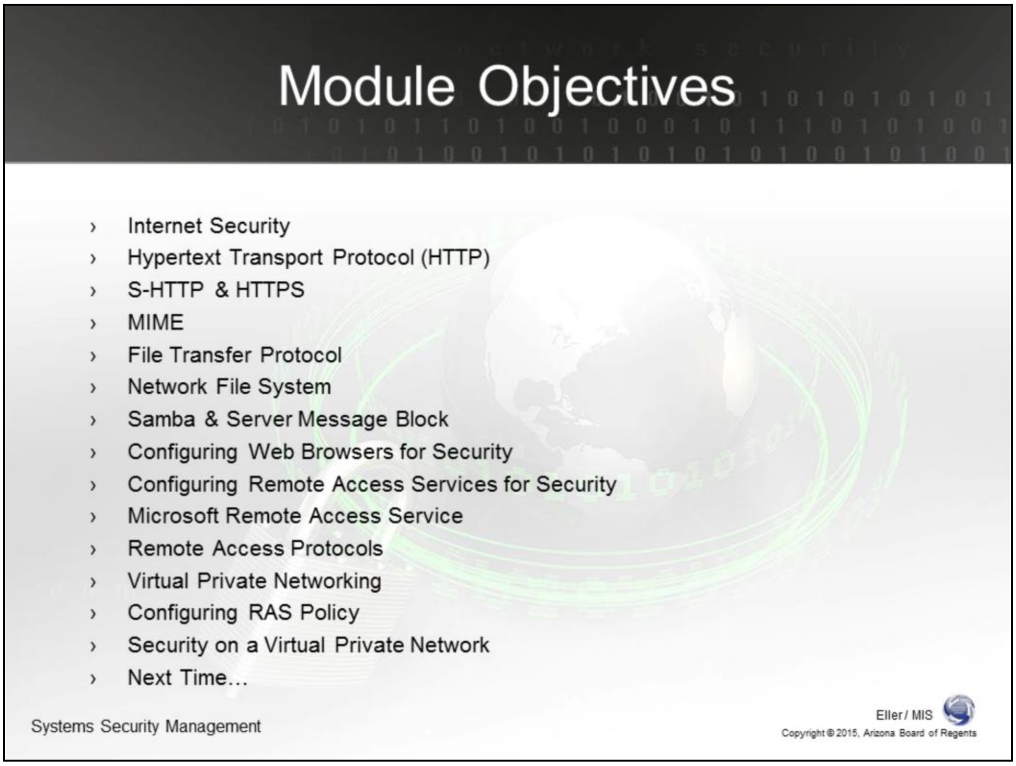
Web, Remote Access, & VPN Security

Module 15

Systems Security Management

Eller / MIS



Module Objectives

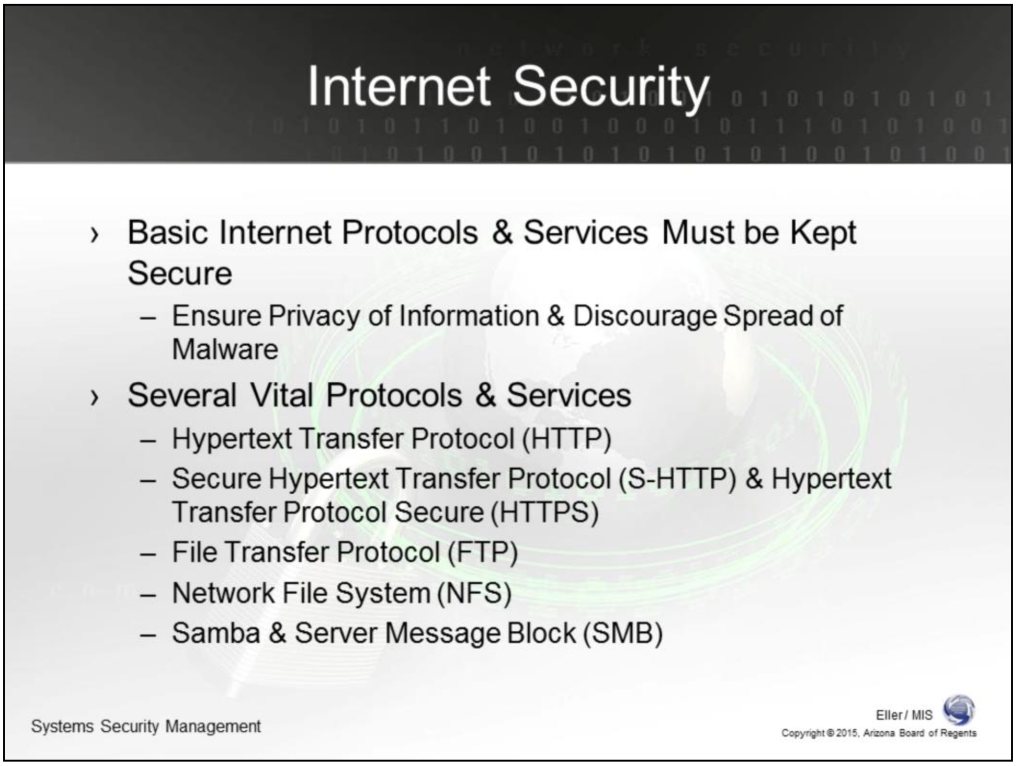
- Internet Security
- Hypertext Transport Protocol (HTTP)
- S-HTTP & HTTPS
- MIME
- File Transfer Protocol
- Network File System
- Samba & Server Message Block
- Configuring Web Browsers for Security
- Configuring Remote Access Services for Security
- Microsoft Remote Access Service
- Remote Access Protocols
- Virtual Private Networking
- Configuring RAS Policy
- Security on a Virtual Private Network
- Next Time…

Systems Security Management

Eller / MIS

At the end of the module, you should be able to:

- Understand the importance of Internet Security.
- Describe the protocols HTTP, S-HTTP, and HTTPS and understand how they differ.
- Understand the purposes for and differences between MIME and MOSS.
- Understand what the file transfer protocol is and why it is still in use.
- Describe how the network file system is used and secured.
- Understand how to secure your web browsers and remote access services for security.
- Describe each of the different remote access protocols, including virtual private networking.
- Understand how to configure a RAS policy and VPN security.



Internet Security

- Basic Internet Protocols & Services Must be Kept Secure
  - Ensure Privacy of Information & Discourage Spread of Malware
- Several Vital Protocols & Services
  - Hypertext Transfer Protocol (HTTP)
  - Secure Hypertext Transfer Protocol (S-HTTP) & Hypertext Transfer Protocol Secure (HTTPS)
  - File Transfer Protocol (FTP)
  - Network File System (NFS)
  - Samba & Server Message Block (SMB)

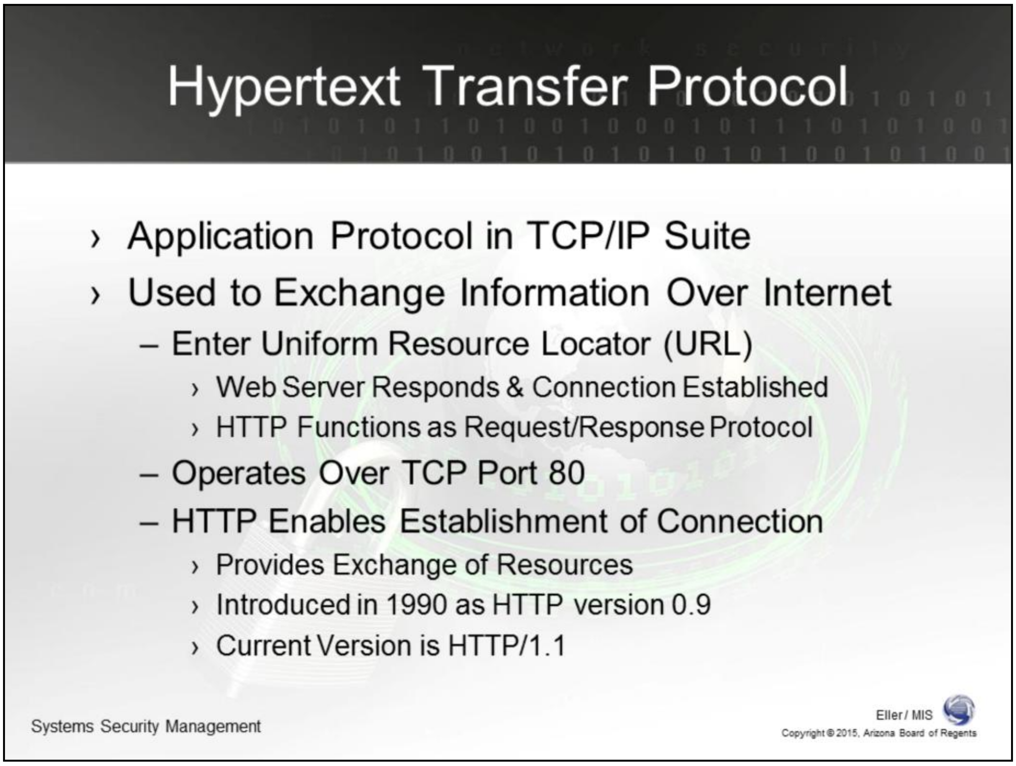
Systems Security Management

Eller / MIS

Internet Security

When it comes to the Internet, there are basic Internet Protocols and Services which must be kept secure in order to ensure the privacy of information and discourage the spread of malware. There are several vital protocols and services which need to be secured, including:

- Hypertext Transfer Protocol (HTTP)
- Secure Hypertext Transfer Protocol (S-HTTP) & Hypertext Transfer Protocol Secure (HTTPS)
- File Transfer Protocol (FTP)
- Network File System (NFS)
- Samba & Server Message Block (SMB)



Hypertext Transfer Protocol

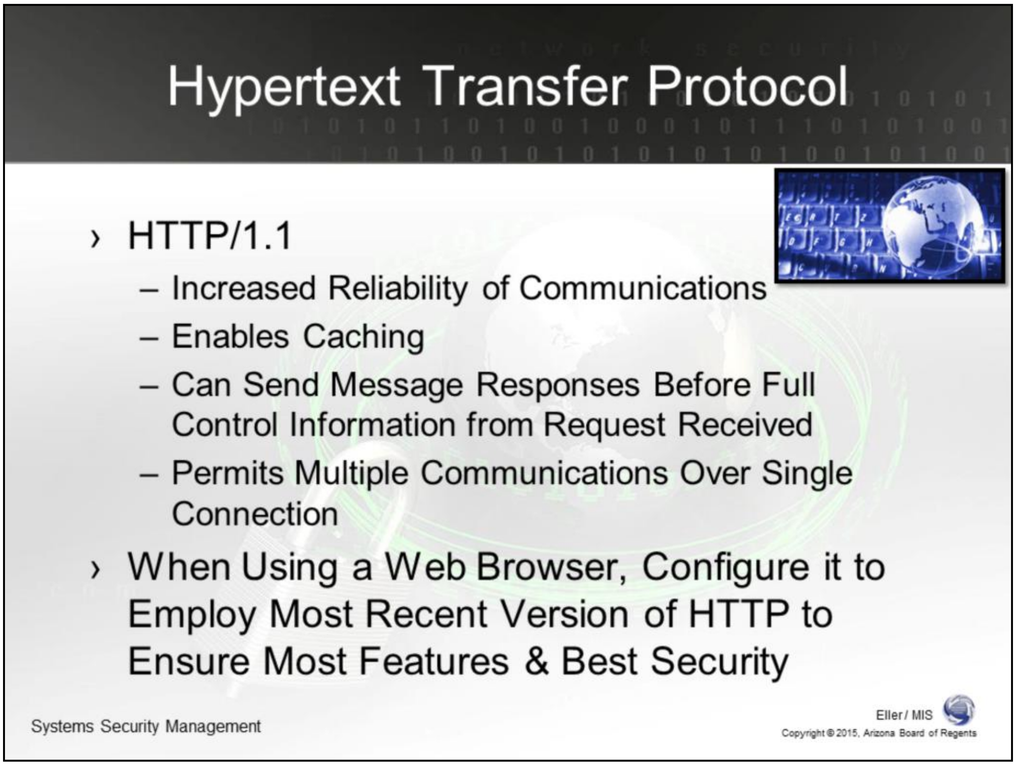
- Application Protocol in TCP/IP Suite
- Used to Exchange Information Over Internet
  - Enter Uniform Resource Locator (URL)
    - Web Server Responds & Connection Established
    - HTTP Functions as Request/Response Protocol
  - Operates Over TCP Port 80
  - HTTP Enables Establishment of Connection
    - Provides Exchange of Resources
    - Introduced in 1990 as HTTP version 0.9
    - Current Version is HTTP/1.1

Systems Security Management

Eller / MIS

Hypertext Transfer Protocol

The hypertext transfer protocol, or HTTP, is an application protocol in the TCP/IP suite and is used to exchange information over the Internet. A user will enter a Uniform Resource Locator, or URL, into a web browser in order to visit a web site. The web server will respond to the request and the connection will be established. HTTP functions as a request/response protocol, meaning communication with this protocol must be established by a system. HTTP uses TCP port 80 to establish communications with servers over the Internet. HTTP enables the establishment of a connection and provides for an exchange of resources. Originally introduced in 1990 as HTTP version 0.9, it has evolved over the past two decades into the current version, HTTP 1.1.



Hypertext Transfer Protocol

- HTTP/1.1
  - Increased Reliability of Communications
  - Enables Caching
  - Can Send Message Responses Before Full Control Information from Request Received
  - Permits Multiple Communications Over Single Connection
- When Using a Web Browser, Configure it to Employ Most Recent Version of HTTP to Ensure Most Features & Best Security

Systems Security Management

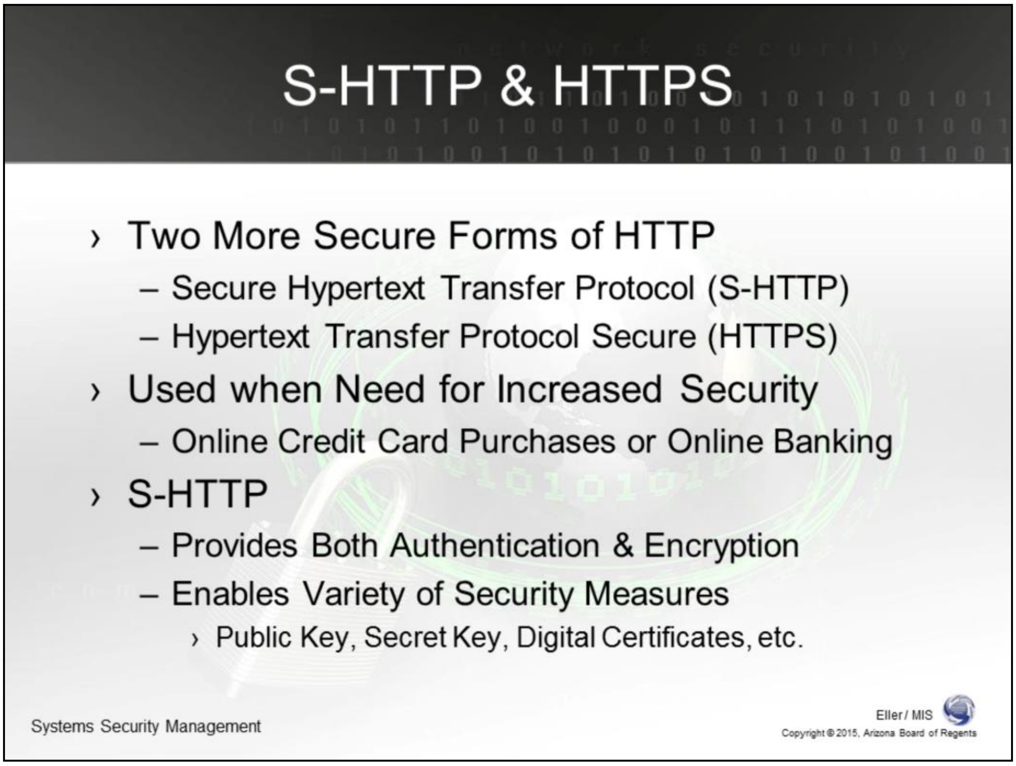
Eller / MIS

Hypertext Transfer Protocol (continued)

HTTP version 1.1 provides a number of improvements for effective communication over the Internet, including:

- Increased Reliability of Communications
- Enables Caching
- Can Send Message Responses Before Full Control Information from Request Received
- Permits Multiple Communications Over Single Connection

When you use a web browser, make certain it is configured to use the most recent version of HTTP, in order to enable as many features as possible and implement the best security options.



S-HTTP & HTTPS

- Two More Secure Forms of HTTP
  - Secure Hypertext Transfer Protocol (S-HTTP)
  - Hypertext Transfer Protocol Secure (HTTPS)
- Used when Need for Increased Security
  - Online Credit Card Purchases or Online Banking
- S-HTTP
  - Provides Both Authentication & Encryption
  - Enables Variety of Security Measures
    - Public Key, Secret Key, Digital Certificates, etc.

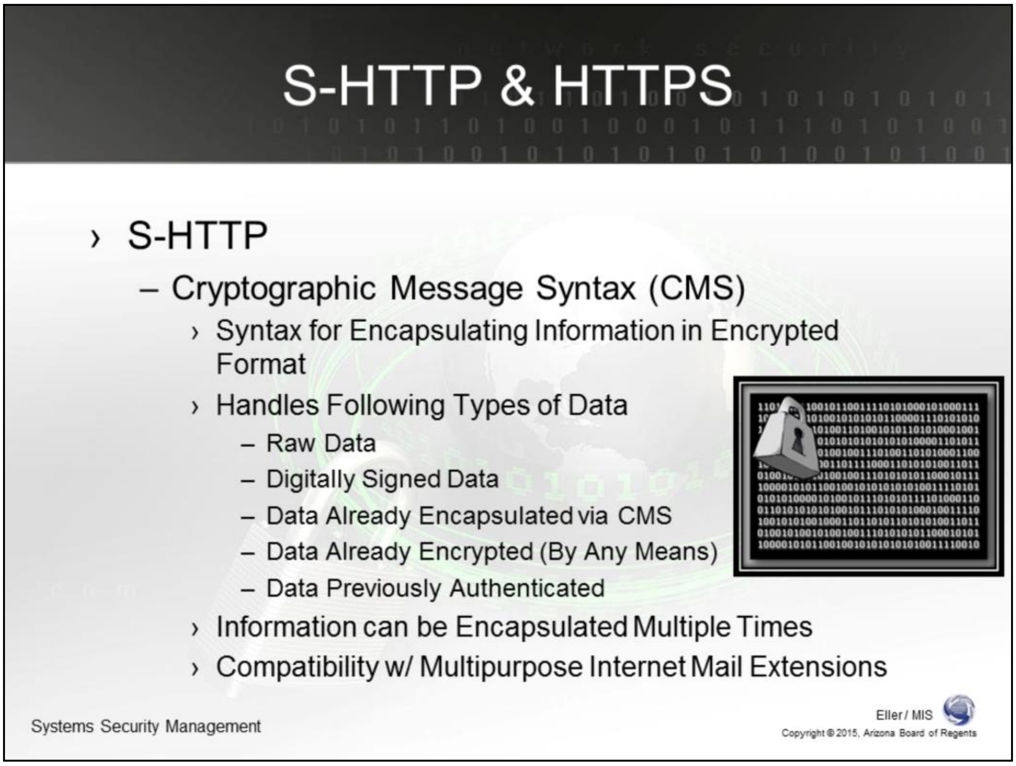
Systems Security Management

Eller / MIS

S-HTTP and HTTPS

While HTTP provides a mechanism to transmit and receive data over the Internet, the protocol does this through insecure methods. There are, however, two more secure forms of HTTP: the Secure Hypertext Transfer Protocol (S-HTTP) and the Hypertext Transfer Protocol Secure (HTTPS). These two protocols are typically used when there is a need for increased security, such as for online credit card purchases or online banking.

