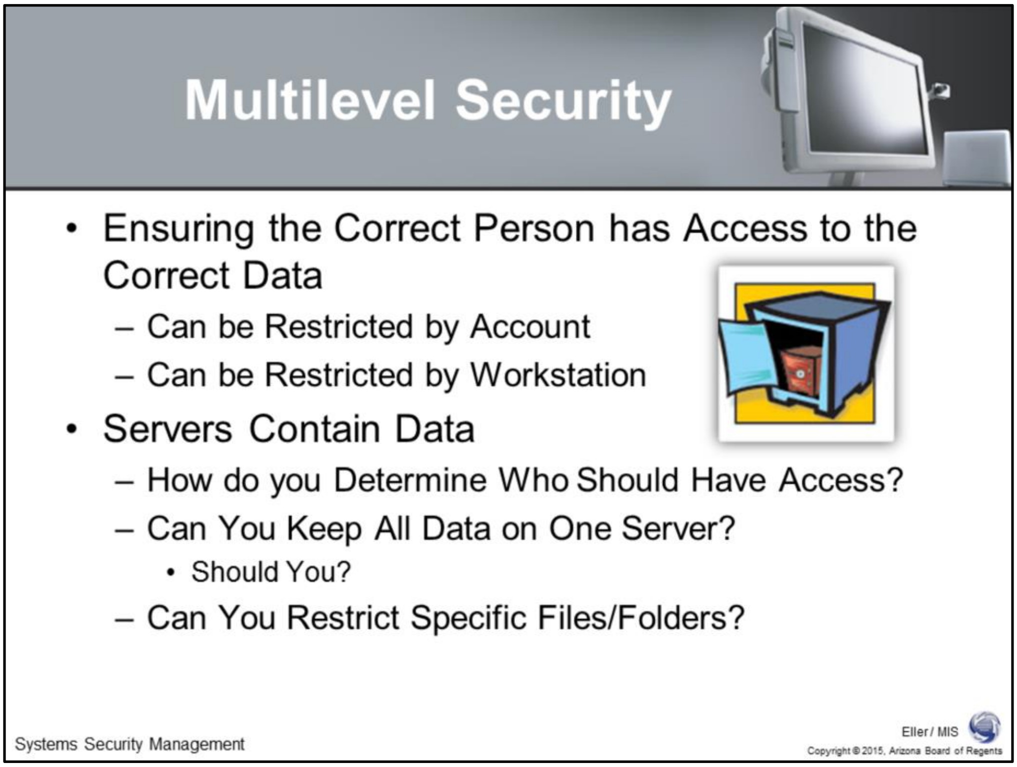
Eller / MIS

Configuration Control

Depending on the needs of an organization, it may be necessary for IT to have control of the Operating System configuration. This is usually done when there is a strong need for standardization of system configurations, a need for locking down the system, or due to licensing requirements. For example, some companies may develop their own applications which may have been designed to run on a specific operating system with specific software. In this case unless the company wants to allocate a budget to upgrade or modify the original application, the company will need to keep employees systems standardized with a specific set of software.

There are some added benefits to using configuration controls. For the IT department, standardized systems make it much easier to restore systems in the event of a hardware or software failure. Another added benefit is by standardizing, the systems are inherently more secure. This is because IT completely understands the configuration and can make specific choices to help keep the system secured. In addition, the IT department will only need to support a specific set of software which helps to streamline the IT support process.

Despite the benefits there are a few negative aspects that should be considered from the user's perspective. When a company uses configuration controls, the users will have little ability to change the configuration. Because of this it usually means the users cannot install software or updates and must contact IT to do this for them. This can create a potential for user frustration since they are now dependent on someone else to do what they feel they need to do. Configuration control can be necessary and should be considered in organizations. Just make sure to spend the time needed to weigh the pros and cons.



Multilevel Security

- Ensuring the Correct Person has Access to the Correct Data
  - Can be Restricted by Account
  - Can be Restricted by Workstation
- Servers Contain Data
  - How do you Determine Who Should Have Access?
  - Can You Keep All Data on One Server?
    - Should You?
  - Can You Restrict Specific Files/Folders?

Systems Security Management

Eller / MIS

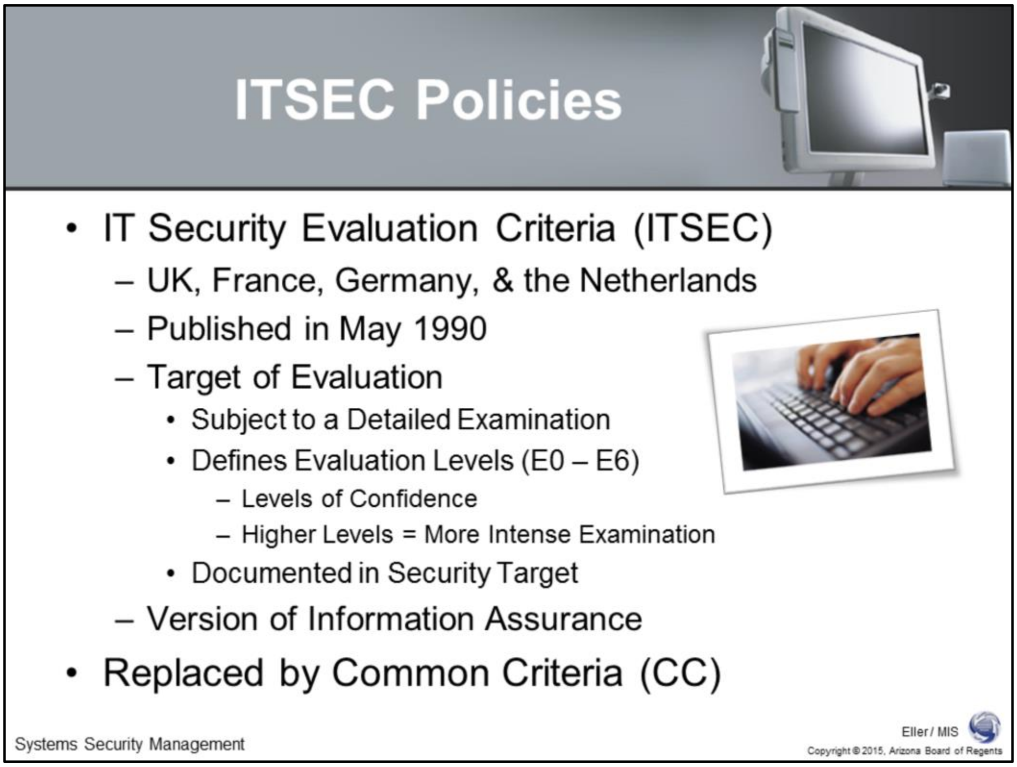
Multilevel Security

As we have discussed before, multilevel security is a technique used to provide multiple layers of security between the users and the data. The main goal is to make certain the correct person has access to the correct data. There are a number of ways this can be accomplished, including restricting access to a system based on user accounts or based on the workstation an account is logged into. Both of these can be used to add an additional layer of security as well.

In general, servers will contain data that needs to be accessed by someone. As a SysAdmin, how do you determine who should have access to the data? This is usually determined by the user's job function, although some companies require management authorization, or security classification, in order to grant access to specific data.

Can you keep all of the data on one server and should you? Yes, you can keep the data all on one server, but the question of should you depends entirely upon the needs of the organization.

Can you restrict specific files and folders? Absolutely. We will discuss how to do this specifically in Module 11.



