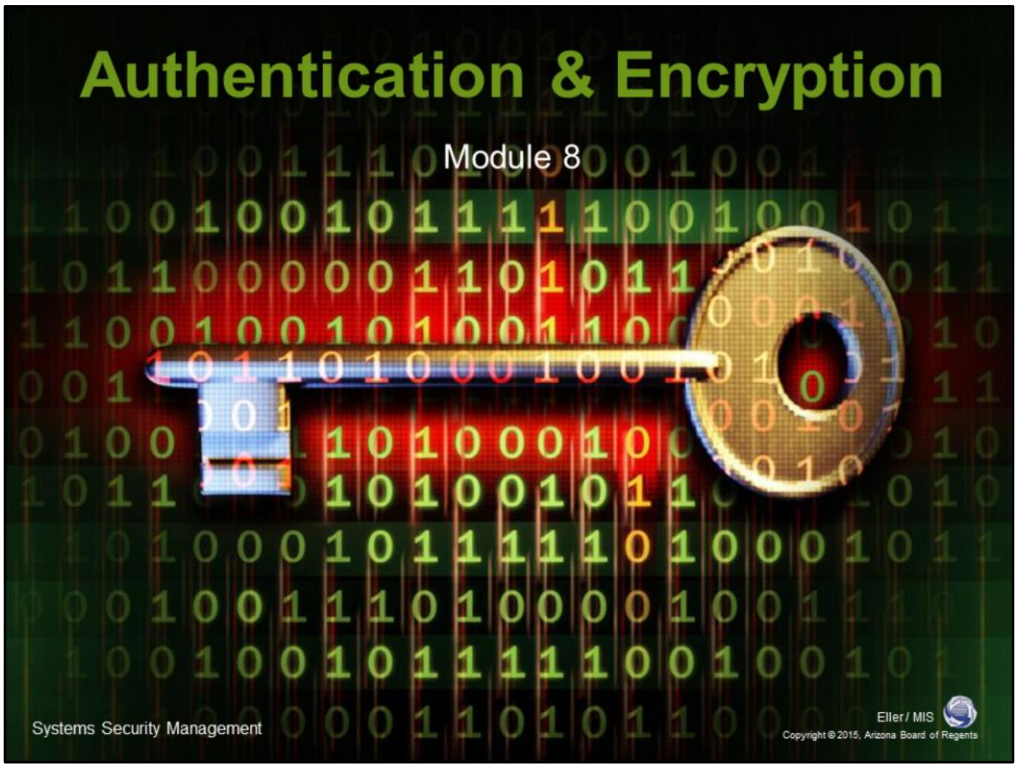
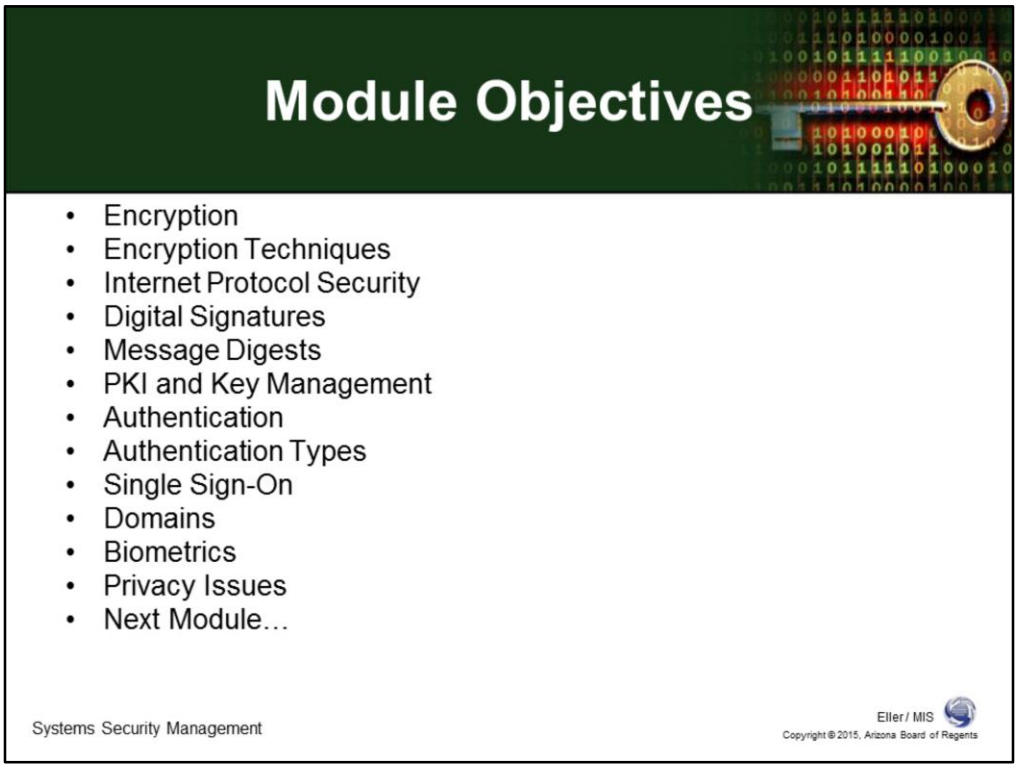
Authentication & Encryption