S-HTTP provides both encryption and authentication as well as enabling a variety of security measures including: public key, secret key, and digital certificates, among others.



S-HTTP & HTTPS

- S-HTTP
  - Cryptographic Message Syntax (CMS)
    - Syntax for Encapsulating Information in Encrypted Format
    - Handles Following Types of Data
      - Raw Data
      - Digitally Signed Data
      - Data Already Encapsulated via CMS
      - Data Already Encrypted (By Any Means)
      - Data Previously Authenticated
    - Information can be Encapsulated Multiple Times
    - Compatibility w/ Multipurpose Internet Mail Extensions

Systems Security Management

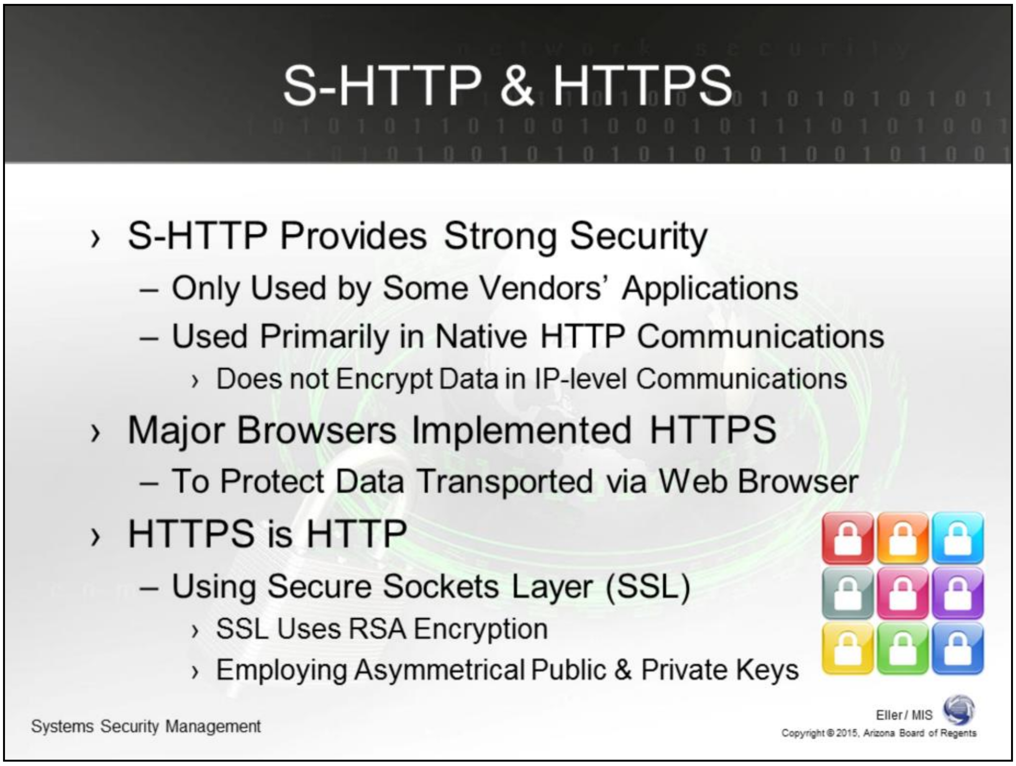
Eller / MIS

S-HTTP and HTTPS (continued)

S-HTTP uses the cryptographic message syntax, or CMS, which is a syntax for encapsulating information in an encrypted format. S-HTTP handles the following types of data:

- Raw Data
- Digitally Signed Data
- Data Already Encapsulated via CMS
- Data Already Encrypted (By Any Means)
- Data Previously Authenticated

In addition, information transmitted using S-HTTP can be encapsulated multiple times for increased security, and is compatible with the Multipurpose Internet Mail Extensions.



S-HTTP & HTTPS

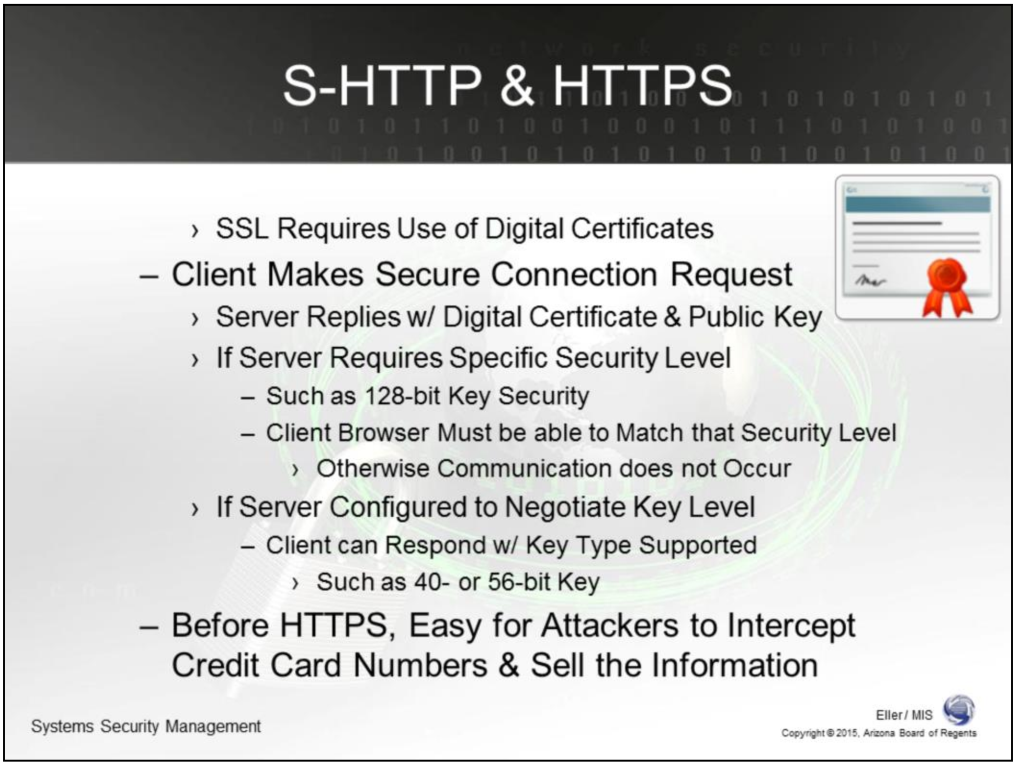
- S-HTTP Provides Strong Security
  - Only Used by Some Vendors' Applications
  - Used Primarily in Native HTTP Communications
    - Does not Encrypt Data in IP-level Communications
- Major Browsers Implemented HTTPS
  - To Protect Data Transported via Web Browser
- HTTPS is HTTP
  - Using Secure Sockets Layer (SSL)
    - SSL Uses RSA Encryption
    - Employing Asymmetrical Public & Private Keys

Systems Security Management

Eller / MIS

S-HTTP and HTTPS (continued)

S-HTTP provides strong security; however, it is only used by some vendors' applications. It is also used primarily in native HTTP communications, which does not encrypt data in IP-level communications. On the other hand, all major web browsers have implemented HTTPS instead in order to protect the data transported via web browser. HTTPS ***is*** HTTP, it simply added secure sockets layer, or SSL, security with RSA encryption. This means it employs asymmetrical public and private keys for encrypting data communications.



S-HTTP & HTTPS

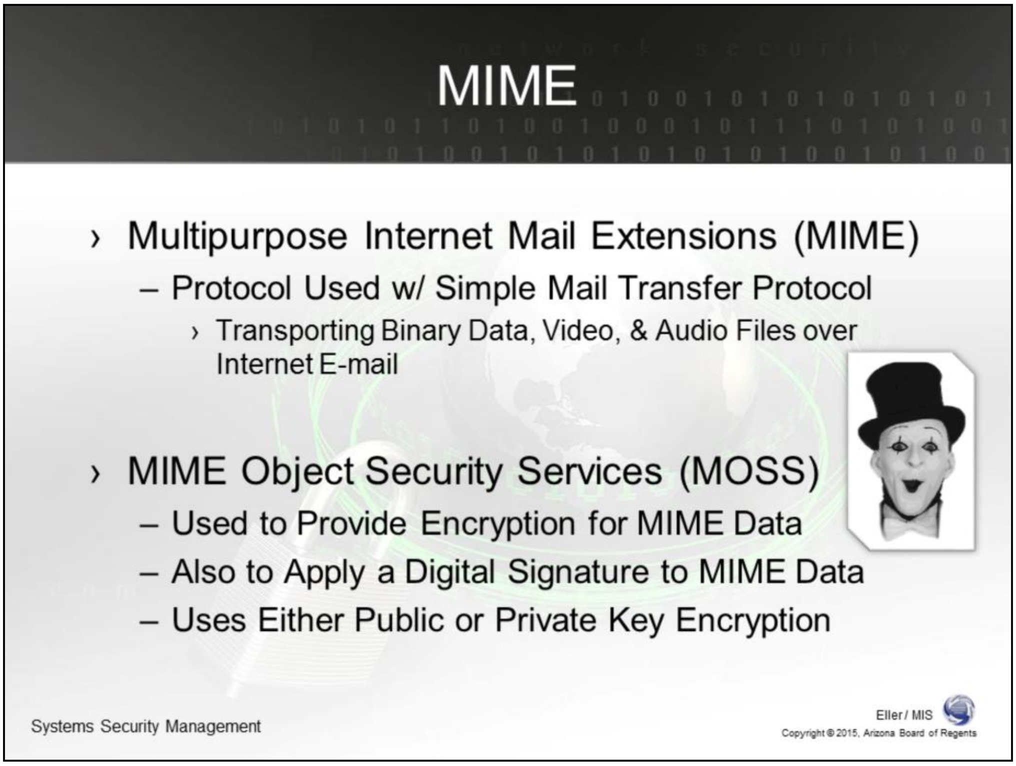
- › SSL Requires Use of Digital Certificates
- – Client Makes Secure Connection Request
  - › Server Replies w/ Digital Certificate & Public Key
  - › If Server Requires Specific Security Level
    - – Such as 128-bit Key Security
    - – Client Browser Must be able to Match that Security Level
      - › Otherwise Communication does not Occur
  - › If Server Configured to Negotiate Key Level
    - – Client can Respond w/ Key Type Supported
      - › Such as 40- or 56-bit Key
- – Before HTTPS, Easy for Attackers to Intercept Credit Card Numbers & Sell the Information

Systems Security Management

Eller / MIS

S-HTTP and HTTPS (continued)

HTTPS using SSL also requires the use of digital certificates to validate the data transmitted. With HTTPS, the client will make a secure connection request. The server then responds with a digital certificate and a public key. If the server responds to the client with a specific security level, such as 128-bit key security, the client web browser must be able to match the security level, otherwise communication will not occur. If the server is configured to negotiate the key level, the client can respond with the key type supported, such as 40-bit or 56-bit key encryption. Before HTTPS, it was very easy for attackers to intercept credit card numbers and sell the information.



MIME

- Multipurpose Internet Mail Extensions (MIME)
  - Protocol Used w/ Simple Mail Transfer Protocol
    - Transporting Binary Data, Video, & Audio Files over Internet E-mail
- MIME Object Security Services (MOSS)
  - Used to Provide Encryption for MIME Data
  - Also to Apply a Digital Signature to MIME Data
  - Uses Either Public or Private Key Encryption

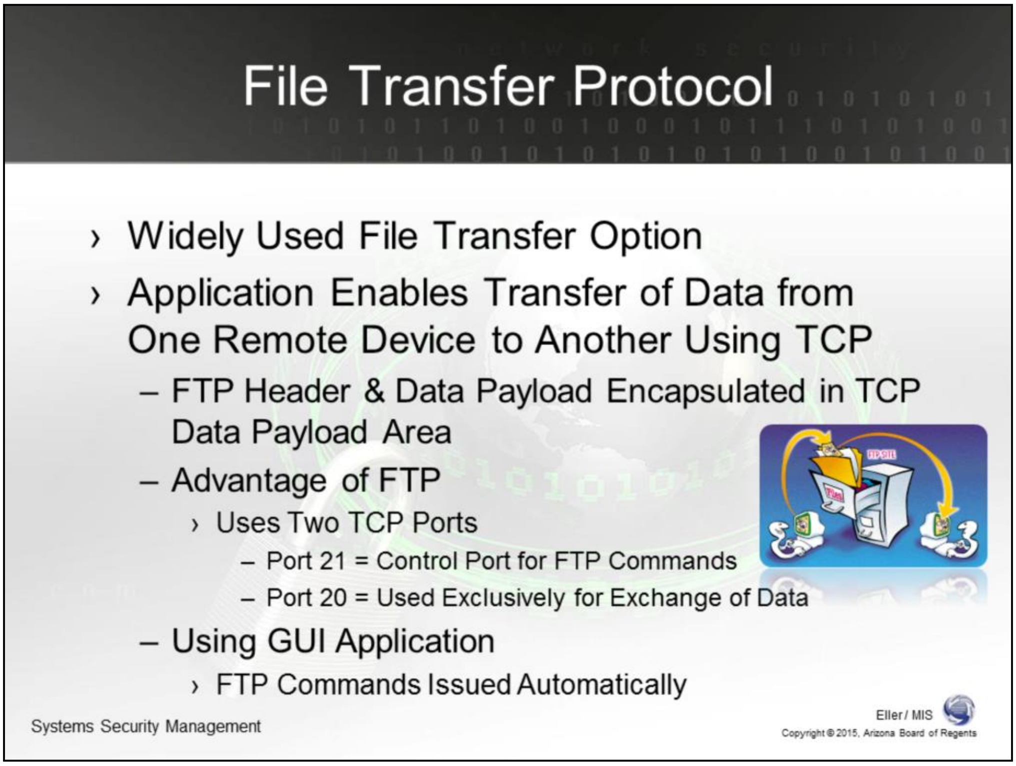
Systems Security Management

Eller / MIS

MIME

Multipurpose Internet Mail Extensions, or MIME, is a protocol that is used in conjunction with the Simple Mail Transfer Protocol, or SMTP, for transporting binary data, video, and audio files over Internet e-mail. We will be discussing MIME in more detail in Module 16.

In order to secure MIME data during transmission, the MIME Object Security Services, or MOSS, was developed. MOSS is used to provide encryption for MIME data and to apply a digital signature to MIME data using either public or private key encryption.



File Transfer Protocol

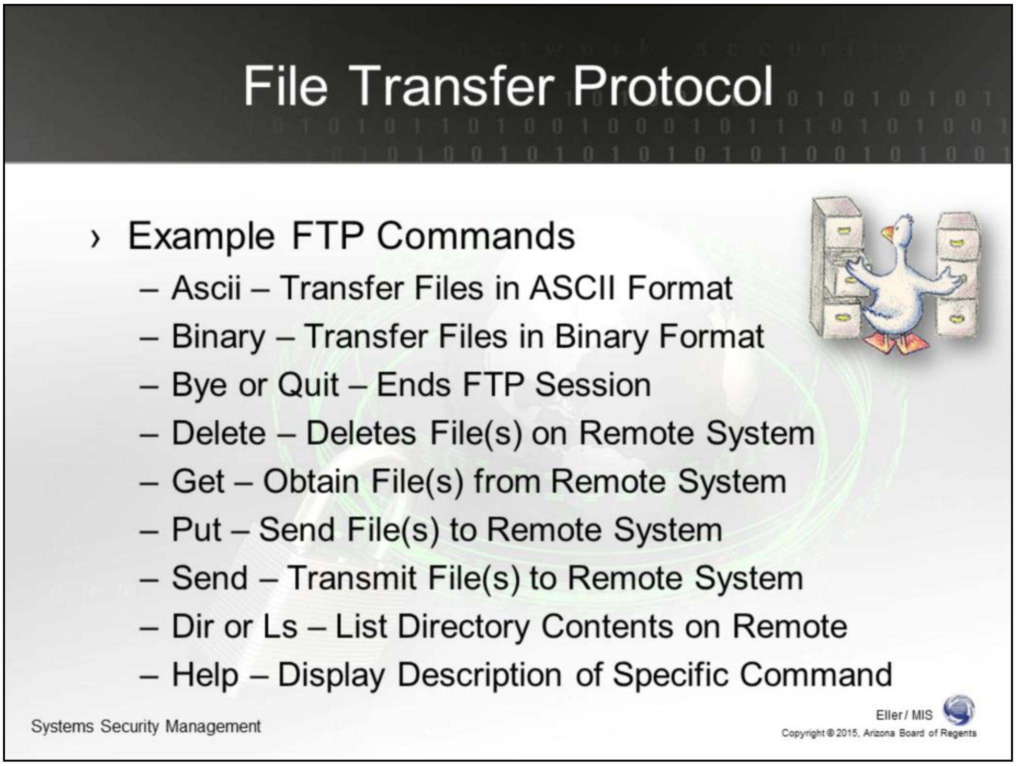
- Widely Used File Transfer Option
- Application Enables Transfer of Data from One Remote Device to Another Using TCP
  - FTP Header & Data Payload Encapsulated in TCP Data Payload Area
  - Advantage of FTP
    - Uses Two TCP Ports
      - Port 21 = Control Port for FTP Commands
      - Port 20 = Used Exclusively for Exchange of Data
  - Using GUI Application
    - FTP Commands Issued Automatically

Systems Security Management

Eller / MIS

File Transfer Protocol

The file transfer protocol, or FTP, is one of the most widely used file transfer options. FTP applications enable the transfer of data from one remote device to another using TCP. The FTP header and data payload are encapsulated in the TCP data payload area. The advantage of FTP is in its use of two TCP ports: 20 and 21. TCP port 21 is used as a control port for FTP communications while TCP port 20 is used exclusively for the exchange of data. When using an FTP application in a graphical user interface, any FTP commands are issued automatically by the application.