ITSEC Policies

- IT Security Evaluation Criteria (ITSEC)
  - UK, France, Germany, & the Netherlands
  - Published in May 1990
  - Target of Evaluation
    - Subject to a Detailed Examination
    - Defines Evaluation Levels (E0 – E6)
      - Levels of Confidence
      - Higher Levels = More Intense Examination
    - Documented in Security Target
  - Version of Information Assurance
- Replaced by Common Criteria (CC)

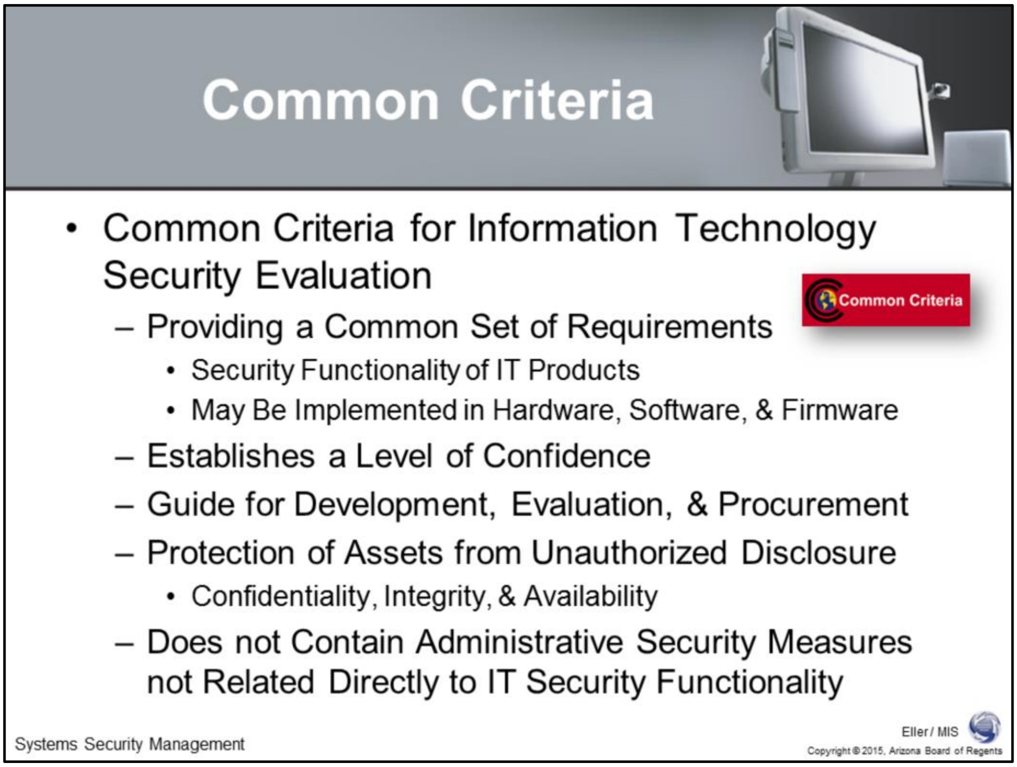
Systems Security Management

Eller / MIS

ITSEC Policies

The Information Technology Security Evaluation Criteria (ITSEC) is a structured set of criteria for evaluating computer security within products and systems. ITSEC was developed and published in May of 1990 and was used primarily in the UK, France, Germany, and the Netherlands. When it was decided a system should become the target of an ITSEC evaluation, the system would be subjected to a very detailed examination. ITSEC policies define a range of evaluation levels, from E0 to E6, which represent levels of confidence needed in the system. The higher the level needed, the more intense the examination will be. Finally, the examination would be fully documented in order to justify any decisions at a later time.

If this sounds vaguely familiar, it is because it should be familiar. This is essentially an early version of Information Assurance. The ITSEC was eventually replaced by an updated policy called the Common Criteria, or CC.



Common Criteria

- Common Criteria for Information Technology Security Evaluation
  - Providing a Common Set of Requirements
    - Security Functionality of IT Products
    - May Be Implemented in Hardware, Software, & Firmware
  - Establishes a Level of Confidence
  - Guide for Development, Evaluation, & Procurement
  - Protection of Assets from Unauthorized Disclosure
    - Confidentiality, Integrity, & Availability
  - Does not Contain Administrative Security Measures not Related Directly to IT Security Functionality

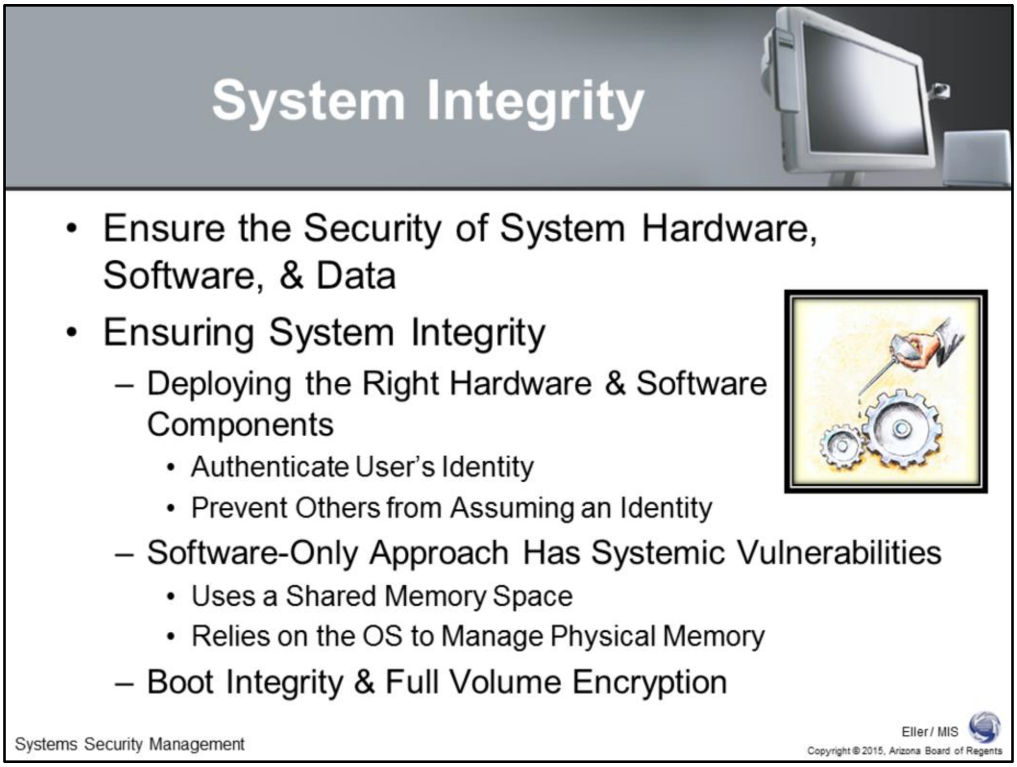
Systems Security Management

Eller / MIS

Common Criteria (CC)

The Common Criteria for Information Technology Security Evaluation is an updated version of ITSEC policies. This criteria provides a common set of requirements for the security functionality of IT products. In addition, the criteria can be used and implemented for evaluating hardware, software and firmware. The criteria was designed to establish a level of confidence in the security of IT products and is used as a guide for the development, evaluation, and procurement of IT systems and software.

The Common Criteria also defines how to protect assets from unauthorized disclosure. This is where the criteria describes the confidentiality, integrity, and availability of IT systems. The one area the CC does not define involves administrative security measures that are not related directly to IT security functionality.



System Integrity

- Ensure the Security of System Hardware, Software, & Data
- Ensuring System Integrity
  - Deploying the Right Hardware & Software Components
    - Authenticate User's Identity
    - Prevent Others from Assuming an Identity
  - Software-Only Approach Has Systemic Vulnerabilities
    - Uses a Shared Memory Space
    - Relies on the OS to Manage Physical Memory
  - Boot Integrity & Full Volume Encryption

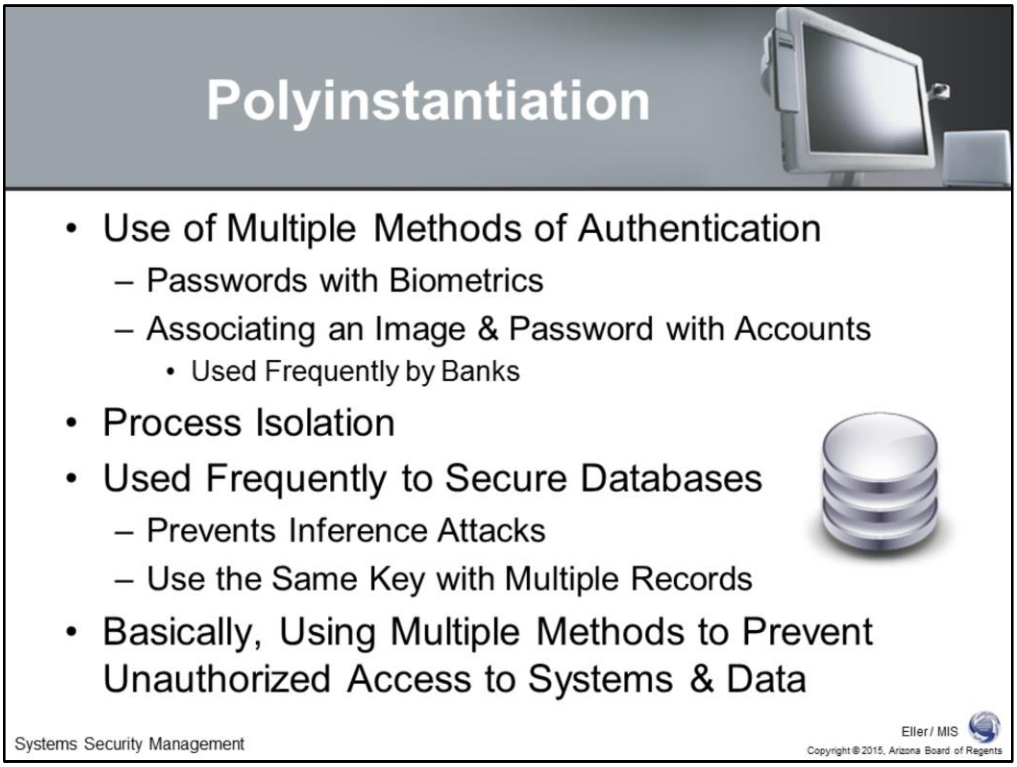
Systems Security Management

Eller / MIS

System Integrity

System integrity is an attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. In other words system integrity is ensuring the security of system hardware, software, and data. Ensuring system integrity means deploying the right hardware and software components to authenticate a user's identity and prevent others from assuming an identity.