Module 8



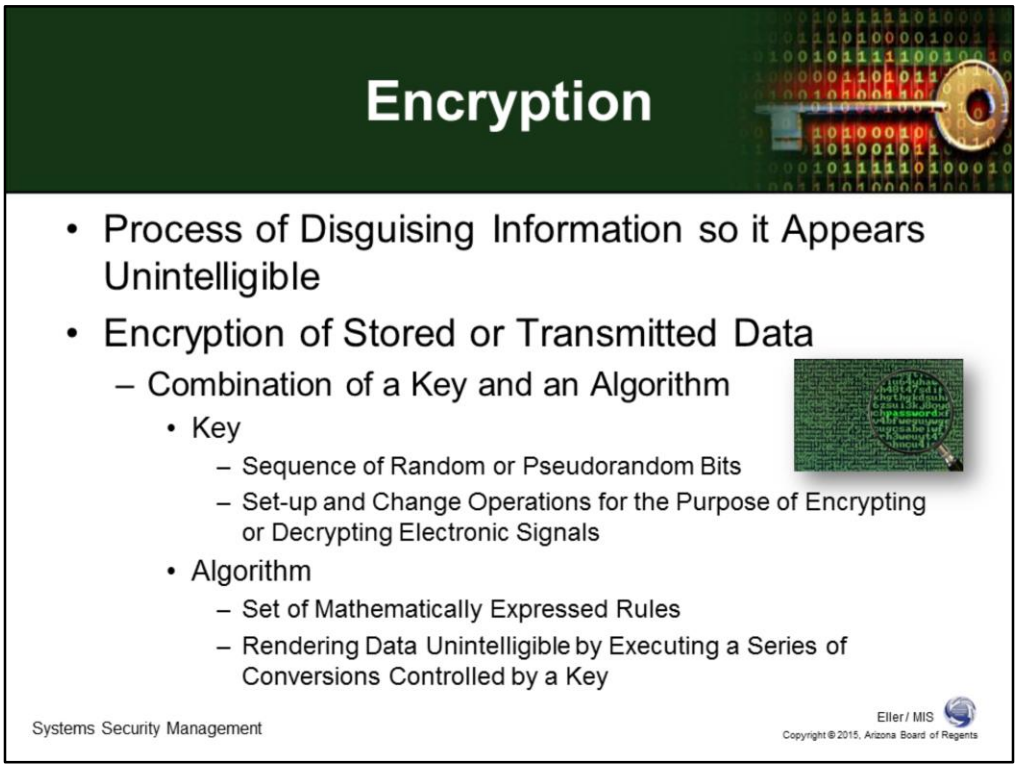
Systems Security Management

Eller / MIS



At the end of the module, you should have a better understanding of:

- Encryption and Encryption Techniques
- Internet Protocol Security
- Digital Signatures
- Message Digests
- PKI and Key Management
- Authentication and Authentication Types
- Single Sign-On
- Domains
- Biometrics
- Privacy Issues