File Transfer Protocol

- Example FTP Commands
  - Ascii – Transfer Files in ASCII Format
  - Binary – Transfer Files in Binary Format
  - Bye or Quit – Ends FTP Session
  - Delete – Deletes File(s) on Remote System
  - Get – Obtain File(s) from Remote System
  - Put – Send File(s) to Remote System
  - Send – Transmit File(s) to Remote System
  - Dir or Ls – List Directory Contents on Remote
  - Help – Display Description of Specific Command

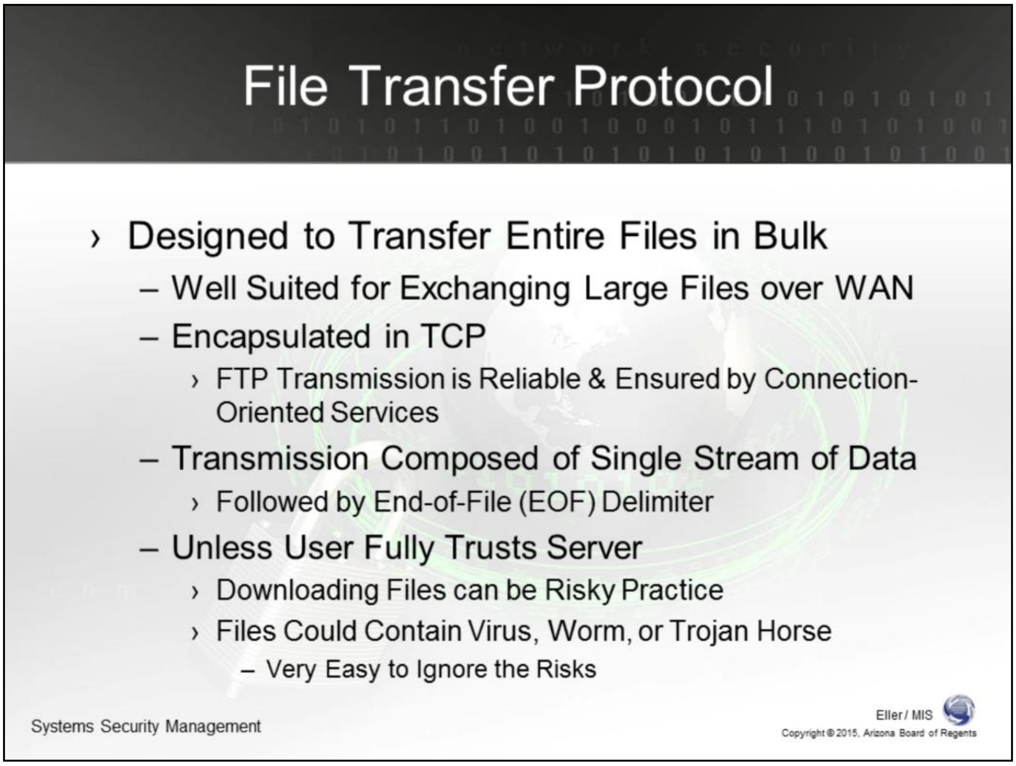
Systems Security Management

Eller / MIS

File Transfer Protocol (continued)

Some examples of FTP commands include:

- Ascii – Transfer Files in ASCII Format
- Binary – Transfer Files in Binary Format
- Bye or Quit – Ends FTP Session
- Delete – Deletes File(s) on Remote System
- Get – Obtain File(s) from Remote System
- Put – Send File(s) to Remote System
- Send – Transmit File(s) to Remote System
- Dir or Ls – List Directory Contents on Remote
- Help – Display Description of Specific Command



File Transfer Protocol

- Designed to Transfer Entire Files in Bulk
  - Well Suited for Exchanging Large Files over WAN
  - Encapsulated in TCP
    - FTP Transmission is Reliable & Ensured by Connection-Oriented Services
  - Transmission Composed of Single Stream of Data
    - Followed by End-of-File (EOF) Delimiter
  - Unless User Fully Trusts Server
    - Downloading Files can be Risky Practice
    - Files Could Contain Virus, Worm, or Trojan Horse
      - Very Easy to Ignore the Risks

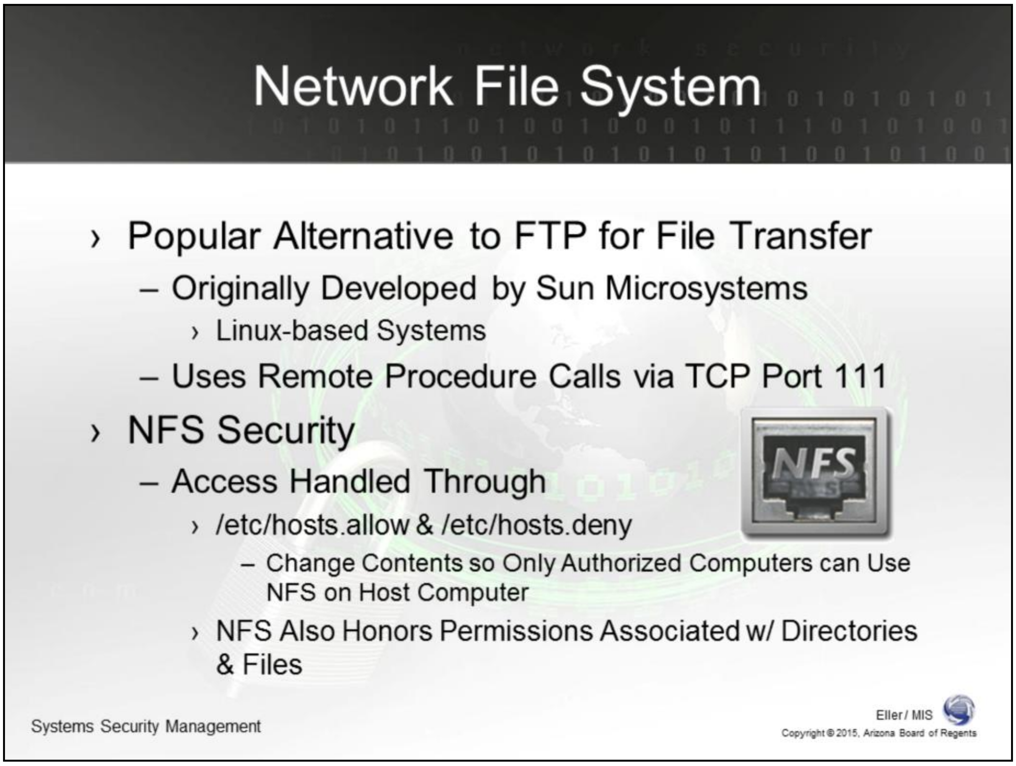
Systems Security Management

Eller / MIS

File Transfer Protocol (continued)

FTP is designed to transfer entire files in bulk, which makes it uniquely suited for exchanging large files over a WAN connection. As previously mentioned, FTP data is encapsulated in TCP packets, so any FTP transmissions are reliable and ensured by connection-oriented services. FTP transmission is comprised of a single stream of data followed by an end-of-file (EOF) delimiter. Something to keep in mind, however, is unless the user fully trusts the server, downloading files from an FTP server can be a risky practice. These files could contain a virus, worm, or Trojan horse, and it can be very easy to ignore the risks.

One thing to be aware of with FTP is that there is no encryption whatsoever. This means that usernames and passwords are transmitted in plaintext on the wire. Anyone tapped into the network will have that information as soon as you use FTP to transfer a file. However, it’s not just the username and password, everything you send over FTP is unencrypted. There are alternatives: Secure FTP (SFTP) is encrypted and sends traffic over port 22 (which, you may remember, is the same port used for Secure Shell (SSH) communications). Another option to secure FTP transfers is an extension called FTPS, also known as FTP-SSL and FTP Secure, which adds support for TLS and SSL, think HTTPS for FTP.



Network File System

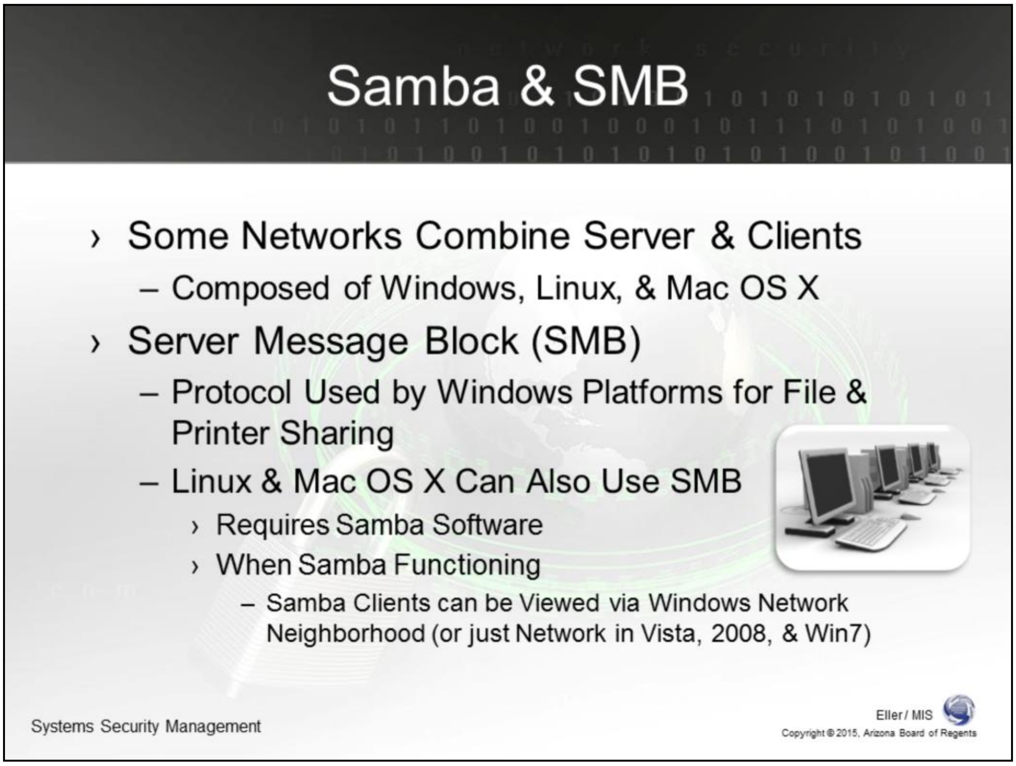
- › Popular Alternative to FTP for File Transfer
  - – Originally Developed by Sun Microsystems
    - › Linux-based Systems
  - – Uses Remote Procedure Calls via TCP Port 111
- › NFS Security
  - – Access Handled Through
    - › /etc/hosts.allow & /etc/hosts.deny
      - – Change Contents so Only Authorized Computers can Use NFS on Host Computer
    - › NFS Also Honors Permissions Associated w/ Directories & Files

Systems Security Management

Eller / MIS

Network File System

The Network File System, or NFS, is a popular alternative to FTP for file transfer. NFS was originally developed by Sun Microsystems for Linux-based systems. NFS uses remote procedure calls via TCP port 111 for transferring files. Security for NFS is handled through the /etc/hosts.allow and /etc/hosts.deny files. The contents of these files can be changed so only authorized computers can use NFS on the host computer. NFS also respects the security permissions that are associated with both directories and files.



Samba & SMB

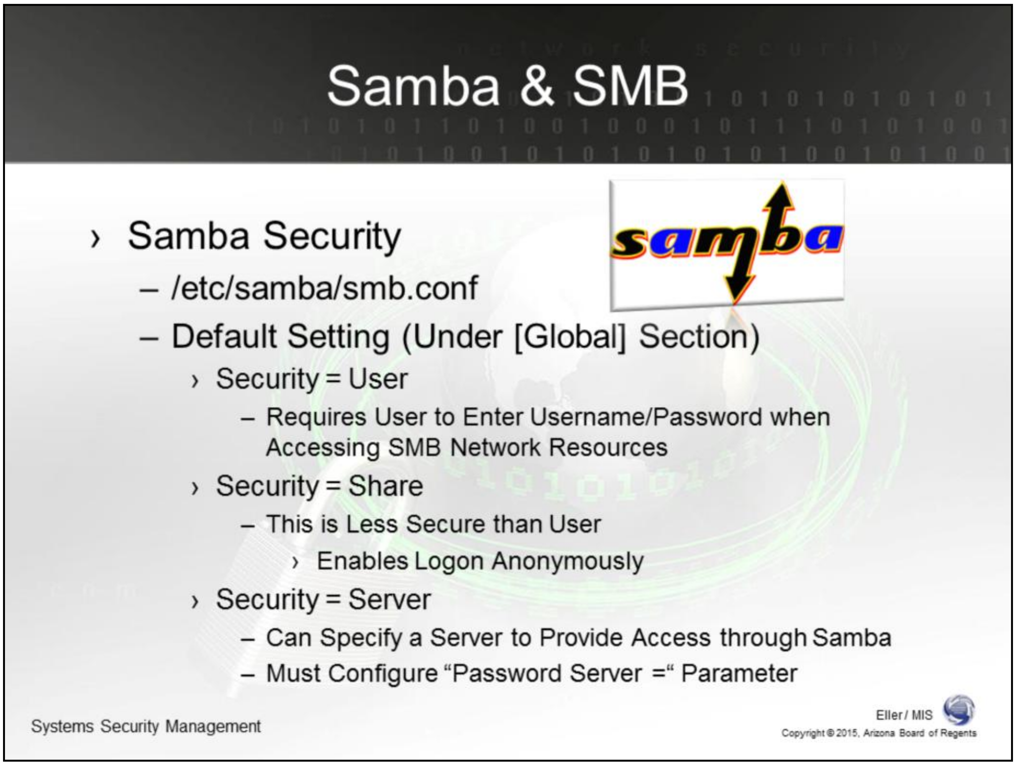
- Some Networks Combine Server & Clients
  - Composed of Windows, Linux, & Mac OS X
- Server Message Block (SMB)
  - Protocol Used by Windows Platforms for File & Printer Sharing
  - Linux & Mac OS X Can Also Use SMB
    - Requires Samba Software
    - When Samba Functioning
      - Samba Clients can be Viewed via Windows Network Neighborhood (or just Network in Vista, 2008, & Win7)

Systems Security Management

Eller / MIS

Samba and SMB

Some organization’s use networks that combine different servers and client systems composed of Windows, Linux, and Mac OS X. The Server Message Block, or SMB, protocol is used by Windows platforms for file and printer sharing services. Both the Linux and Mac OS X platforms can also make use of SMB; however, this requires installing and configuring the Samba software. When Samba is functioning properly, Linux and Mac clients can be viewed on the Windows Network.



Samba & SMB

- Samba Security
  - /etc/samba/smb.conf
  - Default Setting (Under [Global] Section)
    - Security = User
      - Requires User to Enter Username/Password when Accessing SMB Network Resources
    - Security = Share
      - This is Less Secure than User
        - Enables Logon Anonymously
    - Security = Server
      - Can Specify a Server to Provide Access through Samba
      - Must Configure “Password Server =“ Parameter

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

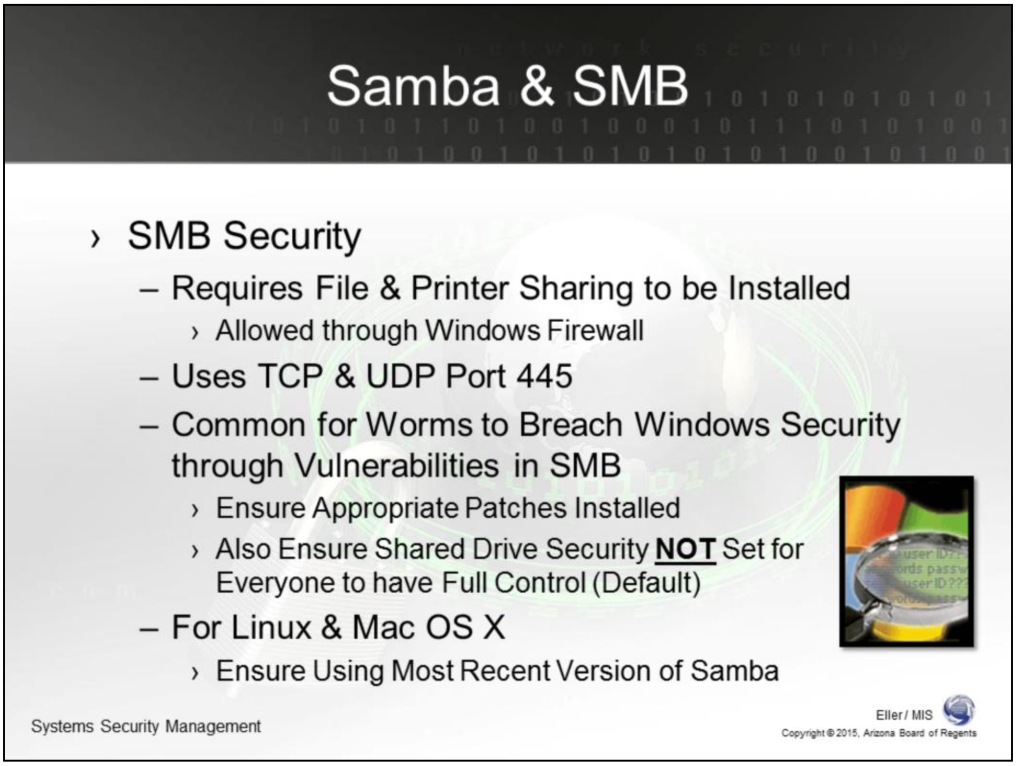
Samba and SMB (continued)

Samba security is configured in the file /etc/samba/smb.conf. The default settings are located under the [Global] section of the file. Possible settings include:

Security = User – Requires User to Enter Username/Password when Accessing SMB Network Resources

Security = Share – This is Less Secure than User, and Enables Logon Anonymously

Security = Server – Can Specify a Server to Provide Access through Samba and Must Configure “Password Server =“ Parameter



Samba & SMB

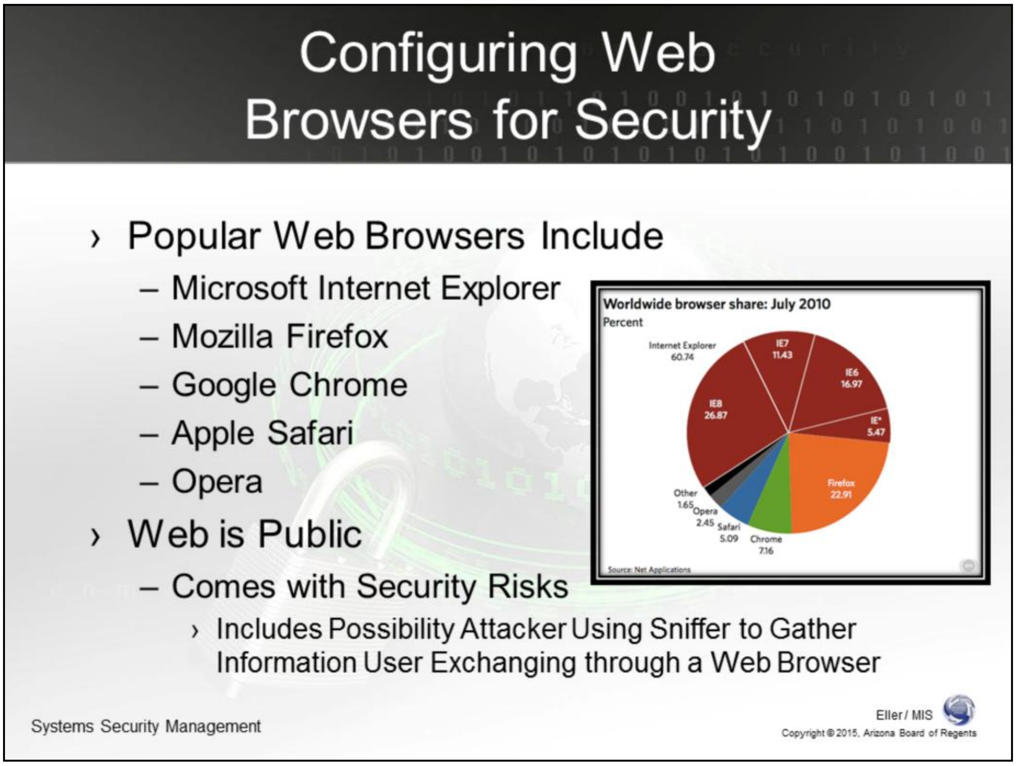
- SMB Security
  - Requires File & Printer Sharing to be Installed
    - Allowed through Windows Firewall
  - Uses TCP & UDP Port 445
  - Common for Worms to Breach Windows Security through Vulnerabilities in SMB
    - Ensure Appropriate Patches Installed
    - Also Ensure Shared Drive Security **NOT** Set for Everyone to have Full Control (Default)
  - For Linux & Mac OS X
    - Ensure Using Most Recent Version of Samba

Systems Security Management

Eller / MIS

Samba and SMB (continued)

SMB security on a Windows server requires that File and Printer Sharing is installed and allowed through the Windows Firewall. SMB uses TCP and UDP port 445 for communications, and because it uses these well known ports, it is common for worms to breach Windows security through vulnerabilities in the SMB protocol. So, it is very important that servers are patched regularly and that shared drive security is ***NOT*** set to allow everyone to have full control, which is the default Windows behavior. With Linux and Mac OS X, just make certain you have installed the most recent version of Samba.