A software-only approach to system integrity has systemic vulnerabilities in that they tend to use a shared memory space and because of this they rely on the operating system to manage the physical memory in the system. A combined approach of hardware and software works well together. A system capable of managing the boot integrity of the system and using full volume encryption are recommended for guaranteeing system integrity.



Polyinstantiation

- Use of Multiple Methods of Authentication
  - Passwords with Biometrics
  - Associating an Image & Password with Accounts
    - Used Frequently by Banks
- Process Isolation
- Used Frequently to Secure Databases
  - Prevents Inference Attacks
  - Use the Same Key with Multiple Records
- Basically, Using Multiple Methods to Prevent Unauthorized Access to Systems & Data

Systems Security Management

Eller / MIS

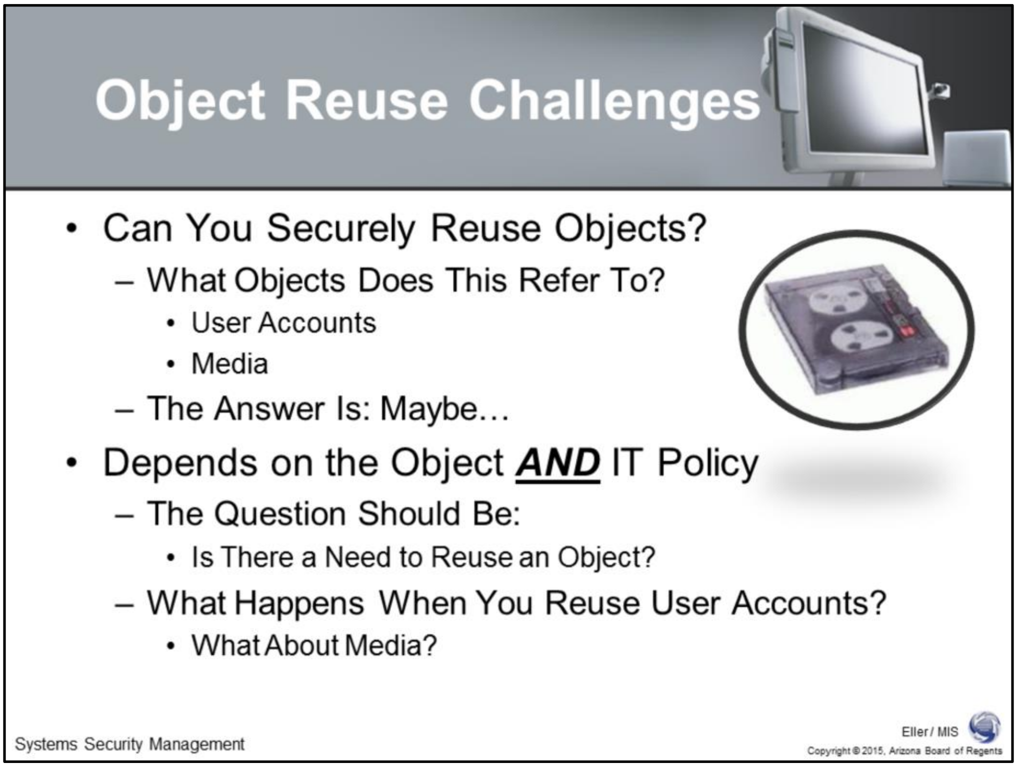
Polyinstantiation

Polyinstantiation has different meanings and uses depending on what you are using it for. For systems security, polyinstantiation can be used to provide multiple methods of authentication, so using a password with biometrics such as a fingerprint scanner or facial recognition would be one example. Another example would involve associating a specific image and password with a user account. This example is commonly used by banks to help ensure the security of a customer’s banking session.

Another use for polyinstantiation in system security involves process isolation. In other words, making sure that the shared memory used by process A cannot interfere with process B when it runs and vice versa.

Polyinstantiation is also used frequently to secure databases in order to prevent inference attacks. Database administrators and developers can use polyinstantiation to make it possible to use the same primary key in a database with multiple records, with the multiple instances being distinguished by security levels. This allows the information in a database to be safeguarded according to company policy; a query will only return the results at the level the operator has access to.

The bottom line with polyinstantiation is that is it uses multiple methods in an effort to prevent unauthorized access to systems and data.



Object Reuse Challenges

- Can You Securely Reuse Objects?
  - What Objects Does This Refer To?
    - User Accounts
    - Media
  - The Answer Is: Maybe…
- Depends on the Object ***AND*** IT Policy
  - The Question Should Be:
    - Is There a Need to Reuse an Object?
  - What Happens When You Reuse User Accounts?
    - What About Media?

Systems Security Management

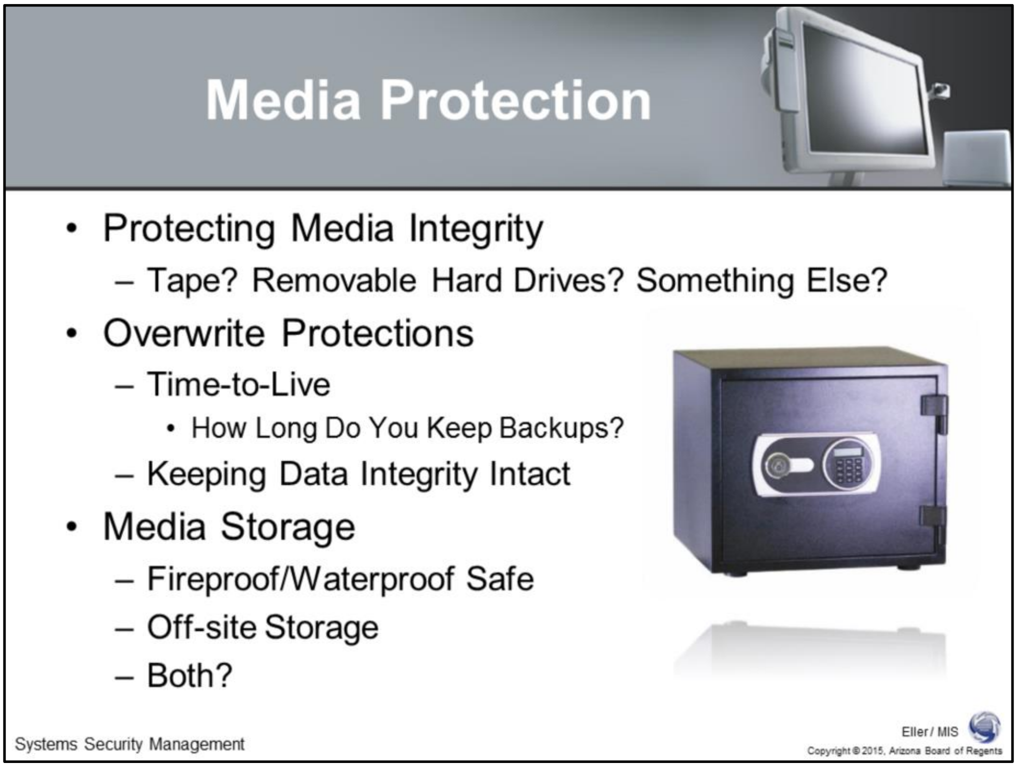
Eller / MIS

Object Reuse Challenges

Let’s start with a question: can you securely reuse objects? Well, this question leads to another: what objects does this refer to? The answer to the second question is any objects. Some objects you might see the first question referring to include user accounts or backup media. The answer to the first question is maybe. It really depends on the object in question and the IT policy the organization is enforcing. Based on this mindset, the next question should be: is there a reason or need to reuse an object?

Taking the above two examples, what happens when you reuse a user account? Well, user accounts, when created, are assigned a specific security ID. If the person using that account is terminated, the SysAdmin should either delete or disable the account. When the reuse question comes into play, this means the SysAdmin disabled the account. Now the organization hires a new employee to take the place of the one who left. Should the SysAdmin create a new account or just rename the old account and reuse it? Again, this depends on the organization’s IT policy. In general, a user account can be renamed and have the password reset and for all intents and purposes it becomes a new account. What makes this a good decision is that when reused it retains the original security ID of the original user account. This means the renamed account will have access to all the same resources as the original account, so it makes administration of user accounts simpler for the SysAdmin.