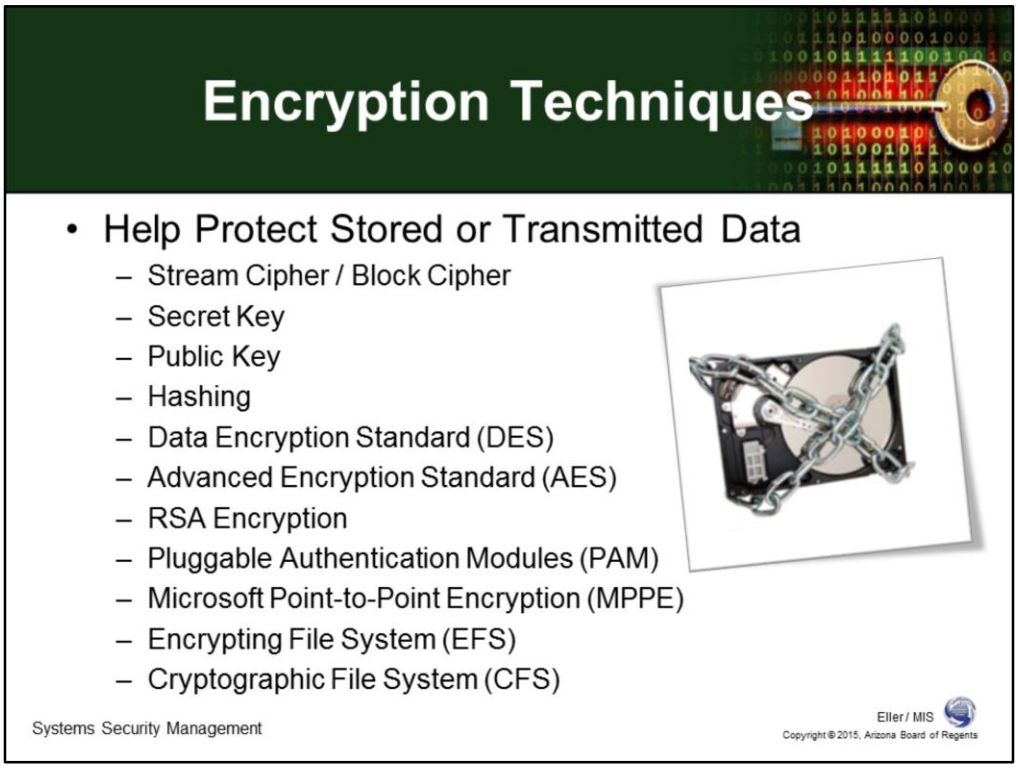


Encryption

Encryption is the process of disguising information so it appears unintelligible. Encryption can be used to store data or during the transmission of data. In order to accomplish this and make it so the data is not irretrievably lost, encryption consists of a key and an algorithm.

A key is a sequence of random or pseudorandom bits that are used for the purpose of encrypting and decrypting electronic signals.

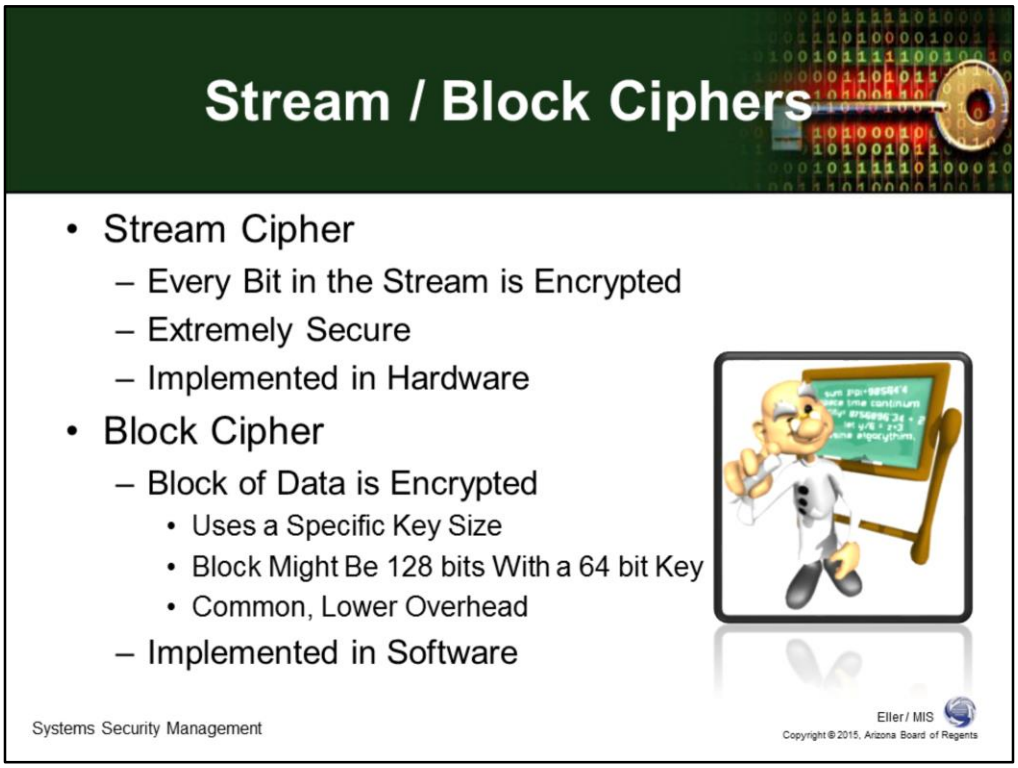
An algorithm is a set of mathematically expressed rules that allows for data to be rendered unintelligible by executing a series of data conversions controlled by a key.