Configuring Web Browsers for Security

- Popular Web Browsers Include
  - Microsoft Internet Explorer
  - Mozilla Firefox
  - Google Chrome
  - Apple Safari
  - Opera
- Web is Public
  - Comes with Security Risks
    - Includes Possibility Attacker Using Sniffer to Gather Information User Exchanging through a Web Browser

Worldwide browser share: July 2010

Percent

Source: Net Applications

Systems Security Management

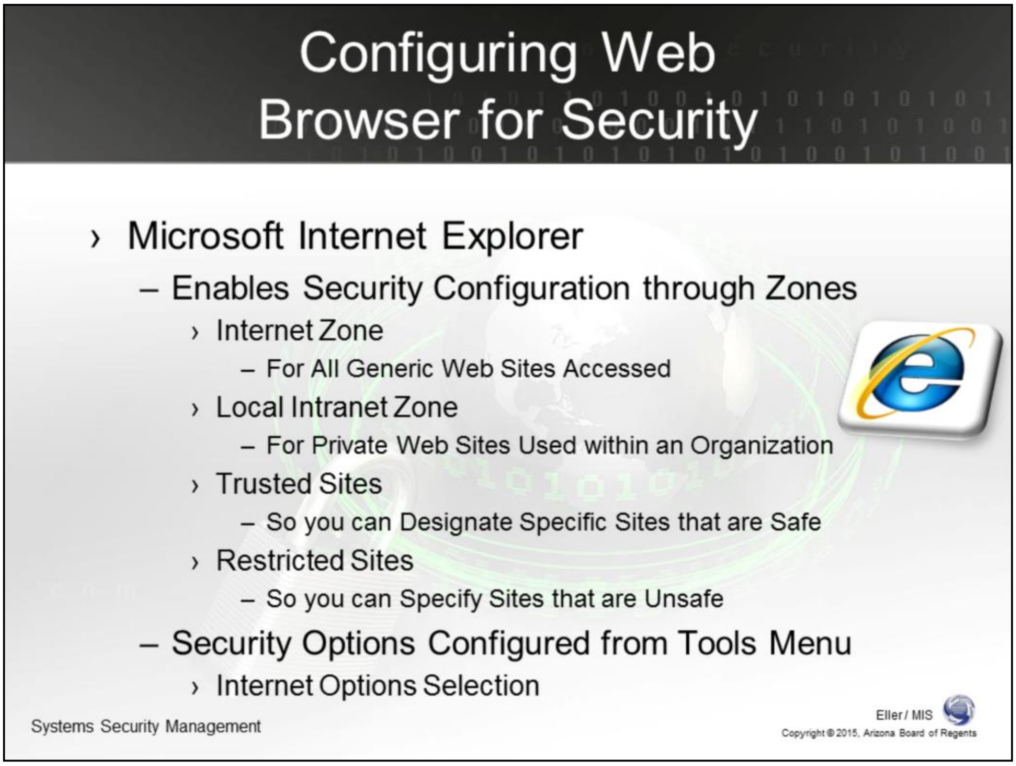
Eller / MIS

Copyright © 2015, Arizona Board of Regents

Configuring Web Browsers for Security

There are a wide variety of web browsers available for anyone to download and use; however, the five major web browsers include: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari, and Opera. The graph on this page takes these five browsers and displays the market share each has won for the month listed.

As we are all aware, the Internet is a public network. As such, it comes with security risks, including the possibility an attacker would use a sniffer to gather information a user is exchanging through the use of a web browser.



Configuring Web Browser for Security

- Microsoft Internet Explorer
  - Enables Security Configuration through Zones
    - Internet Zone
      - For All Generic Web Sites Accessed
    - Local Intranet Zone
      - For Private Web Sites Used within an Organization
    - Trusted Sites
      - So you can Designate Specific Sites that are Safe
    - Restricted Sites
      - So you can Specify Sites that are Unsafe
  - Security Options Configured from Tools Menu
    - Internet Options Selection

Systems Security Management

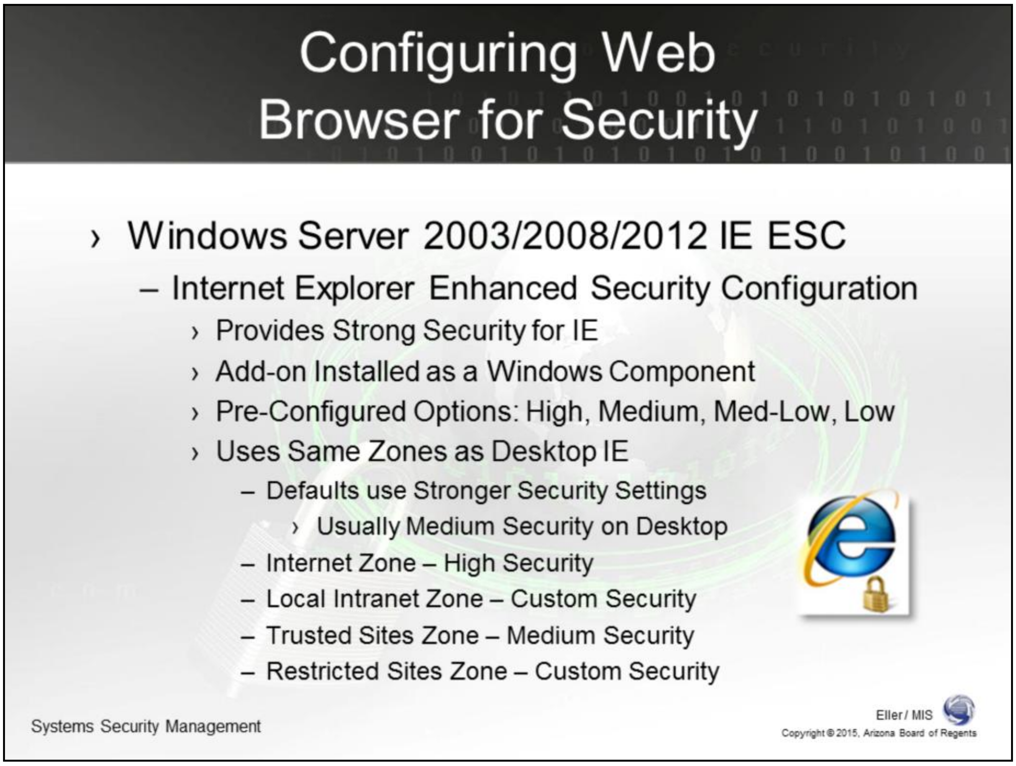
Eller / MIS

Configuring Web Browsers for Security (continued)

Microsoft’s Internet Explorer web browser allows users and SysAdmins to enable security configurations through the use of Zones. There are four primary security zones:

- **Internet Zone** – For All Generic Web Sites Accessed
- **Local Intranet Zone** – For Private Web Sites Used within an Organization
- **Trusted Sites** – So you can Designate Specific Sites that are Safe
- **Restricted Sites** – So you can Specify Sites that are Unsafe

All security options in Internet Explorer are configured from the Tools Menu and then selecting Internet Options.



Configuring Web Browser for Security

- Windows Server 2003/2008/2012 IE ESC
  - Internet Explorer Enhanced Security Configuration
    - Provides Strong Security for IE
    - Add-on Installed as a Windows Component
    - Pre-Configured Options: High, Medium, Med-Low, Low
    - Uses Same Zones as Desktop IE
      - Defaults use Stronger Security Settings
        - Usually Medium Security on Desktop
      - Internet Zone – High Security
      - Local Intranet Zone – Custom Security
      - Trusted Sites Zone – Medium Security
      - Restricted Sites Zone – Custom Security

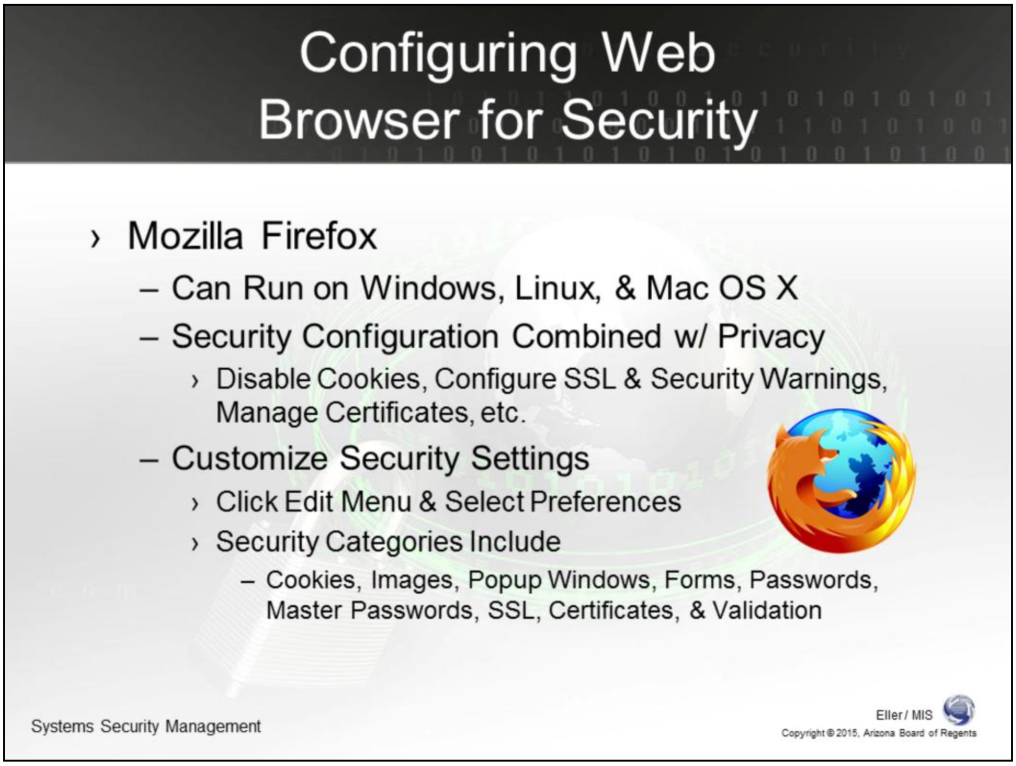
Systems Security Management

Eller / MIS

Configuring Web Browsers for Security (continued)

On Windows Servers 2003, 2008, and 2012, Microsoft has added a feature called the Internet Explorer Enhanced Security Configuration, or IE ESC. This option provides strong security for Internet Explorer and is an add-on that is installed as a Windows Component. On these server products, Internet Explorer uses the same zones as the Desktop version of IE, with pre-configured security levels of high, medium, med-low, and low. While the Desktop version normally sets security levels to Medium, IE ESC defaults to stronger security settings.

- Internet Zone – High Security
- Local Intranet Zone – Custom Security
- Trusted Sites Zone – Medium Security
- Restricted Sites Zone – Custom Security



Configuring Web Browser for Security

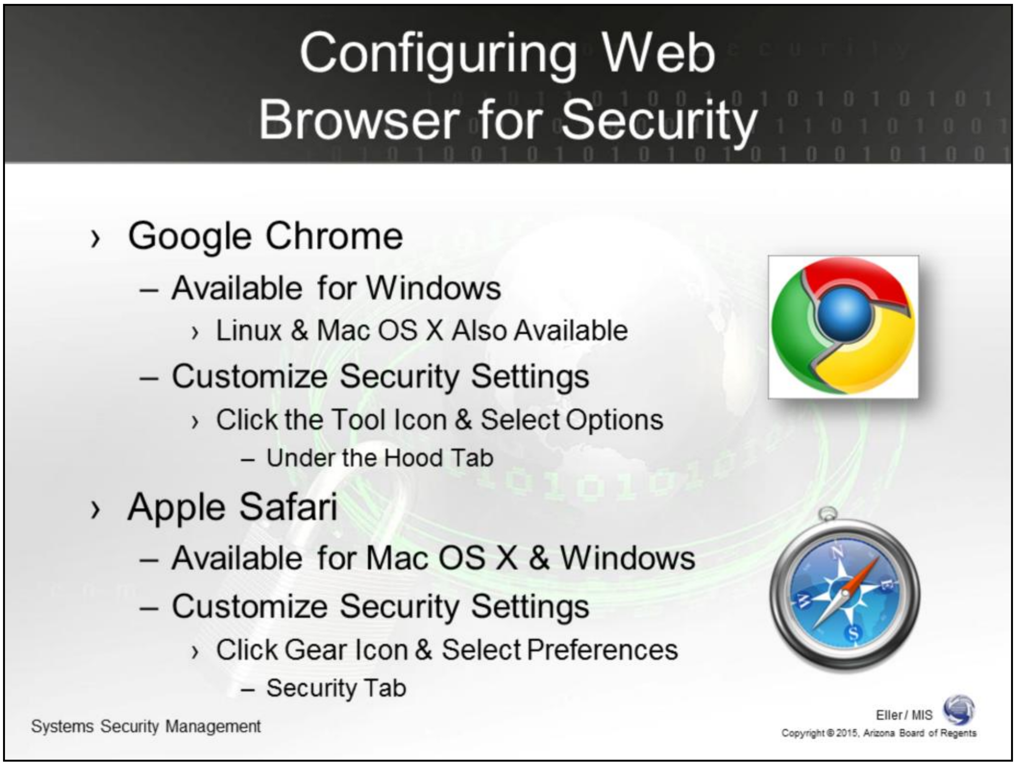
- Mozilla Firefox
  - Can Run on Windows, Linux, & Mac OS X
  - Security Configuration Combined w/ Privacy
    - Disable Cookies, Configure SSL & Security Warnings, Manage Certificates, etc.
  - Customize Security Settings
    - Click Edit Menu & Select Preferences
    - Security Categories Include
      - Cookies, Images, Popup Windows, Forms, Passwords, Master Passwords, SSL, Certificates, & Validation

Systems Security Management

Eller / MIS

Configuring Web Browsers for Security (continued)

Mozilla’s Firefox web browser can be installed on Windows, Linux, and Mac OS X systems. Firefox deploys a security configuration combined with privacy settings, such as disabling cookies, configuring SSL and security warnings, and managing certificates, among others. In order to customize security settings, one must click the Edit menu and select Preferences. Security categories will include: Cookies, Images, Popup Windows, Forms, Passwords, Master Passwords, SSL, Certificates, and Validation.



Configuring Web Browser for Security

- › Google Chrome
  - – Available for Windows
    - › Linux & Mac OS X Also Available
  - – Customize Security Settings
    - › Click the Tool Icon & Select Options
      - – Under the Hood Tab
- › Apple Safari
  - – Available for Mac OS X & Windows
  - – Customize Security Settings
    - › Click Gear Icon & Select Preferences
      - – Security Tab

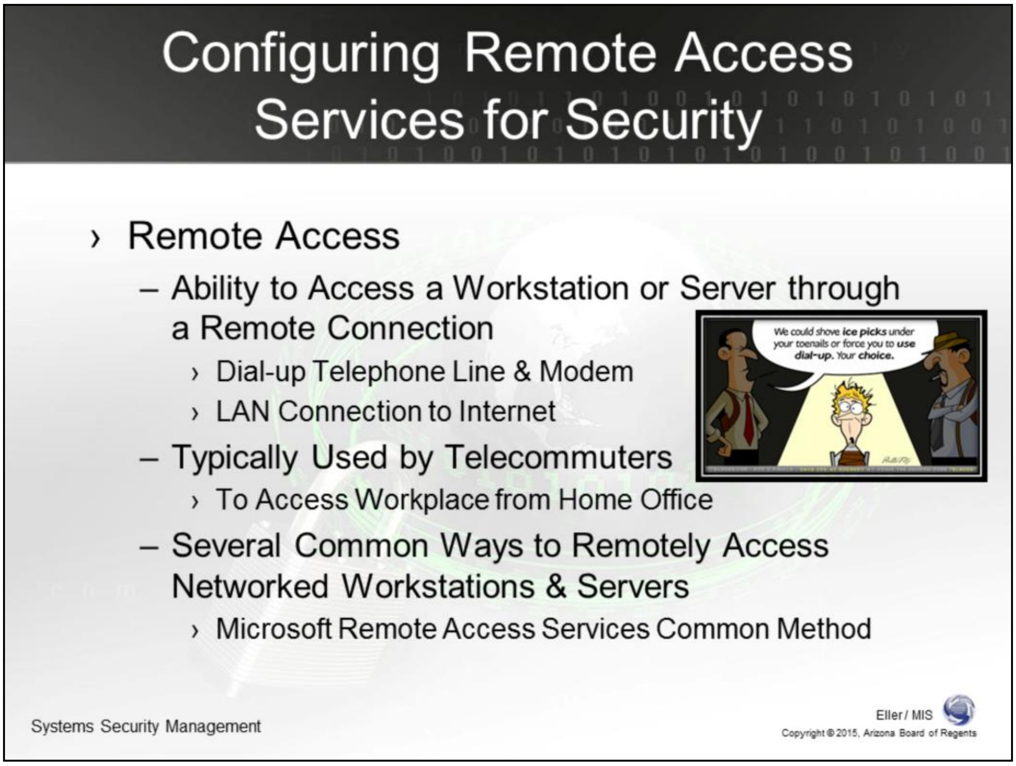
Systems Security Management

Eller / MIS

Configuring Web Browsers for Security (continued)

The Google Chrome browser is available for Windows, Linux, and Mac OS X, and one can customize security settings by clicking on the Tool icon and selecting Options, then the Under the Hood tab.