Now, what happens if you reuse backup media? Well, quite simply, you are erasing the original contents and overwriting them with new backups. This is certainly ok if, and only if, you have a media rotation in-place. What this means is you have multiple sets of backup media that you rotate through in order to retain the backups for a certain amount of time. So, if you have three sets of backup media that can each hold a maximum of 4 weeks of backups and your IT policy dictates that you must have a minimum of 6-8 weeks of backups available at any one time for restoration, you can safely reuse backup media as necessary.



Media Protection

- Protecting Media Integrity
  - Tape? Removable Hard Drives? Something Else?
- Overwrite Protections
  - Time-to-Live
    - How Long Do You Keep Backups?
  - Keeping Data Integrity Intact
- Media Storage
  - Fireproof/Waterproof Safe
  - Off-site Storage
  - Both?

Systems Security Management

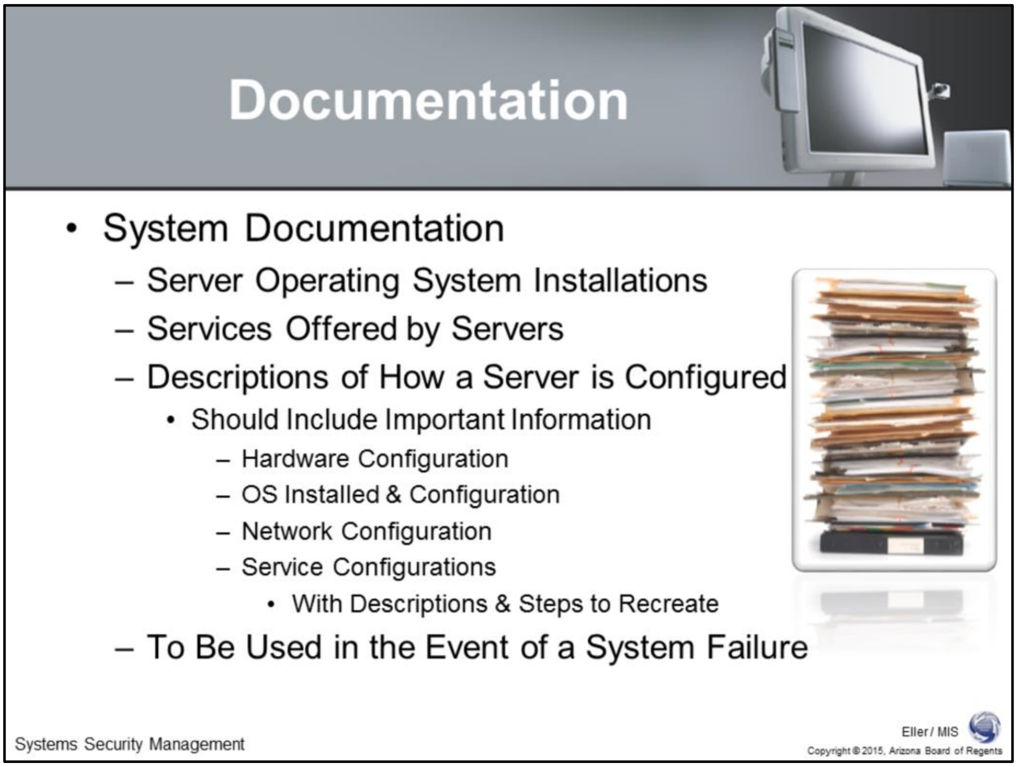
Eller / MIS

Media Protection

How do you protect the integrity of your backup media? It depends on the type of media you use. Do your backups use tapes, removable hard drives or something else? It is important to remember that media such as tapes or even CDs or DVDs have a limited life. You can only write to these media types so many times before they are no longer usable. The manufacturer of the media will be able to describe how long each media type can be used regularly before you should expect integrity failure and need to replace the media. Hard drives generally are less problematic as you can write and erase them for as long as the drives work. If you use consumer-level drives you should get at least 3 years out of them before they might begin to fail. With enterprise-level hard drives (much more expensive) you should get at least 5 years before seeing failures.

All backup software allows the SysAdmin to configure overwrite protection levels for backup media. What overwrite protection does is allow the SysAdmin decide how the backup system should deal with running out of space on the backup media. Should the system automatically begin overwriting older backups or should the system stop the backups until the media can be replaced? This is important to consider. Another option is known as time-to-live, in other words, how long should you keep backups for? Organizational IT policy should dictate the time-to-live and as the amount of data backed up daily grows, the SysAdmin needs to ensure there is enough media available to meet the time-to-live requirements. Both of these protections are designed to help maximize the life of backup media and keep the data integrity of the backups intact.

Finally, the last component of media protection involves how the backup media is stored. Some organizations purchase fireproof and waterproof safes to store tapes in. Others either have an off-site location to store media or hire a third party to store the media off-site. Some even have both, sending the most current backups off-site and keeping older ones on-site to be used in rotation after the current set is full.



Documentation

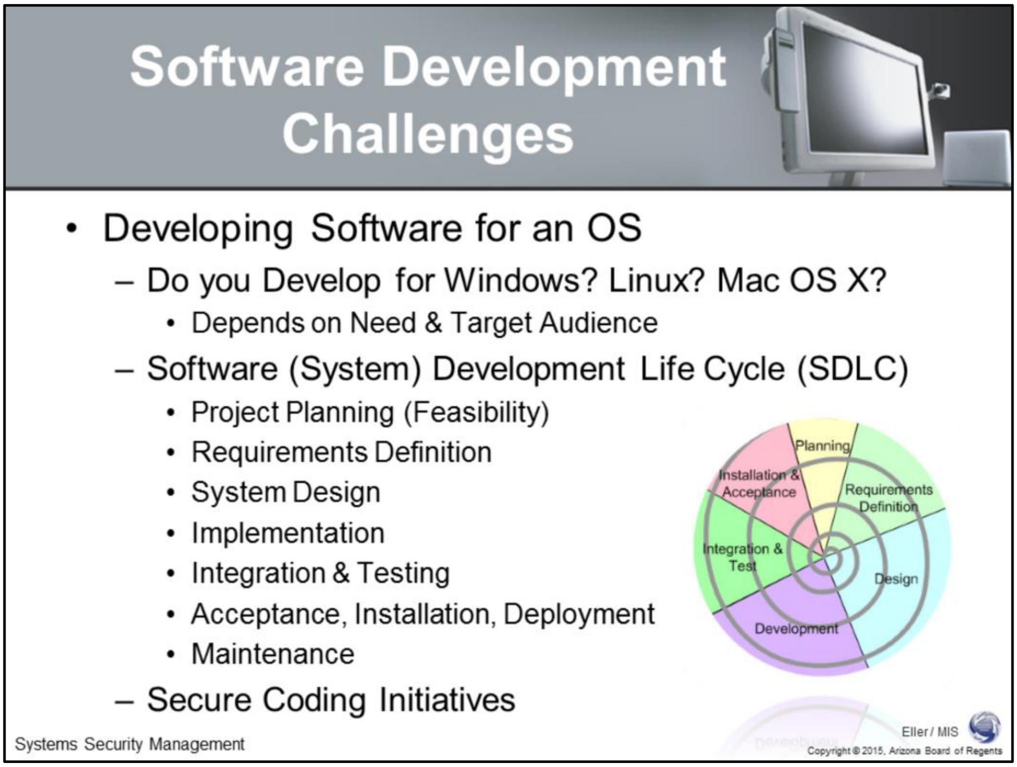
- System Documentation
  - Server Operating System Installations
  - Services Offered by Servers
  - Descriptions of How a Server is Configured
    - Should Include Important Information
      - Hardware Configuration
      - OS Installed & Configuration
      - Network Configuration
      - Service Configurations
        - With Descriptions & Steps to Recreate
  - To Be Used in the Event of a System Failure

Systems Security Management

Eller / MIS

Documentation

System documentation is extremely important, yet it is one of the most despised tasks in IT. This is because system documentation, when done correctly, can be incredibly time consuming. Normally system documentation is used to document server operating system installations, the services offered by the server, and detailed descriptions of how the server is configured. This documentation should include every important piece of information including the hardware configuration, the OS installed and its configuration, the network configuration, and service configurations. Each piece should be described in detail with full steps to be used in order to recreate the system from scratch. This type of documentation is generally only used in the event of a massive system failure that backups cannot completely help a SysAdmin recover from.