Encryption Techniques

There are many different encryption techniques available to choose from, some more secure than others. In this module we will be looking at:

- Stream Cipher / Block Cipher
- Secret Key
- Public Key
- Hashing
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- RSA Encryption
- Pluggable Authentication Modules (PAM)
- Microsoft Point-to-Point Encryption (MPPE)
- Encrypting File System (EFS)
- Cryptographic File System (CFS)



Stream/Block Ciphers

A stream cipher is an encryption method where every single bit in the stream is encrypted. This is accomplished by combining a pseudorandom cipher bit stream with the plain text bit by means of an exclusive OR (XOR) operation. Stream ciphers operate at a higher speed than block ciphers and are well suited for implementation in hardware. Stream ciphers are commonly used for encrypted wireless traffic where the stream length is unknown.

Block ciphers, on the other hand, encrypt data in blocks using a specific key size. For example, the block might contain 128 bits and use a 64-bit key. This is a much more common cipher than steam ciphers simply because they involve much less overhead to encrypt and decrypt and are easily implemented in software.

Secret Key

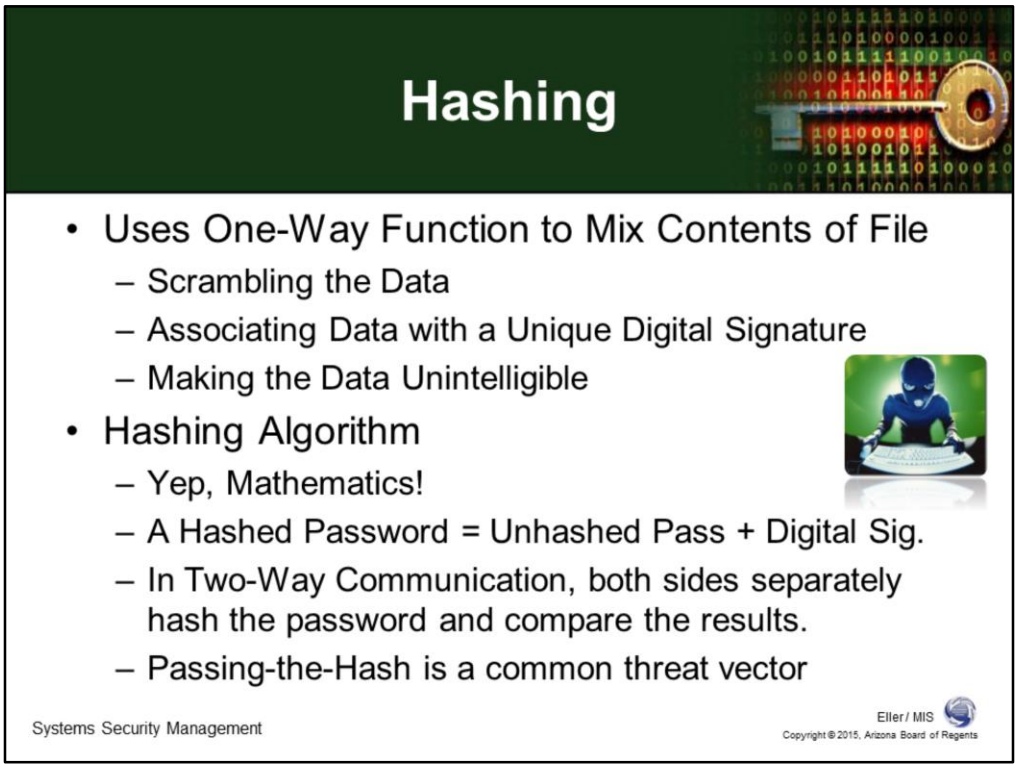
Secret Key encryption takes its encryption key and keeps it a secret from public access, particularly over a network connection. The same key is then used to both encrypt and decrypt the data. This is referred to as symmetrical encryption and the process is purposely kept simple. When using a secret key, both the source and the target systems have the same key.