Apple’s Safari is available for Mac OS X and Windows. One can customize security settings by clicking on the Gear icon and selecting Preferences, then navigating to the Security tab.



Configuring Remote Access Services for Security

- Remote Access
  - Ability to Access a Workstation or Server through a Remote Connection
    - Dial-up Telephone Line & Modem
    - LAN Connection to Internet
  - Typically Used by Telecommuters
    - To Access Workplace from Home Office
  - Several Common Ways to Remotely Access Networked Workstations & Servers
    - Microsoft Remote Access Services Common Method

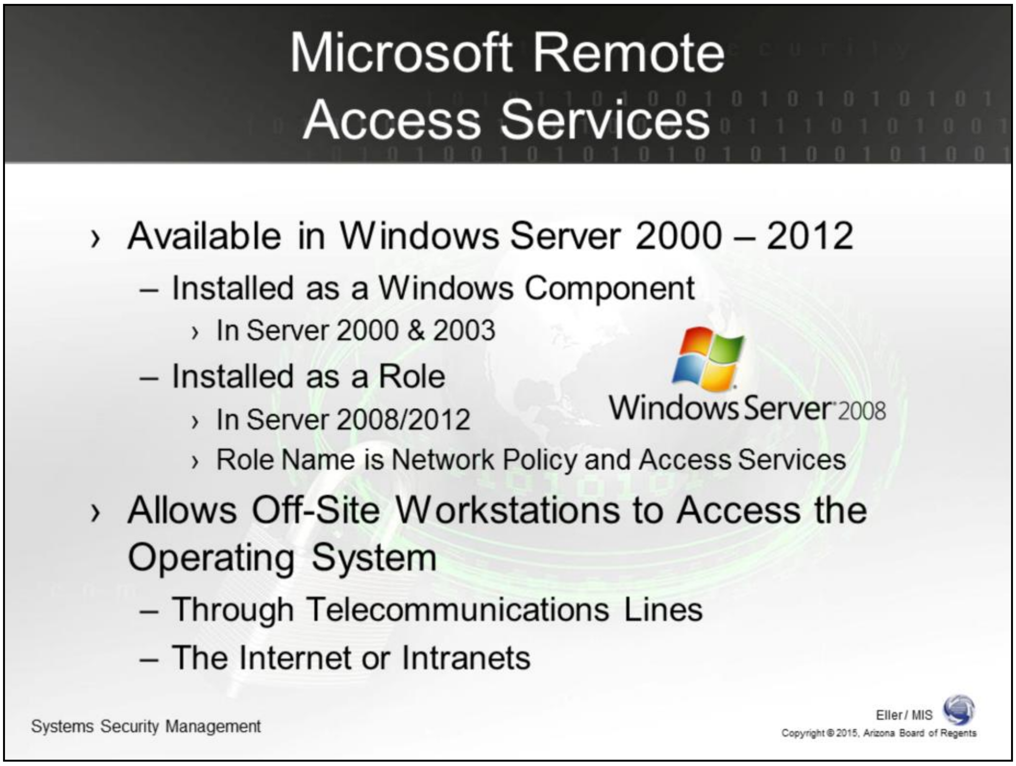
We could shove **ice picks** under your toenails or force you to **use dial-up.** *Your* **choice.**

Systems Security Management

Eller / MIS

Configuring Remote Access Services for Security

When you think about the term Remote Access, accessing your office from the road comes to mind. Remote Access is the ability to access a workstation or server through a remote connection, such as a dial-up telephone line and modem, or a LAN connection to the Internet. Typically remote access is used by telecommuters to access the workplace from a home office. There are several common ways to remotely access networked workstations and servers, one of which is Microsoft's Remote Access Services.



Microsoft Remote Access Services

- Available in Windows Server 2000 – 2012
  - Installed as a Windows Component
    - In Server 2000 & 2003
  - Installed as a Role
    - In Server 2008/2012
    - Role Name is Network Policy and Access Services
- Allows Off-Site Workstations to Access the Operating System
  - Through Telecommunications Lines
  - The Internet or Intranets

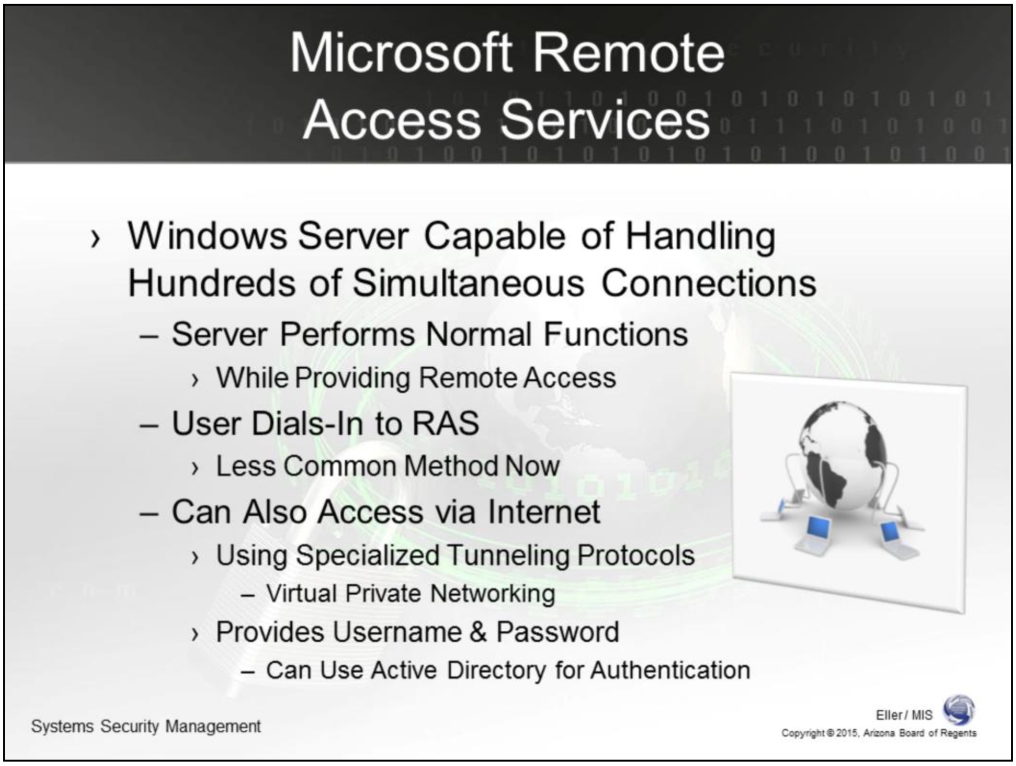
Windows Server 2008

Systems Security Management

Eller / MIS

Microsoft Remote Access Services

Microsoft Remote Access Services, or RAS, is available in Windows Server 2000, 2003, 2008, and 2012 versions. The service is installed as a Windows Component in Server 2000 and 2003. Under Windows Server 2008 and 2012, it is installed as a Role under the new name: Network Policy and Access Services. RAS allows off-site workstations to access the operating system through telecommunications lines, the Internet, or Intranets.



Microsoft Remote Access Services

- Windows Server Capable of Handling Hundreds of Simultaneous Connections
  - Server Performs Normal Functions
    - While Providing Remote Access
  - User Dials-In to RAS
    - Less Common Method Now
  - Can Also Access via Internet
    - Using Specialized Tunneling Protocols
      - Virtual Private Networking
    - Provides Username & Password
      - Can Use Active Directory for Authentication

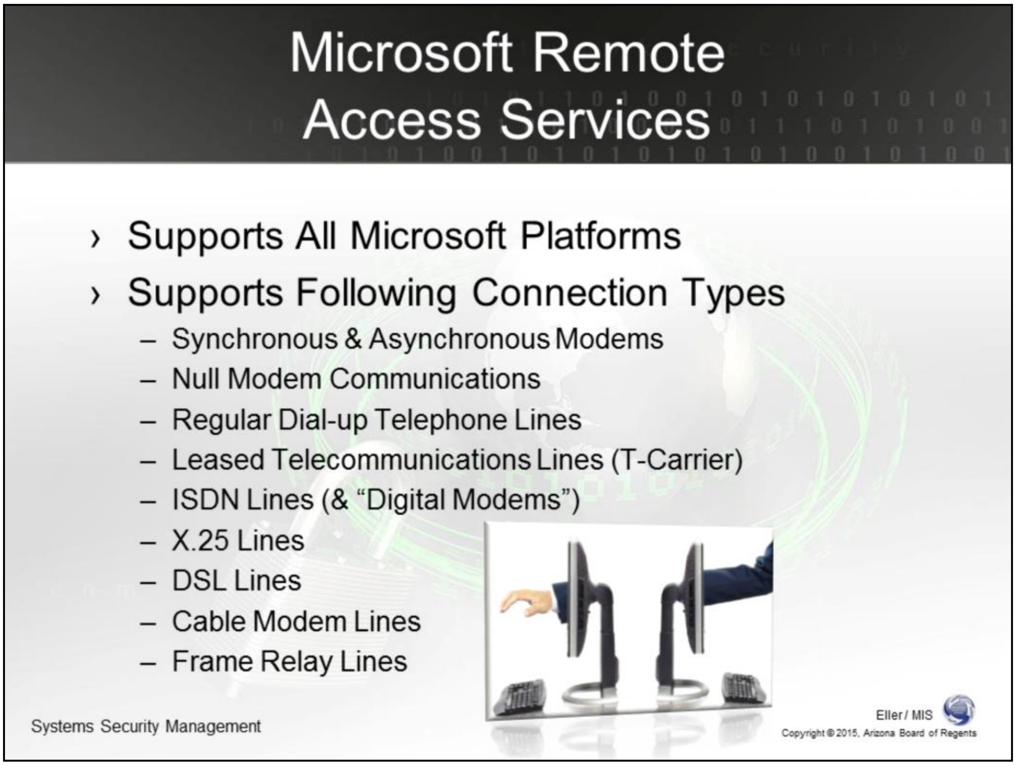
Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

Microsoft Remote Access Services (continued)

Windows Server is capable of handling hundreds of simultaneous connections through RAS, and the server will continue to perform all the normal functions while still providing remote access. A user will dial-in to a RAS server via telephone, which is a less common method now. Alternatively, the user can “dial-in” to RAS through an Internet connection using specialized tunneling protocols, such as a virtual private network. The user will then provide a username and password, which can be authenticated against an Active Directory.



Microsoft Remote Access Services

- › Supports All Microsoft Platforms
- › Supports Following Connection Types
  - – Synchronous & Asynchronous Modems
  - – Null Modem Communications
  - – Regular Dial-up Telephone Lines
  - – Leased Telecommunications Lines (T-Carrier)
  - – ISDN Lines (& “Digital Modems”)
  - – X.25 Lines
  - – DSL Lines
  - – Cable Modem Lines
  - – Frame Relay Lines

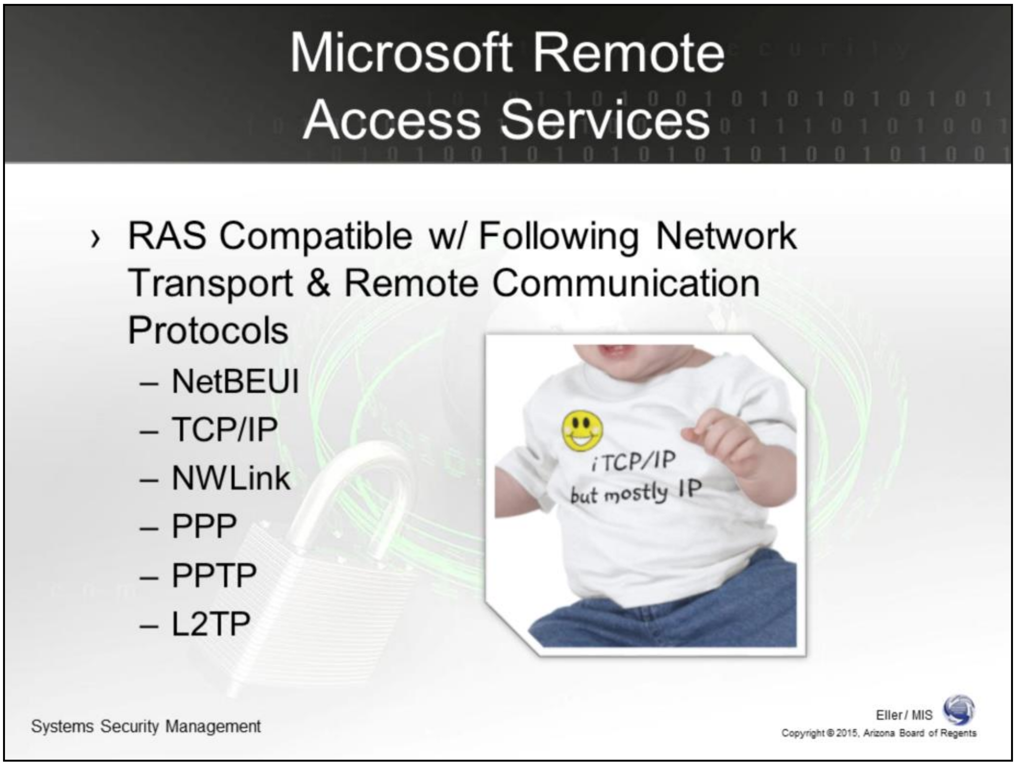
Systems Security Management

Eller / MIS

Microsoft Remote Access Services (continued)

RAS supports all Microsoft platforms as well as the following connection types:

- Synchronous & Asynchronous Modems
- Null Modem Communications
- Regular Dial-up Telephone Lines
- Leased Telecommunications Lines (T-Carrier)
- ISDN Lines (& “Digital Modems”)
- X.25 Lines
- DSL Lines
- Cable Modem Lines
- Frame Relay Lines



Microsoft Remote Access Services

› RAS Compatible w/ Following Network Transport & Remote Communication Protocols
  – NetBEUI
  – TCP/IP
  – NWLink
  – PPP
  – PPTP
  – L2TP

iTCP/IP
but mostly IP

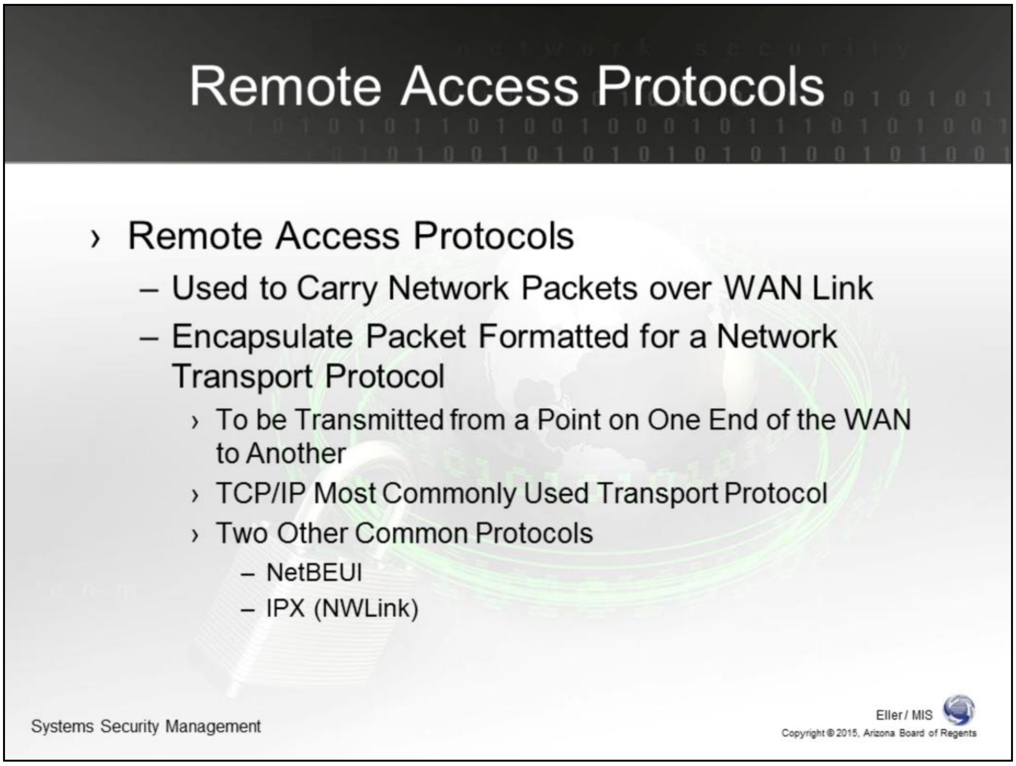
Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Microsoft Remote Access Services (continued)

RAS is also compatible with a number of different network transport and remote communication protocols, including:

- NetBEUI
- TCP/IP
- NWLink
- PPP
- PPTP
- L2TP



Remote Access Protocols

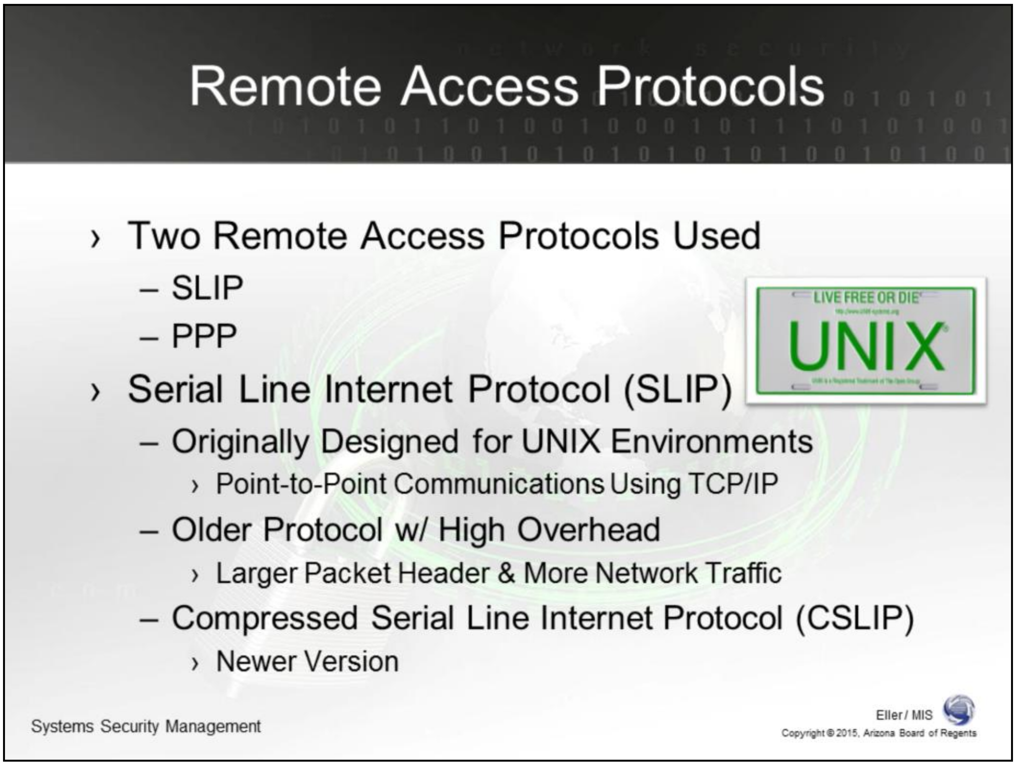
- Remote Access Protocols
  - Used to Carry Network Packets over WAN Link
  - Encapsulate Packet Formatted for a Network Transport Protocol
    - To be Transmitted from a Point on One End of the WAN to Another
    - TCP/IP Most Commonly Used Transport Protocol
    - Two Other Common Protocols
      - NetBEUI
      - IPX (NWLink)

Systems Security Management

Eller / MIS

Remote Access Protocols

Remote access protocols are used to carry network packets over a WAN link. Typically these protocols will encapsulate a packet that is formatted for a network transport protocol in order to allow transmission from a point on one end of the WAN to another. TCP/IP is the most commonly used transport protocol; however, the NetBEUI and IPX protocols are also commonly used.