Software Development Challenges

- Developing Software for an OS
  - Do you Develop for Windows? Linux? Mac OS X?
    - Depends on Need & Target Audience
  - Software (System) Development Life Cycle (SDLC)
    - Project Planning (Feasibility)
    - Requirements Definition
    - System Design
    - Implementation
    - Integration & Testing
    - Acceptance, Installation, Deployment
    - Maintenance
  - Secure Coding Initiatives

Systems Security Management

Eller / MIS

Software Development Challenges

When developing software for a specific Operating System, the developers will need to determine if the software needs to be developed for Windows, Linux, or Mac OS X systems. This will depend on the organization's need and the target audience for the software. When taking on a software development project, smart developers will make use of the software development life cycle (or SDLC). This is a project management tool designed to help guide a software development team through the different steps necessary when writing software. These steps include the following:

Project Planning (Feasibility) – This initial step is essentially the discovery phase of the project. This will involve meetings and interviews to determine user needs for the software and to determine if the project is feasible given any constraints on development.

Requirements Definition – Once the initial interview and information collection has completed, the lead project manager for the developers will need to write up a requirements definition. This is an overview of the system and what the users will require the system to do and output. This document should be signed off on by the stakeholders.

System Design – The system design phase is where the developers actually begin to write the software code and develop the initial user interface screens. This is where the OS that the developer is writing the software for comes into play. Each OS has a different semantic style: for example, Windows has the "minimize", "maximize" and "close" buttons in the upper right corner, whereas OS X has them in the upper left corner. The buttons also don't always function the same way between operating systems - when you click the "X" in Windows, the entire program usually exits; in OS X, it just closes the active window, while the main program remains running. These interface semantics need to be kept in mind and adhered to when creating a program for a specific OS. The stakeholders will usually be involved in this phase in order to ensure the system looks as expected.

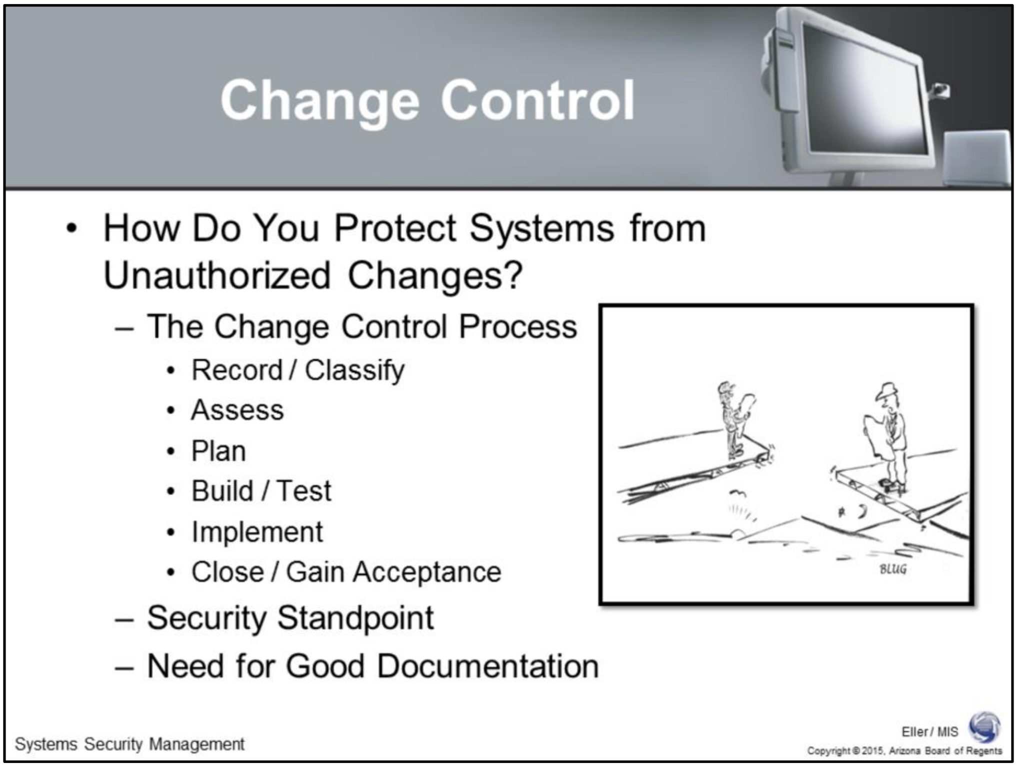
Implementation – During the implementation phase, the developers are doing the bulk of the internal code, writing the various functions that will take the user input and create the desired outputs.

Integration & Testing – The integration and testing phase will involve the stakeholders again. They will be trained on how the system works and will be used to help find bugs and other issues with the software.

Acceptance, Installation, Deployment – Once the software has gone through the testing phase and the stakeholders are happy with the results, the software will be deemed ready for use and will be installed and deployed to the users who need it.

Maintenance – Some may think the installation and deployment phase would be the end of the project; however, they would be wrong. The final phase is the maintenance phase, where developers work to fix any bugs that did not appear during the testing phase. This phase is also the longest phase of the project as the developers will be expected to continue supporting the software for as long as it is in use. This would include additional training and the occasional bug fix or feature modification. Note that if there are a large number of modifications to be made, this should be used to initiate a new project and not part of the continual maintenance.

In addition to the above steps, software developers should be using secure coding initiatives in order to ensure their software is not vulnerable to attacks from anyone looking to breach an organization's systems



Change Control

- How Do You Protect Systems from Unauthorized Changes?
  - The Change Control Process
    - Record / Classify
    - Assess
    - Plan
    - Build / Test
    - Implement
    - Close / Gain Acceptance
  - Security Standpoint
  - Need for Good Documentation

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

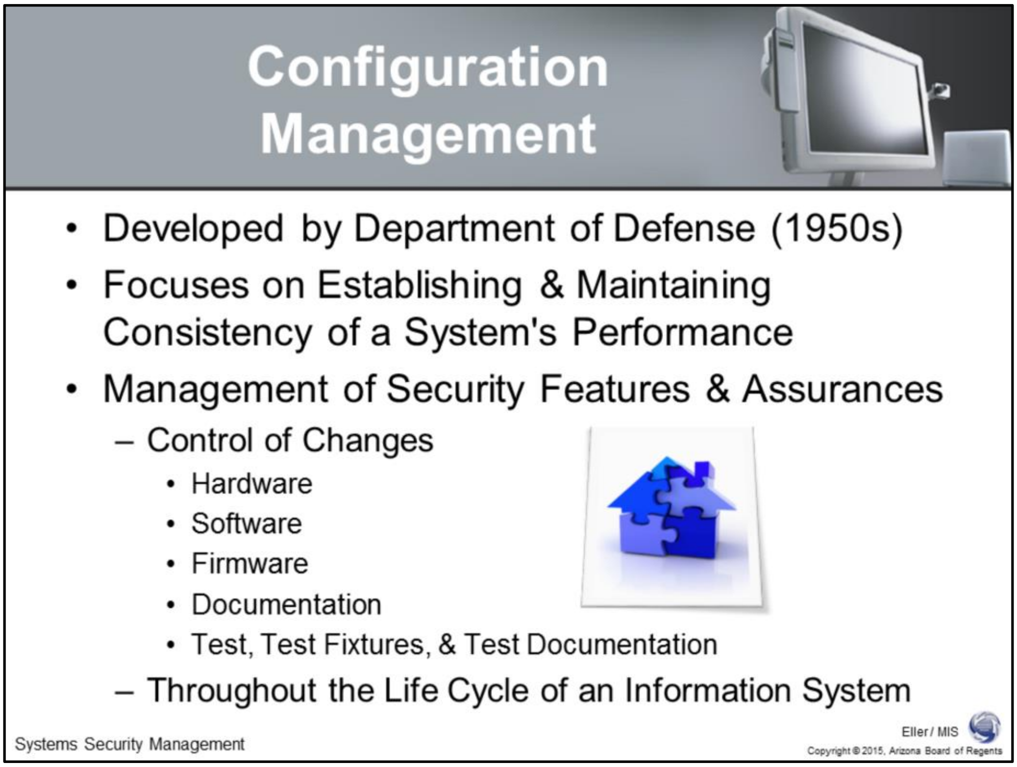
Change Control

Change controls are used to help protect systems from unauthorized changes. These are used for both systems and software development, and in many cases require documentation. The level of change control used is either dictated by the organization or the IT department responsible for making system or software changes.

In general, the change control process is a series of steps that mimic many of the steps of the SDLC. The process steps include the following:

Record / Classify – What is the change and why is it necessary?
Assess – Will the change have the expected effect and is it desirable?
Plan – How will the change be made?
Build / Test – Make the change and test the results of the change.
Implement – Make the change available to the users who needed the change.
Close / Gain Acceptance – Close out the change control process and get acceptance from the users that the change works as they expected.

From a security standpoint, change controls are an important piece in security design. This is because if the change had an undesired effect it can be reversed more easily with an official change control process than without. However, this will mean that good documentation is absolutely necessary to be able to reverse or recreate the change should a problem occur down the line.



Configuration Management

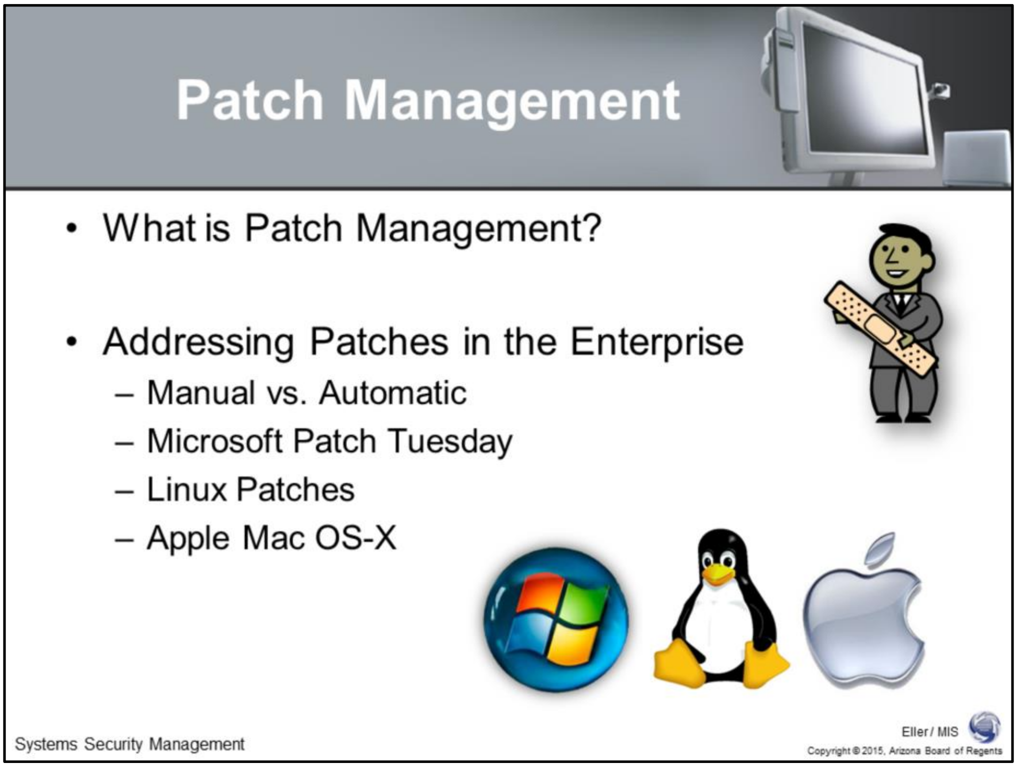
- Developed by Department of Defense (1950s)
- Focuses on Establishing & Maintaining Consistency of a System's Performance
- Management of Security Features & Assurances
  - Control of Changes
    - Hardware
    - Software
    - Firmware
    - Documentation
    - Test, Test Fixtures, & Test Documentation
  - Throughout the Life Cycle of an Information System

Systems Security Management

Eller / MIS

Configuration Management

Configuration management is a concept that was originally developed by the Department of Defense in the 1950s. It focuses on establishing and maintaining the consistency of a system's performance. In addition the concept was designed around the management of security features and assurances in a system and insists upon the use of change controls. Change controls are used to govern any changes to hardware, software, firmware, and documentation, including testing, test fixtures, and test documentation. The DoD's configuration management was expected to govern the entire life cycle of an information system.



Patch Management

- What is Patch Management?
- Addressing Patches in the Enterprise
  - Manual vs. Automatic
  - Microsoft Patch Tuesday
  - Linux Patches
  - Apple Mac OS-X

Systems Security Management

Eller / MIS

Patch Management

All operating systems require periodic updates to fix bugs or resolve security issues. While the pressure has been on Microsoft over the past decade with regard to the security of the Windows and Office platforms, all operating systems, including UNIX, Linux, and Apple's Mac OS X are no strangers to security patches. Because of this necessity, systems administrators have needed to find a way to manage the deployment of new patches, regardless of the operating system they are designed for. This is referred to as patch management, and over time, this has become a part of the systems administrator's responsibilities.

So, how do you address patch management within an enterprise environment?

There are a number of ways to address patch management. If you have a small number of computer systems to manage, manual patching is a reasonable solution; however, automating the patching process is often the most effective way to ensure the computers managed by the systems administrator are kept up-to-date. Automating the process can be done in a number of ways, depending on the operating system in use.

Microsoft Windows

The Microsoft Windows operating systems (from Windows XP/2003 and up) have a built-in automatic update client, which will look for new patches and can be configured in a few ways. By default, newer versions of the Windows OS (e.g. XP, Vista, Win7, Win8.1, and Servers 2003, 2008, and 2012) recommend automatic installation of patches at 3:00 am. Another option allows the user to opt to not install automatically, but notify them should new patches be available. The final option involves not installing patches at all, which indicates either the user does not want the computer patched (there are reasons why you might not want your computer patched) or they want to update manually.

To make the patching process easier on users and systems administrators, Microsoft introduced the concept of Patch Tuesday. Each month, Microsoft accumulates patches for all of its products, and once a month (on the second Tuesday of each month), Microsoft releases the new patches. Over the years there have been a few times where Microsoft has made the decision to release a patch "out-of-cycle." In this event, Microsoft is releasing a security patch to fix a specific security flaw (deemed to be critical) that is currently being exploited by attackers. The risk of not installing these patches out-of-cycle means your systems could be vulnerable to attack.

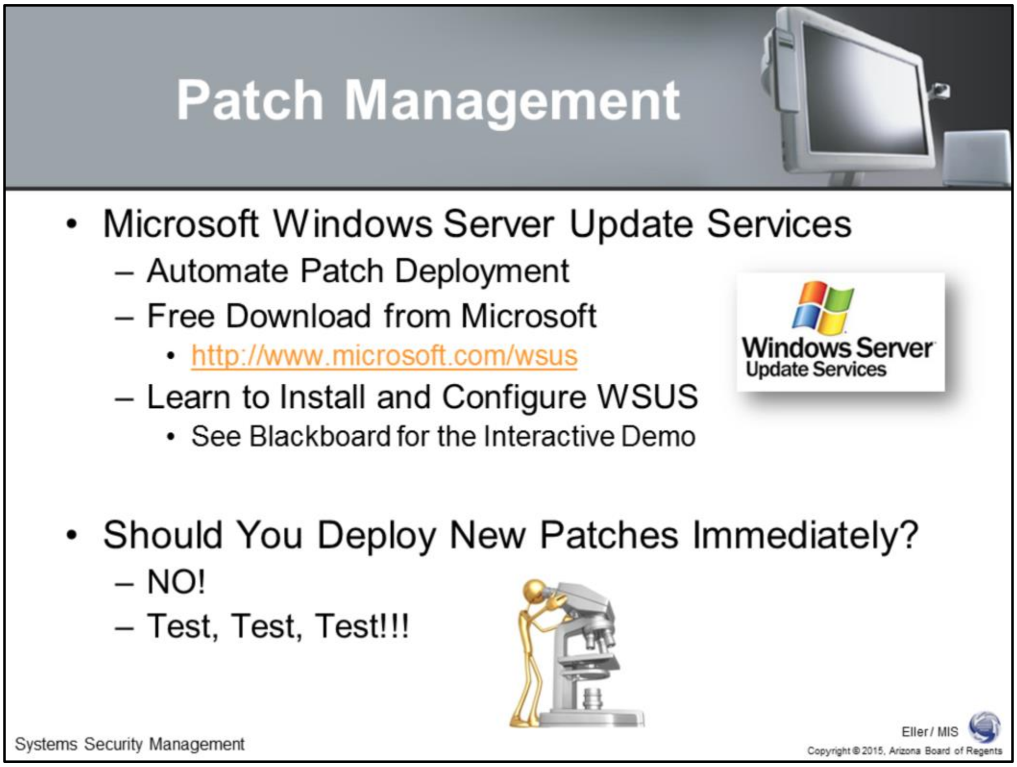
There are two different types of updates from Microsoft: Windows Updates and Microsoft Updates. Windows Updates are specifically designed for the various Windows operating systems. In general, this should be the minimum level of patching done within an enterprise. Microsoft Updates combine the updates for the Windows operating systems and add patches for all of Microsoft's other software packages, including Office, SQL, SharePoint, etc. In order to keep your systems completely up-to-date, Microsoft Update should be the preferred choice.