Remote Access Protocols

- Two Remote Access Protocols Used
  - SLIP
  - PPP
- Serial Line Internet Protocol (SLIP)
  - Originally Designed for UNIX Environments
    - Point-to-Point Communications Using TCP/IP
  - Older Protocol w/ High Overhead
    - Larger Packet Header & More Network Traffic
  - Compressed Serial Line Internet Protocol (CSLIP)
    - Newer Version

network security
LIVE FREE OR DIE
UNIX

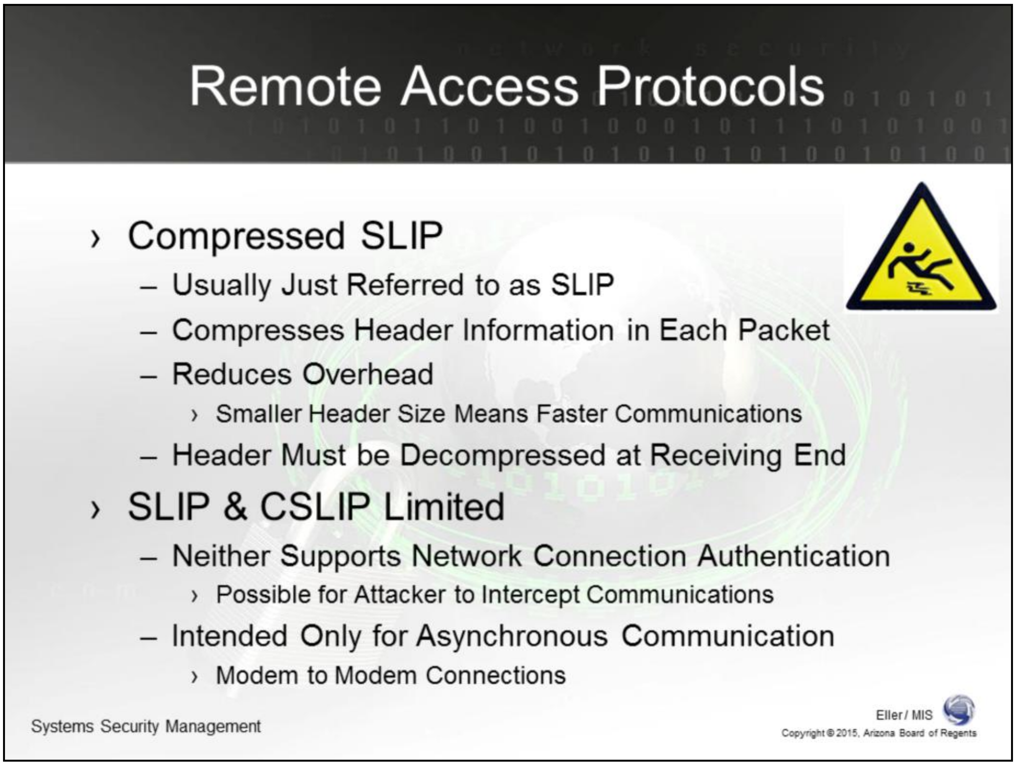
Systems Security Management

Eller / MIS

Remote Access Protocols (continued)

Two remote access protocols are commonly used by RAS servers: SLIP and PPP.

The Serial Line Internet Protocol, or SLIP, was originally designed for UNIX environments to provide point-to-point communications using TCP/IP. This is an older protocol with high overhead. This means SLIP packets have a larger packet header and it generates more network traffic during transmission. SLIP has been improved with a newer version called the Compressed Serial Line Internet Protocol, or CSLIP.



Remote Access Protocols

- Compressed SLIP
  - Usually Just Referred to as SLIP
  - Compresses Header Information in Each Packet
  - Reduces Overhead
    - Smaller Header Size Means Faster Communications
  - Header Must be Decompressed at Receiving End
- SLIP & CSLIP Limited
  - Neither Supports Network Connection Authentication
    - Possible for Attacker to Intercept Communications
  - Intended Only for Asynchronous Communication
    - Modem to Modem Connections

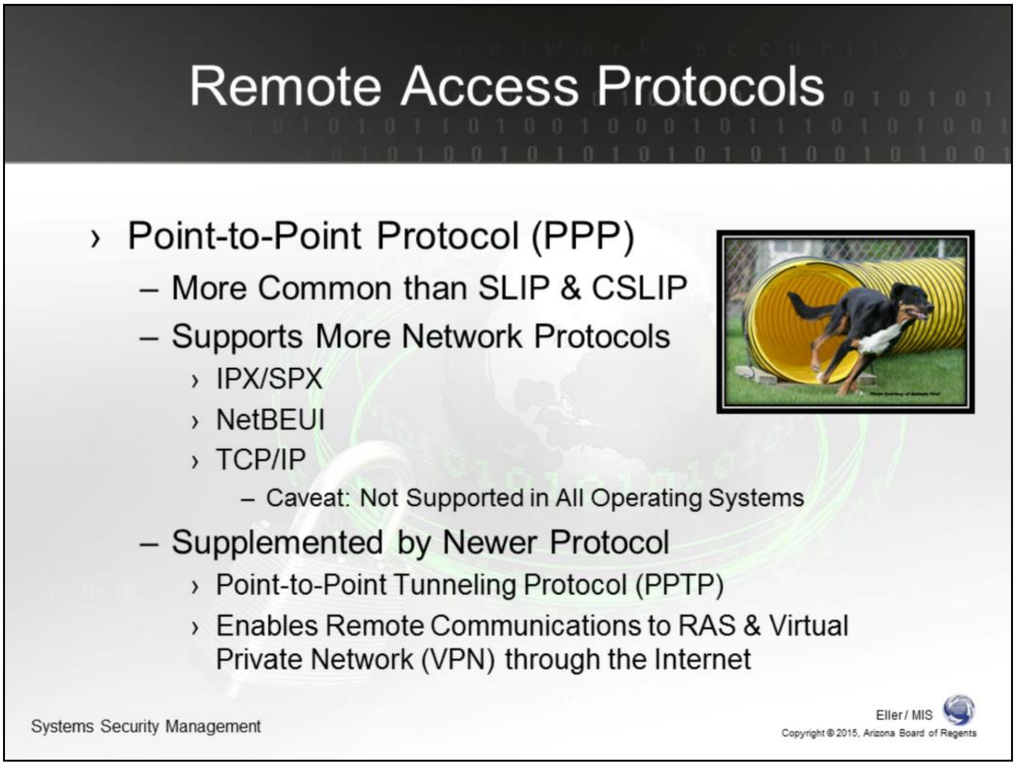
Systems Security Management

Eller / MIS

Remote Access Protocols (continued)

CSLIP, which is still referred to as SLIP, was designed to compress header information in each packet in order to reduce the overhead during transport. This compression reduces the size of the packet headers, which makes for faster communications; however, this packet header must be decompressed at the receiving end.

SLIP and CSLIP are both limited in that neither one supports network connection authentication, so it is possible for an attacker to intercept communications. These two protocols were intended only for asynchronous communication, such as modem-to-modem connections.



Remote Access Protocols

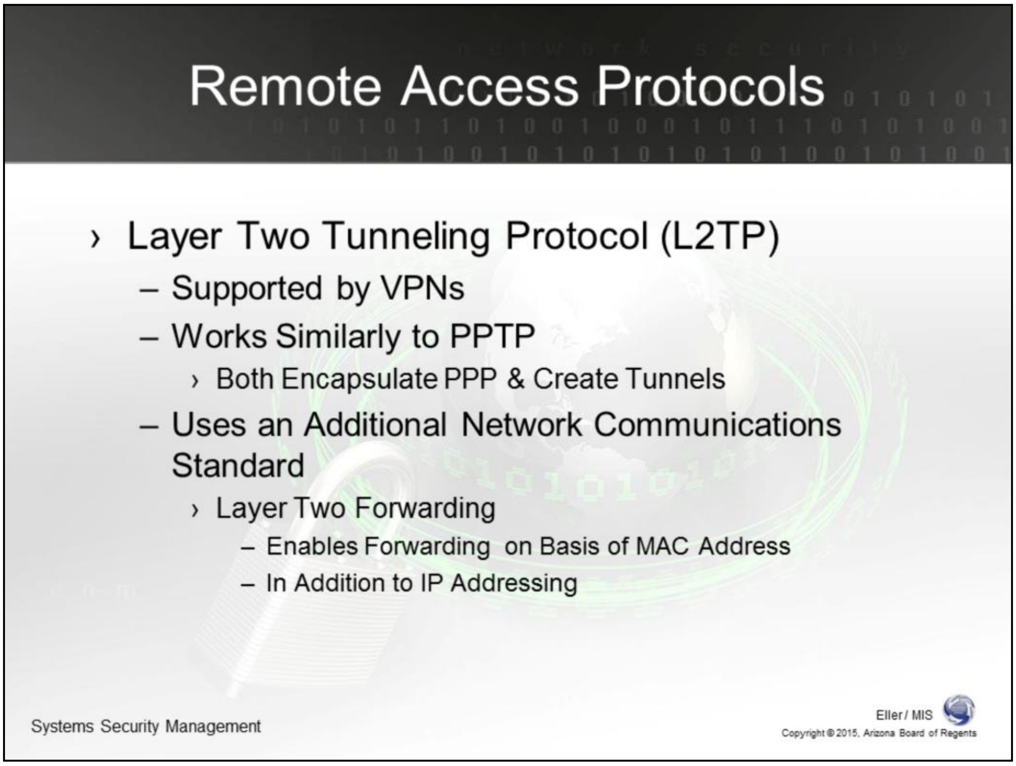
- Point-to-Point Protocol (PPP)
  - More Common than SLIP & CSLIP
  - Supports More Network Protocols
    - IPX/SPX
    - NetBEUI
    - TCP/IP
      - Caveat: Not Supported in All Operating Systems
  - Supplemented by Newer Protocol
    - Point-to-Point Tunneling Protocol (PPTP)
    - Enables Remote Communications to RAS & Virtual Private Network (VPN) through the Internet

Systems Security Management

Eller / MIS

Remote Access Protocols (continued)

Another common remote access protocol is the Point-to-Point Protocol, or PPP. This protocol is much more common than SLIP and CSLIP as it supports more network protocols, such as IPX, NetBEUI, and TCP/IP. The caveat here is that PPP is not supported in all operating systems. PPP has been supplemented by a newer protocol called the Point-to-Point Tunneling Protocol, or PPTP. This newer protocol enables remote communications to Microsoft RAS and Virtual Private Networks through the Internet.



Remote Access Protocols

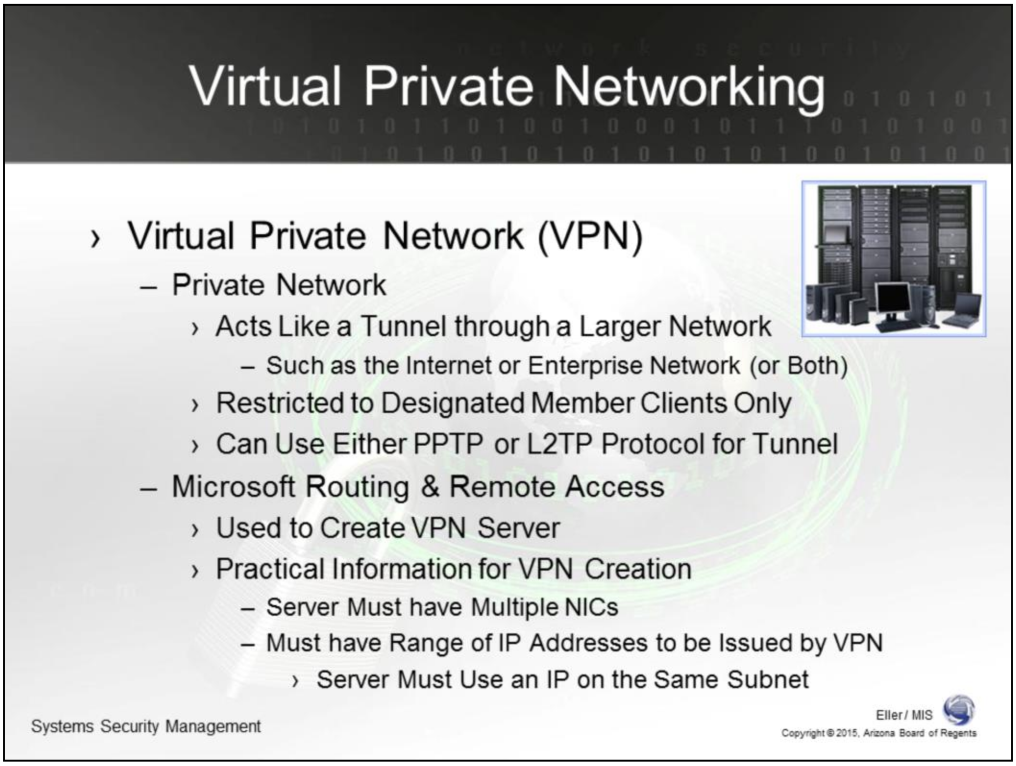
- Layer Two Tunneling Protocol (L2TP)
  - Supported by VPNs
  - Works Similarly to PPTP
    - Both Encapsulate PPP & Create Tunnels
  - Uses an Additional Network Communications Standard
    - Layer Two Forwarding
      - Enables Forwarding on Basis of MAC Address
      - In Addition to IP Addressing

Systems Security Management

Eller / MIS

Remote Access Protocols (continued)

The Layer Two Tunneling Protocol, or L2TP, is another remote access protocol that is supported primarily by VPNs. This protocol works similarly to PPTP, in that both encapsulate PPP and create tunnels from one network to another. L2TP uses an additional network communications standard called Layer Two Forwarding. This enables forwarding on the basis of MAC Address in addition to IP Addressing. L2TP gets its name because it works in the data-link layer, or layer 2, of the OSI model.



Virtual Private Networking

- Virtual Private Network (VPN)
  - Private Network
    - Acts Like a Tunnel through a Larger Network
      - Such as the Internet or Enterprise Network (or Both)
    - Restricted to Designated Member Clients Only
    - Can Use Either PPTP or L2TP Protocol for Tunnel
  - Microsoft Routing & Remote Access
    - Used to Create VPN Server
    - Practical Information for VPN Creation
      - Server Must have Multiple NICs
      - Must have Range of IP Addresses to be Issued by VPN
        - Server Must Use an IP on the Same Subnet

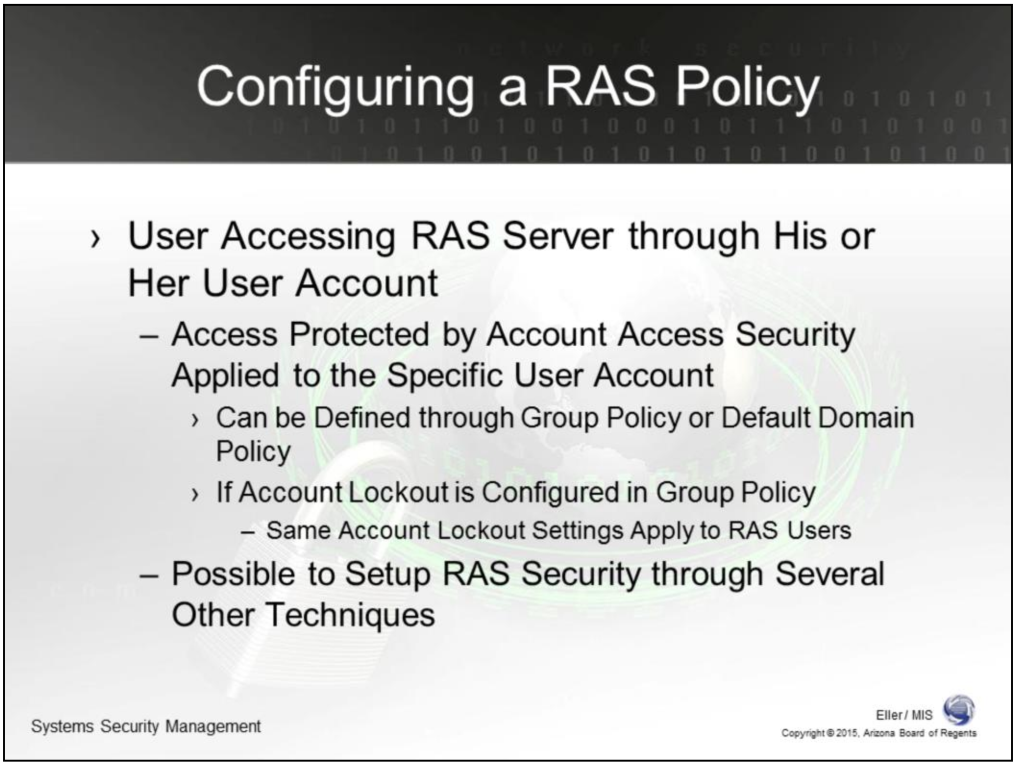
Systems Security Management

Eller / MIS

Virtual Private Networking

Virtual Private Networks, or VPNs, are a private network standard that acts like a tunnel through a larger network, such as the Internet or Enterprise, or both. VPNs are typically used by telecommuters who need to access organizational resources from a home office. Since VPNs are restricted to designated member clients only, this makes the use of VPNs a secure option for accommodating those who need remote access to resources. VPNs can use either PPTP or L2TP as the effective protocol for the tunnel, this is an option selected by the SysAdmin when configuring the VPN.