Linux

As an open source operating system with a multitude of variations and flavors, Linux also sees patches on a fairly regular basis; however, due to its open source nature, patches are released when they are finalized and not on any specific schedule. Most flavors of Linux support automatic updating based on a schedule of the user's choosing; however, this support generally only becomes available through custom scripting. Most Linux variants will notify users when updates are available for manual install.

Apple Mac OS X

Despite the long-standing belief that Apple's operating systems have no security problems, this is simply not true. As of September, 2014, Apple's Mac OS X was estimated to have a market share of approximately 9% of the desktop market, and malicious software is generally not developed for the Mac, because of this low market share. However, vulnerabilities still exist in platform-independent software packages like Java, Adobe, the BASH environment (terminal emulation), and various browsers (Javascript vulnerabilities being chief among these). Because of this, Apple has publically acknowledged security issues when they arise and provides updates to patch these problems. When a patch is necessary Apple works with the vendor to make the updates available, and the user has the same update options as available in Windows: automatically check for updates, download, install, and install system data files and security updates.


Windows Server
Update Services

Patch Management

- Microsoft Windows Server Update Services
  - Automate Patch Deployment
  - Free Download from Microsoft
    - http://www.microsoft.com/wsus
  - Learn to Install and Configure WSUS
    - See Blackboard for the Interactive Demo
- Should You Deploy New Patches Immediately?
  - NO!
  - Test, Test, Test!!!

Systems Security Management

Eller / MIS

Patch Management (continued)

What do you do when you have a large number of computer systems to patch?

In environments where manual patching or the need to configure each computer with the appropriate automatic update settings are unfeasible, the systems administrator will need to search for an enterprise-level solution to this problem. There are a number of third party solutions; however, Microsoft offers a free server solution to anyone who wishes to provide a centralized patch management solution. This product is called Microsoft Windows Server Update Services (WSUS) and is available on the Microsoft web site for download.

WSUS offers a number of features, including centralized management tools, reporting, and the ability to pick and choose the types of updates you wish to support in your organization. For example, if your company does not use Microsoft Exchange for e-mail, then there is no reason to configure your WSUS server to provide Exchange-related patches. These are options you select during the initial install and configuration of your server and can be changed at any time.

If you would like to learn how to install and configure Microsoft's Windows Server Update Services, check your Blackboard course for the interactive flash demo.

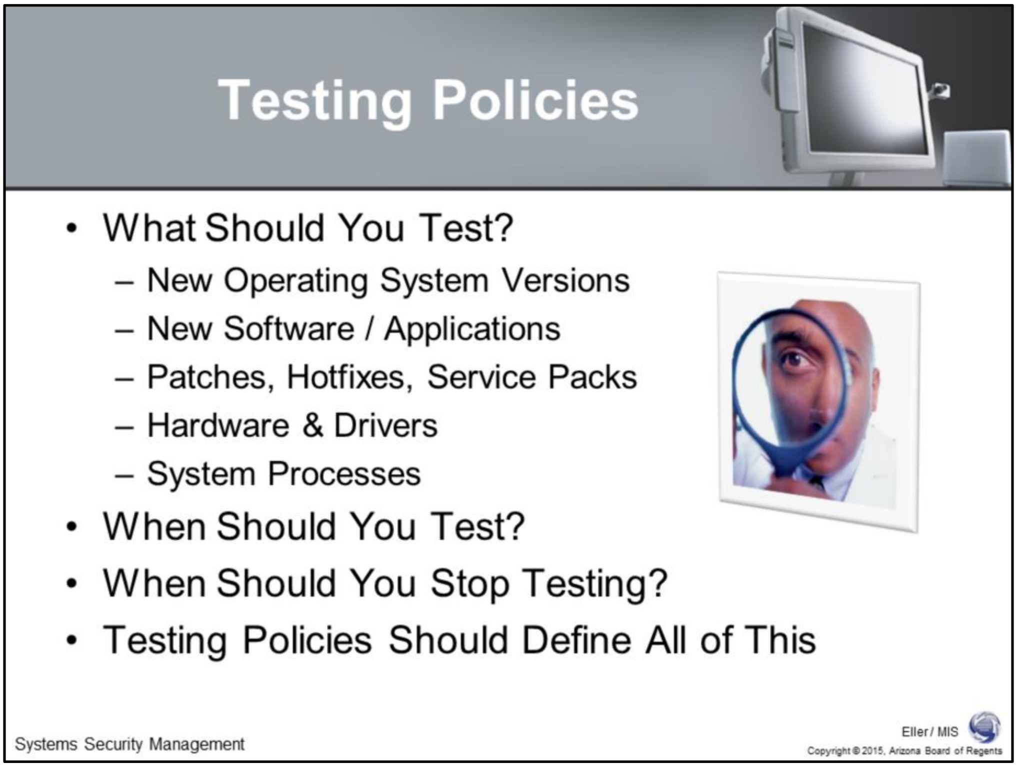
Should you deploy new patches immediately?

Absolutely not!

While it is considered good security to patch your computer systems when patches release, occasionally a patch will have an unintended side-effect on computers within your organization. The great part of Microsoft's WSUS server is that new updates will not be automatically approved for install when they become available, instead the system administrator must approve the patches for install within the organization. This ability gives the system administrator the flexibility to test the patches prior to making them available.

In order to support an enterprise, systems administrators need to act in the best interest of the organization, and occasionally this means not installing patches immediately. The systems administrator should be involved in the process of developing patch management policies within the organization in order to help keep the systems secure and ensure compatibility with existing applications.

Just remember: test, test, test!



Testing Policies

- What Should You Test?
  - New Operating System Versions
  - New Software / Applications
  - Patches, Hotfixes, Service Packs
  - Hardware & Drivers
  - System Processes
- When Should You Test?
- When Should You Stop Testing?
- Testing Policies Should Define All of This

Systems Security Management

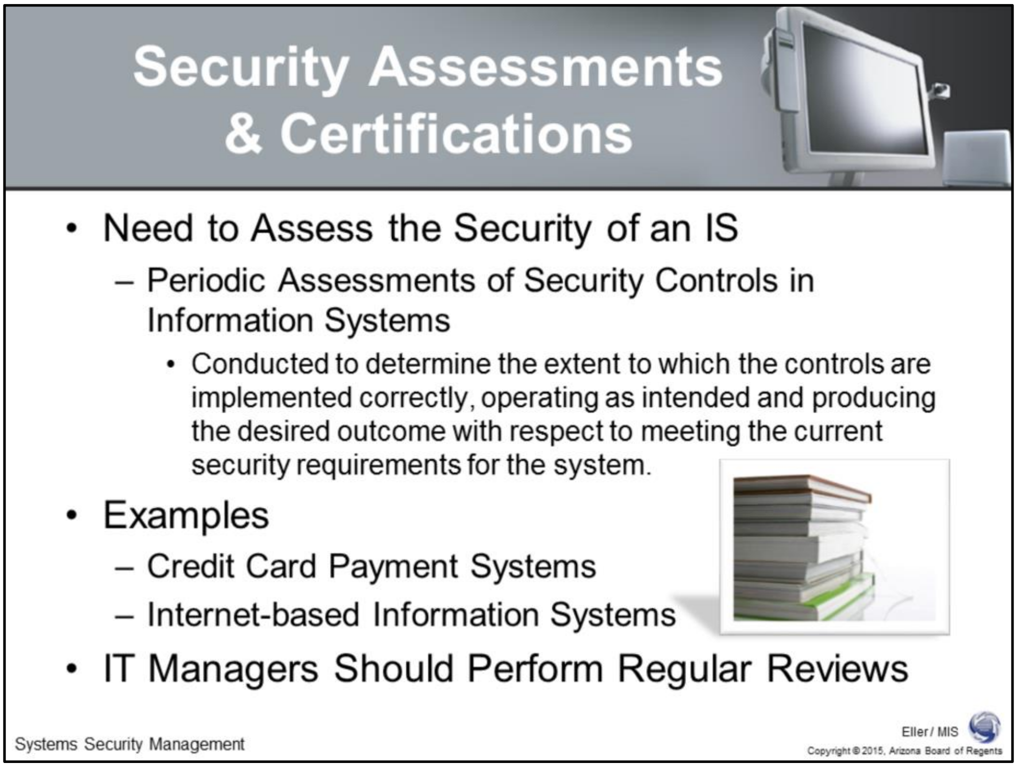
Eller / MIS

Testing Policies

Organizations should consider having an official IT testing policy in-place; however, what should be tested? Anything that will be new in the organization! This would include new operating system versions, new software or applications, new patches, hotfixes, or service packs, new hardware and drivers, and new system processes.

Testing should always begin as soon as is feasible for the organization. If there is no immediate need for deployment, this makes the testing process even easier as IT can take its time to learn more about what it is testing in order to gain a better understanding of its potential fit in the organization. Testing should only stop once IT is confident the system can be deployed without any major issues.

All of this should be defined in official testing policies; however, it is not always the case that an organization would have official policies governing the testing process. Perhaps it is time to develop and implement such a policy.



Security Assessments & Certifications

- Need to Assess the Security of an IS
  - Periodic Assessments of Security Controls in Information Systems
    - Conducted to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the current security requirements for the system.
- Examples
  - Credit Card Payment Systems
  - Internet-based Information Systems
- IT Managers Should Perform Regular Reviews

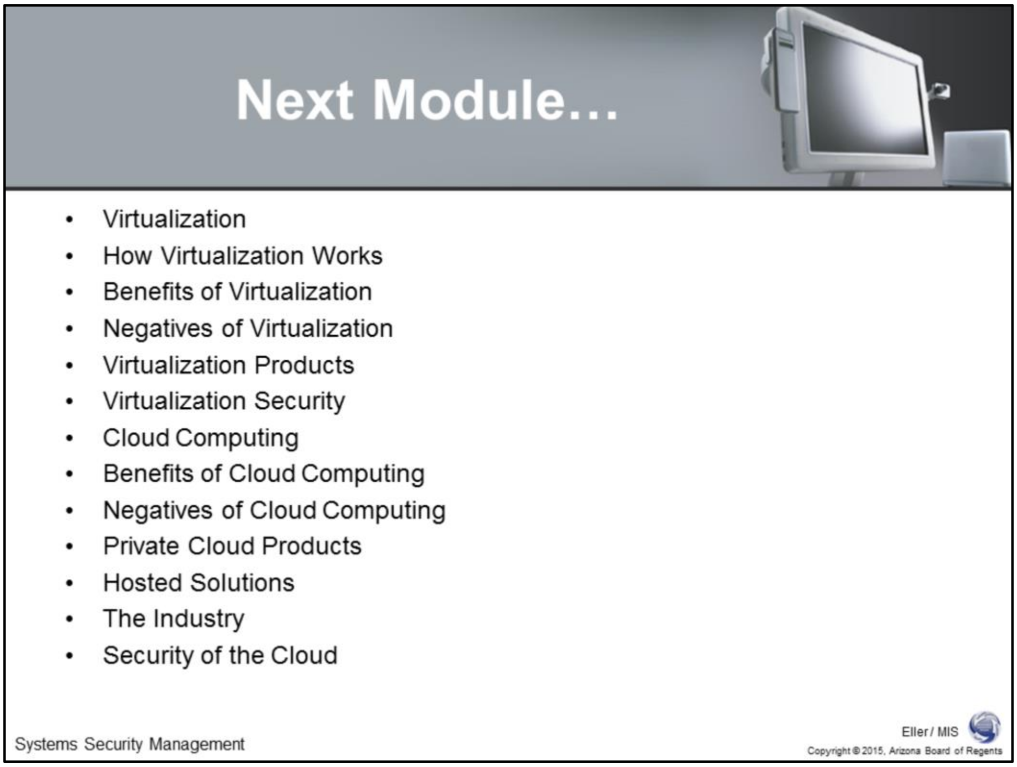
Systems Security Management

Eller / MIS

Security Assessments and Certifications

From time to time it will be necessary to assess the security of an information system. Periodic assessments of security controls in information systems should be conducted to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the current security requirements for the system.

Some examples of systems which will require periodic security assessments and certification include credit card payment systems and information systems that have a direct connection to the Internet. There is a real threat that these types of systems could be more easily breached than other types of systems. IT managers should be tasked with performing regular reviews of these systems to ensure security standards are met.



Next Module…

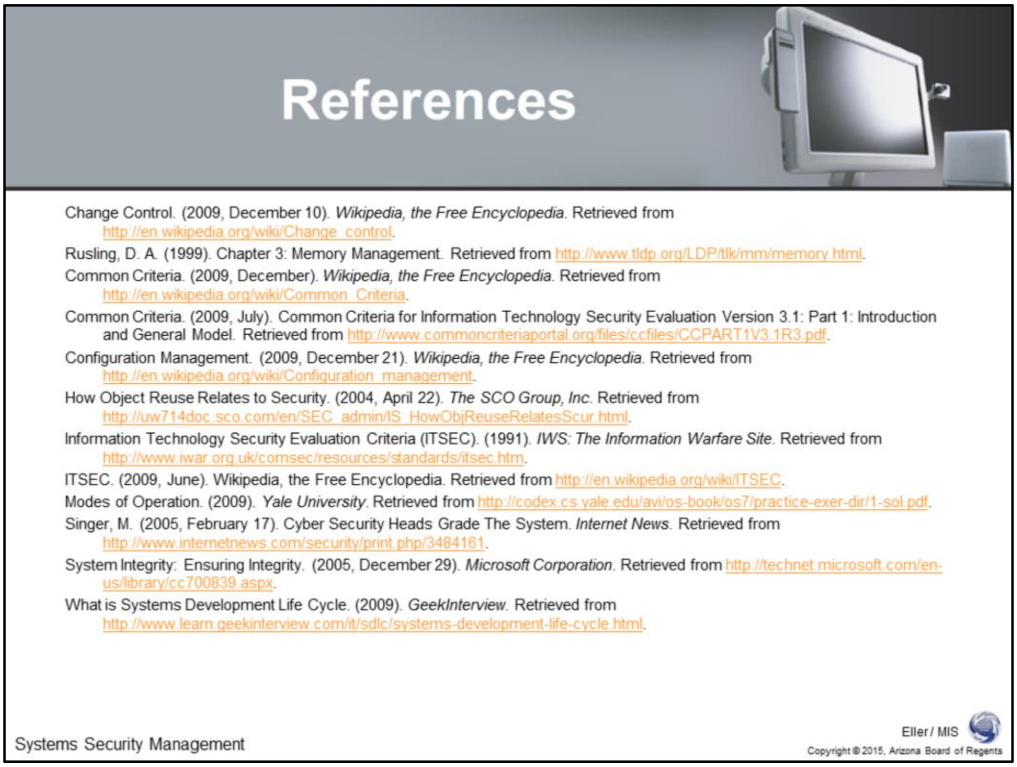
- Virtualization
- How Virtualization Works
- Benefits of Virtualization
- Negatives of Virtualization
- Virtualization Products
- Virtualization Security
- Cloud Computing
- Benefits of Cloud Computing
- Negatives of Cloud Computing
- Private Cloud Products
- Hosted Solutions
- The Industry
- Security of the Cloud

Systems Security Management

Eller / MIS

In the next module we will be discussing Virtualization and Cloud Computing, including:

- Virtualization
- How Virtualization Works
- Pros and Cons of Virtualization
- Virtualization Products & Security
- Cloud Computing
- Pros and Cons of Cloud Computing
- Private Cloud Products
- Hosted Solutions
- How The Industry Views Cloud Computing
- Security of the Cloud



References

Change Control. (2009, December 10). *Wikipedia, the Free Encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Change_control.

Rusling, D. A. (1999). Chapter 3: Memory Management. Retrieved from http://www.tldp.org/LDP/tlk/mm/memory.html.

Common Criteria. (2009, December). *Wikipedia, the Free Encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Common_Criteria.

Common Criteria. (2009, July). Common Criteria for Information Technology Security Evaluation Version 3.1: Part 1: Introduction and General Model. Retrieved from http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf.

Configuration Management. (2009, December 21). *Wikipedia, the Free Encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Configuration_management.

How Object Reuse Relates to Security. (2004, April 22). *The SCO Group, Inc*. Retrieved from http://uw714doc.sco.com/en/SEC_admin/IS_HowObjReuseRelatesScur.html.

Information Technology Security Evaluation Criteria (ITSEC). (1991). *IWS: The Information Warfare Site*. Retrieved from http://www.iwar.org.uk/comsec/resources/standards/itsec.htm.

ITSEC. (2009, June). Wikipedia, the Free Encyclopedia. Retrieved from http://en.wikipedia.org/wiki/ITSEC.

Modes of Operation. (2009). *Yale University*. Retrieved from http://codex.cs.yale.edu/avi/os-book/os7/practice-exer-dir/1-sol.pdf.

Singer, M. (2005, February 17). Cyber Security Heads Grade The System. *Internet News*. Retrieved from http://www.internetnews.com/security/print.php/3484161.

System Integrity: Ensuring Integrity. (2005, December 29). *Microsoft Corporation*. Retrieved from http://technet.microsoft.com/en-us/library/cc700839.aspx.

What is Systems Development Life Cycle. (2009). *GeekInterview*. Retrieved from http://www.learn.geekinterview.com/it/sdlc/systems-development-life-cycle.html.