In Windows, Microsoft's Routing and Remote Access is used to create a VPN server. When configuring a VPN using RAS, there is some important information to consider. The server itself must have at least two network interface cards. This is to allow for one card that accepts incoming requests from remote clients, while the other card sends the data out into the organization's network. In addition, the RAS server will need to be configured with a range of IP addresses. These addresses will be issued to dial-up clients who connect to the VPN so their remote systems appear to be a local system on the organization's network. In order for everything to work smoothly, the server must have at least one of the network cards configured to use an IP address that is part of the same subnetwork as the IP range that has been added to the RAS configuration.



Configuring a RAS Policy

- User Accessing RAS Server through His or Her User Account
  - Access Protected by Account Access Security Applied to the Specific User Account
    - Can be Defined through Group Policy or Default Domain Policy
    - If Account Lockout is Configured in Group Policy
      - Same Account Lockout Settings Apply to RAS Users
  - Possible to Setup RAS Security through Several Other Techniques

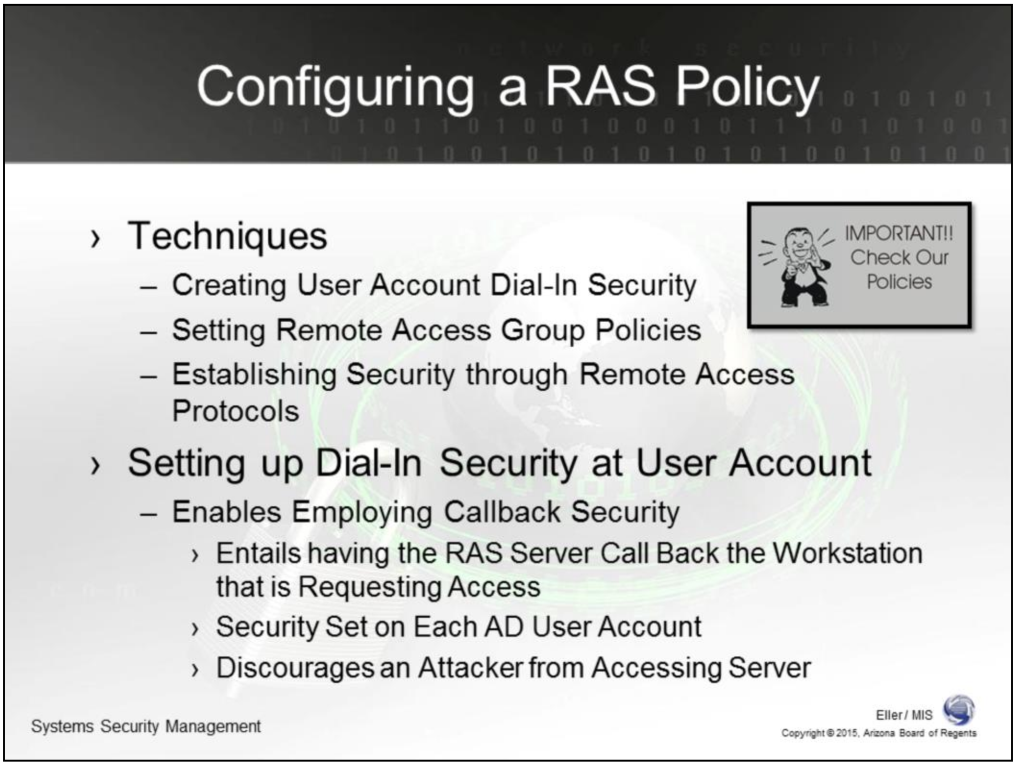
Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

Configuring a RAS Policy

When connecting to a RAS server, users will access the server through the use of his or her user account. Access to the RAS system is protected by account access security that is applied to the specific user account. In other words, there are attributes in user account objects in Active Directory that control whether or not a specific account can dial-in to a RAS server. These attributes can be defined through group policy or the default domain policy. In the event a SysAdmin has configured account lockout policies in group policy, then the same account lockout settings will apply to RAS users as well. It is also possible to setup RAS security through several other techniques.



Configuring a RAS Policy

IMPORTANT!! Check Our Policies

- Techniques
  - Creating User Account Dial-In Security
  - Setting Remote Access Group Policies
  - Establishing Security through Remote Access Protocols
- Setting up Dial-In Security at User Account
  - Enables Employing Callback Security
    - Entails having the RAS Server Call Back the Workstation that is Requesting Access
    - Security Set on Each AD User Account
    - Discourages an Attacker from Accessing Server

Systems Security Management

Eller / MIS

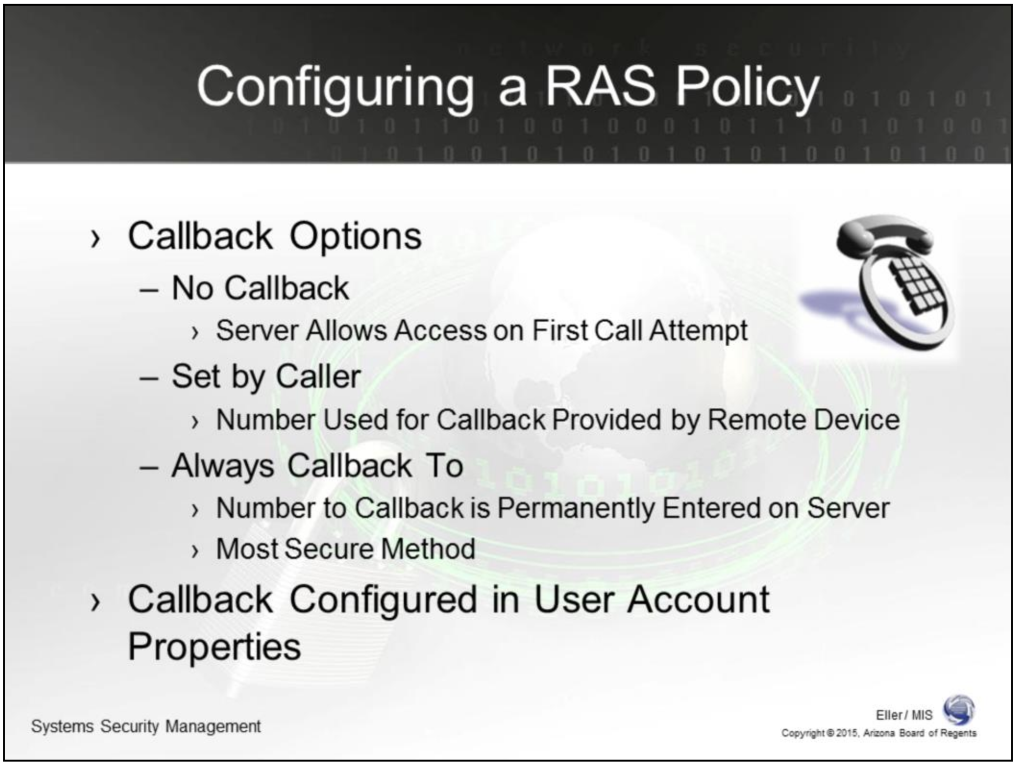
Copyright © 2015, Arizona Board of Regents

Configuring a RAS Policy (continued)

Such techniques include:

- Creating User Account Dial-In Security
- Setting Remote Access Group Policies
- Establishing Security through Remote Access Protocols

When setting up dial-in security at the user account level, this enables employing callback security. Callback security entails having the RAS server call the workstation back which is requesting access remotely. In other words, the client will dial-in to the RAS server and the RAS server will disconnect the client. The RAS server then dials the client back in order to establish the connection. Note that while the term dial-in has roots in using telephone lines connecting to modems, more modern uses involve “dialing” an IP address to establish a connection. This callback information is set on each Active Directory user account, and since clients cannot directly connect to the RAS server, this helps to discourage an attacker from accessing the server.



Configuring a RAS Policy

- Callback Options
  - No Callback
    - Server Allows Access on First Call Attempt
  - Set by Caller
    - Number Used for Callback Provided by Remote Device
  - Always Callback To
    - Number to Callback is Permanently Entered on Server
    - Most Secure Method
- Callback Configured in User Account Properties

Systems Security Management

Eller / MIS

Configuring a RAS Policy (continued)

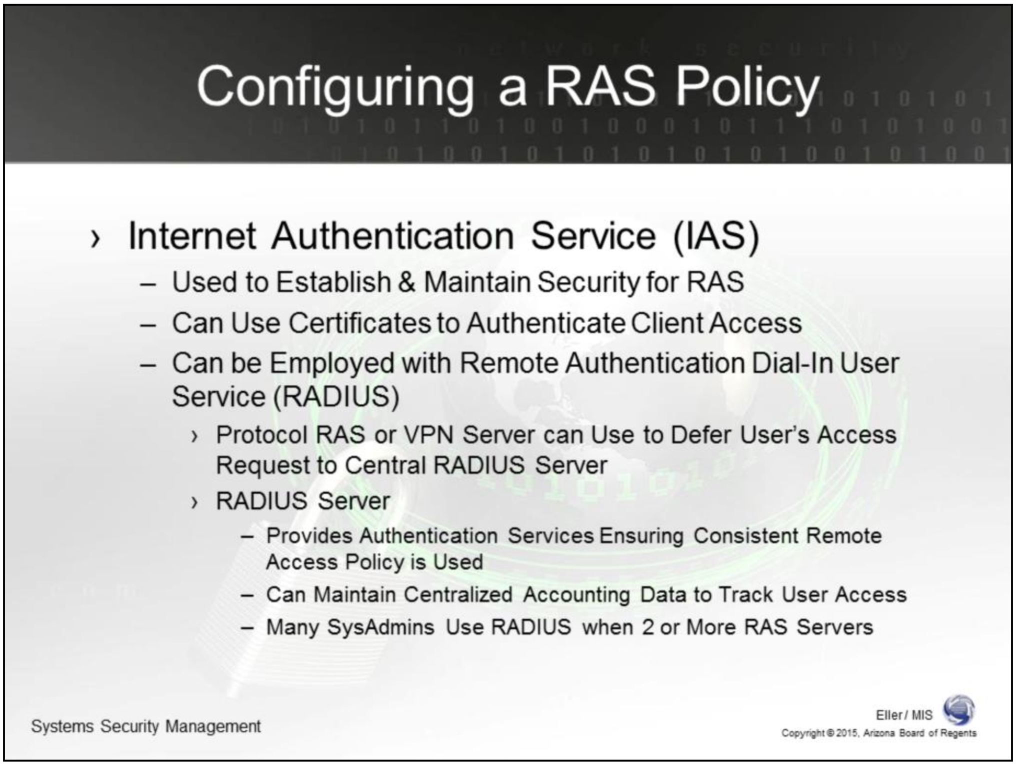
When configuring callback security, there are a few options that can be selected:

No Callback – Server Allows Access on First Call Attempt

Set by Caller – Number Used for Callback Provided by Remote Device

Always Callback To – Number to Callback is Permanently Entered on Server. This is the Most Secure Method

Again, the callback security options are configured in the user account properties.



Configuring a RAS Policy

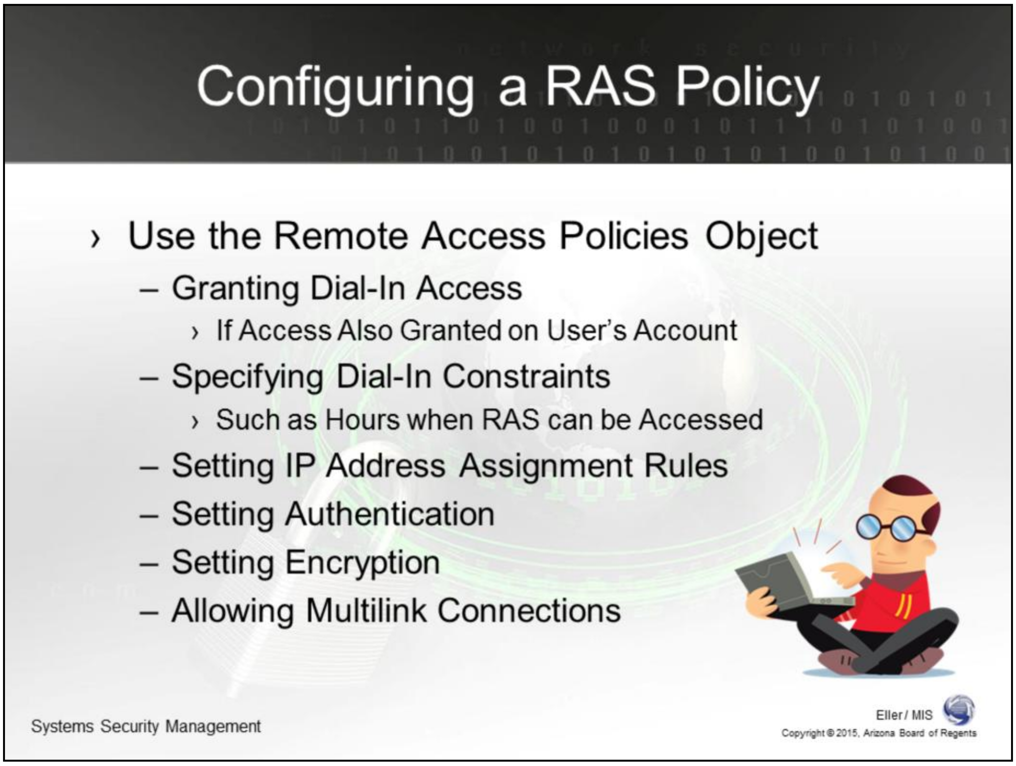
- Internet Authentication Service (IAS)
  - Used to Establish & Maintain Security for RAS
  - Can Use Certificates to Authenticate Client Access
  - Can be Employed with Remote Authentication Dial-In User Service (RADIUS)
    - Protocol RAS or VPN Server can Use to Defer User's Access Request to Central RADIUS Server
    - RADIUS Server
      - Provides Authentication Services Ensuring Consistent Remote Access Policy is Used
      - Can Maintain Centralized Accounting Data to Track User Access
      - Many SysAdmins Use RADIUS when 2 or More RAS Servers

Systems Security Management

Eller / MIS

Configuring a RAS Policy (continued)

Another RAS policy option would involve installing the Internet Authentication Service, or IAS. This service is used to establish and maintain security for a RAS server. IAS security makes use of certificates to help authenticate client access, and this service can be deployed with a RADIUS server. RADIUS is an authentication protocol that a RAS or VPN server can use to defer user access requests to a central server. The RADIUS server will provide authentication services, ensuring that consistent remote access policies are used. This server can also maintain centralized accounting data to track user access. Many SysAdmins choose to use RADIUS servers for authentication when there are two or more RAS servers deployed on a network.



Configuring a RAS Policy

- Use the Remote Access Policies Object
  - Granting Dial-In Access
    - If Access Also Granted on User's Account
  - Specifying Dial-In Constraints
    - Such as Hours when RAS can be Accessed
  - Setting IP Address Assignment Rules
  - Setting Authentication
  - Setting Encryption
  - Allowing Multilink Connections

Systems Security Management

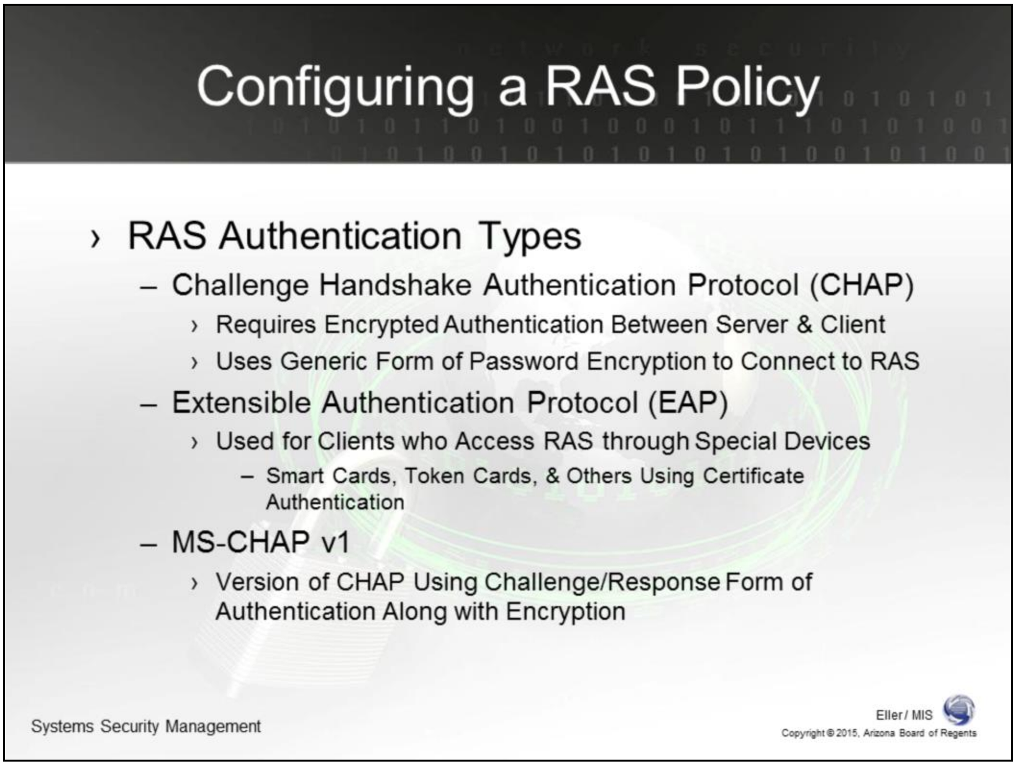
Eller / MIS

Copyright © 2015, Arizona Board of Regents

Configuring a RAS Policy (continued)

Another way to configure RAS policies on the network involves using the remote access policies object. This policy object will allow for all of the following configuration options:

- Granting Dial-In Access – If Access Also Granted on User's Account
- Specifying Dial-In Constraints – Such as Hours when RAS can be Accessed
- Setting IP Address Assignment Rules
- Setting Authentication
- Setting Encryption
- Allowing Multilink Connections



Configuring a RAS Policy

- RAS Authentication Types
  - Challenge Handshake Authentication Protocol (CHAP)
    - Requires Encrypted Authentication Between Server & Client
    - Uses Generic Form of Password Encryption to Connect to RAS
  - Extensible Authentication Protocol (EAP)
    - Used for Clients who Access RAS through Special Devices
      - Smart Cards, Token Cards, & Others Using Certificate Authentication
  - MS-CHAP v1
    - Version of CHAP Using Challenge/Response Form of Authentication Along with Encryption

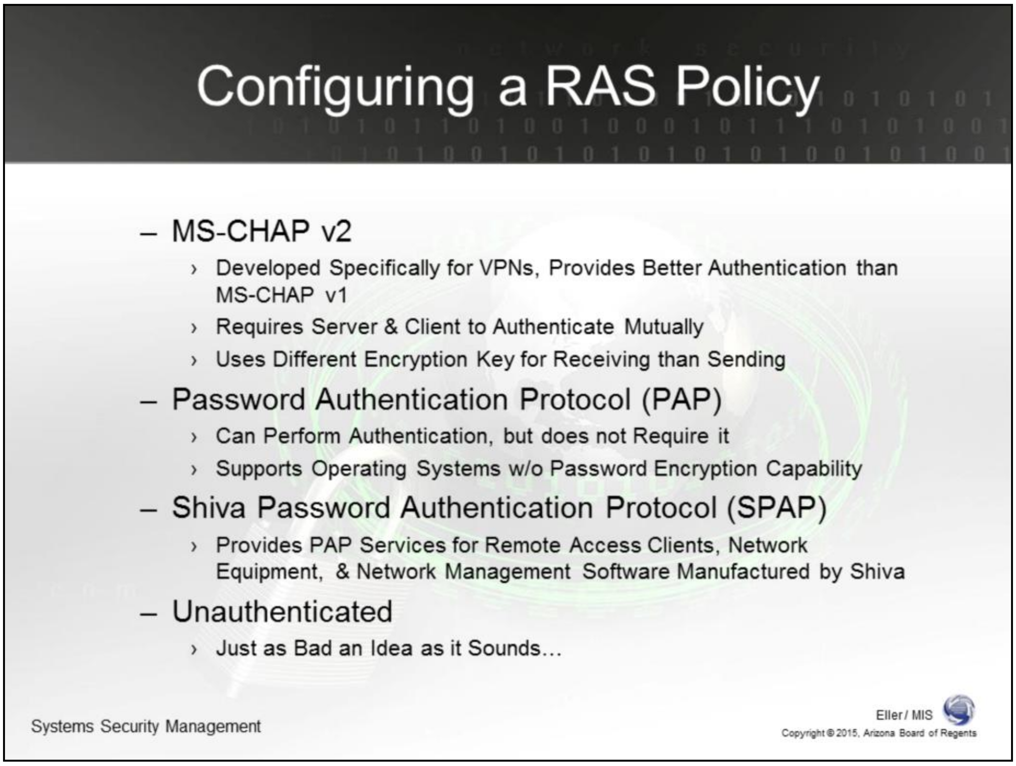
Systems Security Management

Eller / MIS

Configuring a RAS Policy (continued)

RAS can also be configured to use specific authentication types. The possible authentication options include:

- Challenge Handshake Authentication Protocol (CHAP)
  - Requires Encrypted Authentication Between Server & Client and Uses a Generic Form of Password Encryption to Connect to RAS
- Extensible Authentication Protocol (EAP)
  - Used for Clients who Access RAS through Special Devices such as Smart Cards, Token Cards, & Others Using Certificate Authentication
- MS-CHAP v1
  - Version of CHAP Using Challenge/Response Form of Authentication Along with Encryption



Configuring a RAS Policy

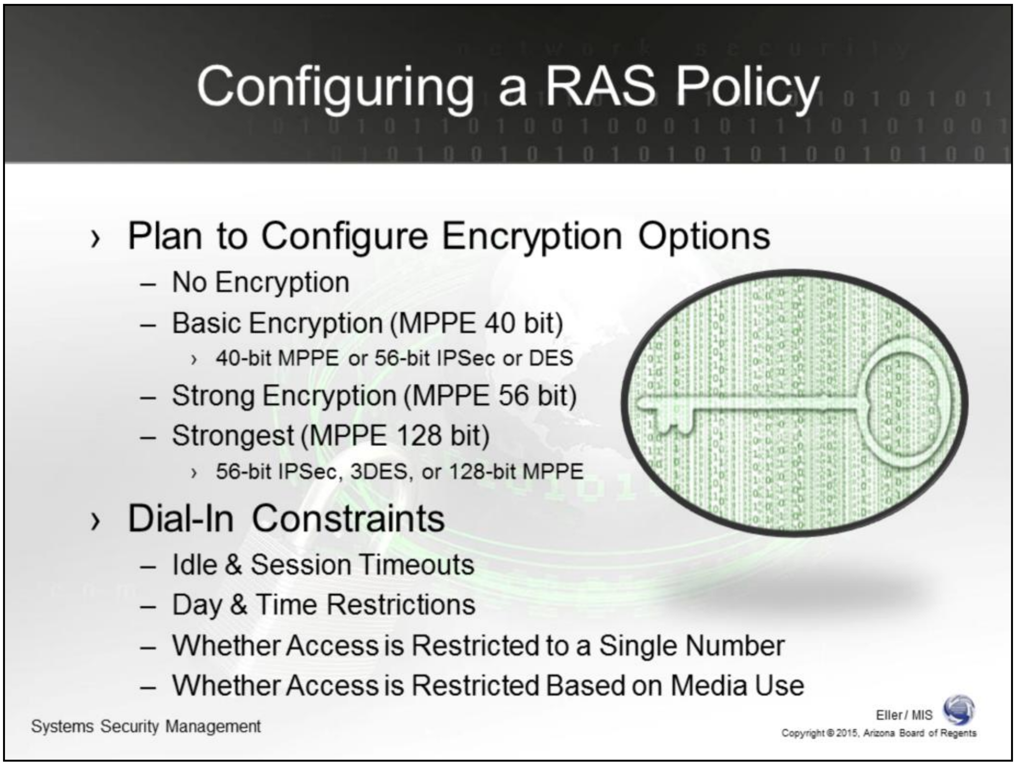
- MS-CHAP v2
  - Developed Specifically for VPNs, Provides Better Authentication than MS-CHAP v1
  - Requires Server & Client to Authenticate Mutually
  - Uses Different Encryption Key for Receiving than Sending
- Password Authentication Protocol (PAP)
  - Can Perform Authentication, but does not Require it
  - Supports Operating Systems w/o Password Encryption Capability
- Shiva Password Authentication Protocol (SPAP)
  - Provides PAP Services for Remote Access Clients, Network Equipment, & Network Management Software Manufactured by Shiva
- Unauthenticated
  - Just as Bad an Idea as it Sounds…

Systems Security Management

Eller / MIS

Configuring a RAS Policy (continued)

- MS-CHAP v2
  - Developed Specifically for VPNs, Provides Better Authentication than MS-CHAP v1
  - Requires Server & Client to Authenticate Mutually
  - Uses Different Encryption Key for Receiving than Sending
- Password Authentication Protocol (PAP)
  - Can Perform Authentication, but does not Require it
  - Supports Operating Systems w/o Password Encryption Capability
- Shiva Password Authentication Protocol (SPAP)
  - Provides PAP Services for Remote Access Clients, Network Equipment, & Network Management Software Manufactured by Shiva
- Unauthenticated
  - This is Just as Bad an Idea as it Sounds



Configuring a RAS Policy

- Plan to Configure Encryption Options
  - No Encryption
  - Basic Encryption (MPPE 40 bit)
    - 40-bit MPPE or 56-bit IPSec or DES
  - Strong Encryption (MPPE 56 bit)
  - Strongest (MPPE 128 bit)
    - 56-bit IPSec, 3DES, or 128-bit MPPE
- Dial-In Constraints
  - Idle & Session Timeouts
  - Day & Time Restrictions
  - Whether Access is Restricted to a Single Number
  - Whether Access is Restricted Based on Media Use

Systems Security Management

Eller / MIS

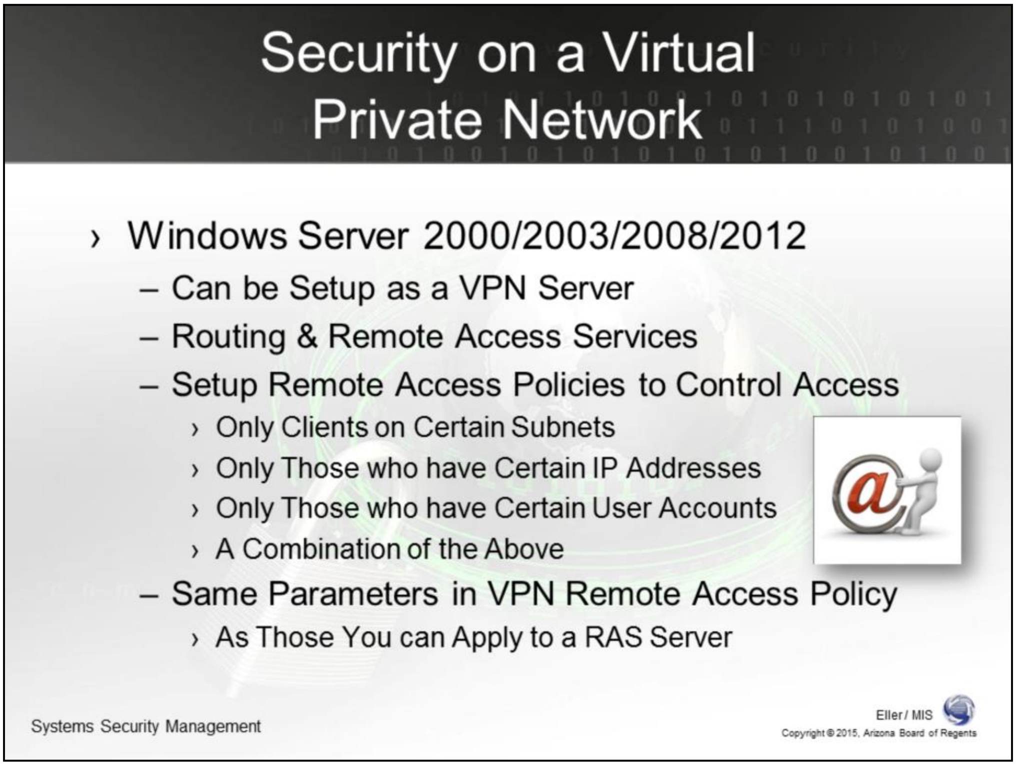
Configuring a RAS Policy (continued)

SysAdmins should plan to configure encryption options when setting up a RAS server. The possible encryption options include:

- No Encryption
- Basic Encryption – 40-bit MPPE or 56-bit IPSec or DES
- Strong Encryption –56 bit MPPE
- Strongest – 56-bit IPSec, 3DES, or 128-bit MPPE

In addition, a SysAdmin can configure certain dial-in constraints to help improve security. These constraints include:

- Idle & Session Timeouts
- Day & Time Restrictions
- Whether Access is Restricted to a Single Number
- Whether Access is Restricted Based on Media Use



Security on a Virtual Private Network

- Windows Server 2000/2003/2008/2012
  - Can be Setup as a VPN Server
  - Routing & Remote Access Services
  - Setup Remote Access Policies to Control Access
    - Only Clients on Certain Subnets
    - Only Those who have Certain IP Addresses
    - Only Those who have Certain User Accounts
    - A Combination of the Above
  - Same Parameters in VPN Remote Access Policy
    - As Those You can Apply to a RAS Server

Systems Security Management

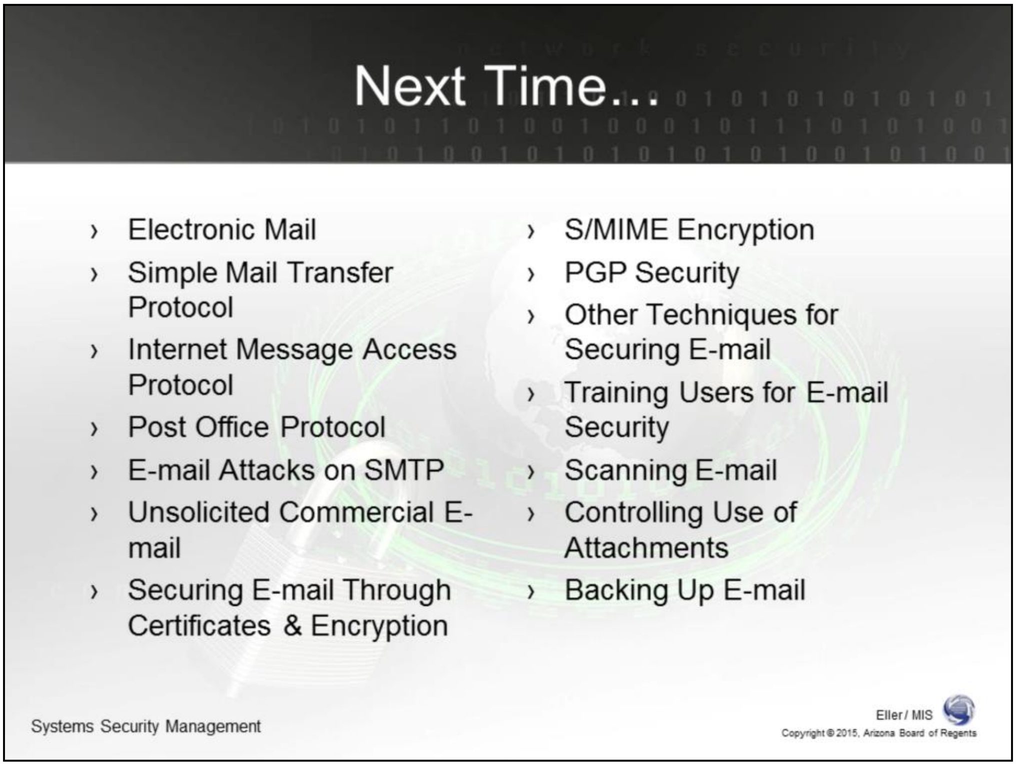
Eller / MIS

Security on a Virtual Private Network

Using RAS, a SysAdmin can configure the Windows Server to act as a VPN server for remote access. When configuring the VPN, the server can setup some additional remote access policies in order to help control access. These policies include:

- Only Clients on Certain Subnets
- Only Those who have Certain IP Addresses
- Only Those who have Certain User Accounts
- A Combination of the Above

Finally, the parameters in VPN remote access policy are the same policies as those you can apply to a RAS server.



Next Time…

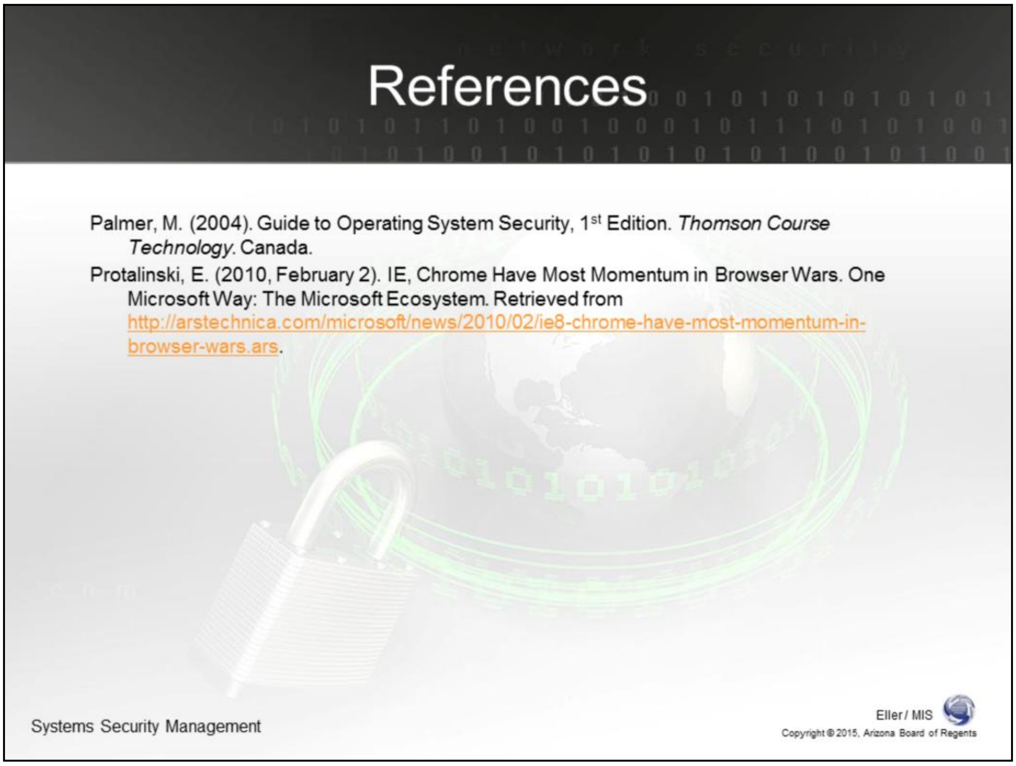
- Electronic Mail
- Simple Mail Transfer Protocol
- Internet Message Access Protocol
- Post Office Protocol
- E-mail Attacks on SMTP
- Unsolicited Commercial E-mail
- Securing E-mail Through Certificates & Encryption
- S/MIME Encryption
- PGP Security
- Other Techniques for Securing E-mail
- Training Users for E-mail Security
- Scanning E-mail
- Controlling Use of Attachments
- Backing Up E-mail

Systems Security Management

Eller / MIS

In the next module we will discuss E-mail Security, including:

- Electronic Mail
- Simple Mail Transfer Protocol
- Internet Message Access Protocol
- Post Office Protocol
- E-mail Attacks on SMTP
- Unsolicited Commercial E-mail
- Securing E-mail Through Certificates & Encryption
- S/MIME Encryption
- PGP Security
- Other Techniques for Securing E-mail
- Training Users for E-mail Security
- Scanning E-mail
- Controlling Use of Attachments
- Backing Up E-mail



References

Palmer, M. (2004). Guide to Operating System Security, 1st Edition. *Thomson Course Technology.* Canada.

Protalinski, E. (2010, February 2). IE, Chrome Have Most Momentum in Browser Wars. One Microsoft Way: The Microsoft Ecosystem. Retrieved from http://arstechnica.com/microsoft/news/2010/02/ie8-chrome-have-most-momentum-in-browser-wars.ars.