The disadvantages to using a secret key is that both the source and the target must go to great lengths to keep the key secret. The key must be transmitted out-of-band in order to maintain security. If a message is sent with the key attached to it, anyone who intercepts the message has both the cipher text and the key to decrypt it.

Private Key

Private key encryption makes use of two keys, a private key and a public key. The public key can be freely transmitted over a network, and private keys are used by the sender and receiver. The private key is never shared over an open network, so it remains secure. In this scenario, one private key will encrypt while the other will decrypt. This is referred to as asymmetrical encryption.

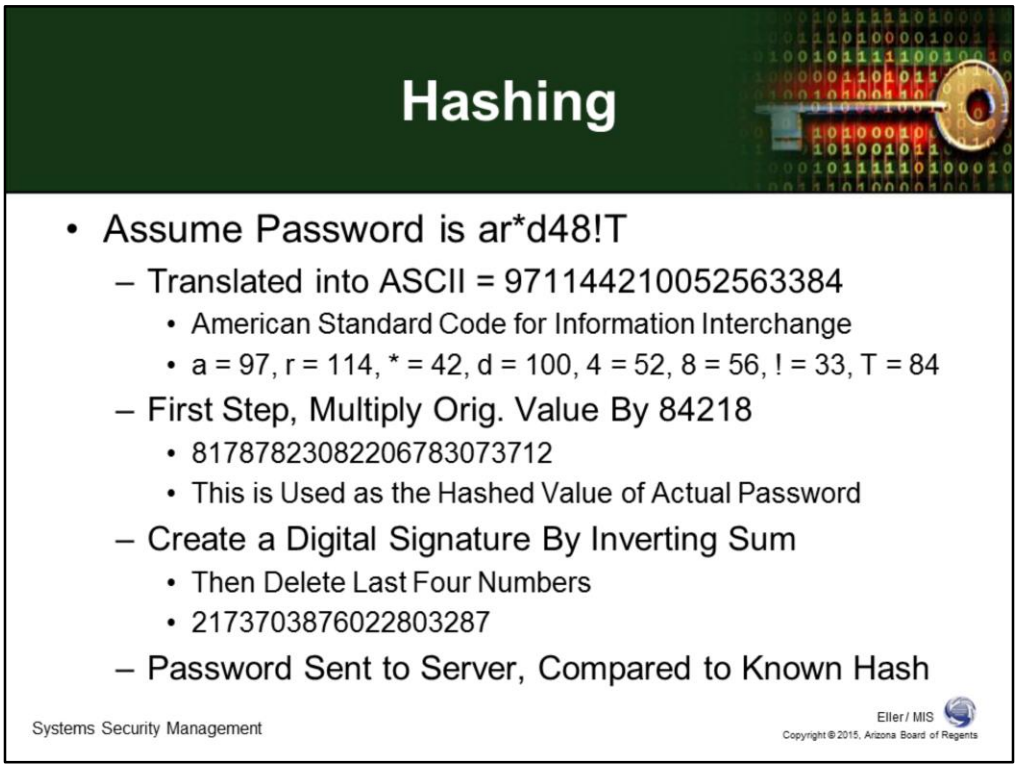
So, for example, computer user A (Bob) wants to send an encrypted file to computer user B (Joe). Bob (A) will request and obtain Joe's (B) public key. Bob (A) will then use his own private key to create a digital signature. Taking that digital signature, Bob (A) encrypts the file with Joe's (B) public key. Joe (B) then decrypts the file using his own private key. Then in order to verify the file is authentic, Joe (B) requests and obtains Bob's (A) public key in order to authenticate the digital signature.



Hashing

Hashing is an encryption technique that uses a one-way function to mix up the contents of a file. This scrambles the data, associating it with a unique digital signature, making the data unintelligible.

Hashing uses an algorithm in order to determine how to scramble the data, so yep, it uses mathematics! When using hashing, a hashed password is a combination of the unhashed password plus a digital signature. In a two-way communication using hashing, both parties will independently hash the password and then compare the results, if the hash matches, a session is formed. Unfortunately, an attack known as passing-the-hash is a very common threat vector in this scenario, where an attacker has a copy of the user's hash and passes it to the server, establishing a session without needing to know the user's password.

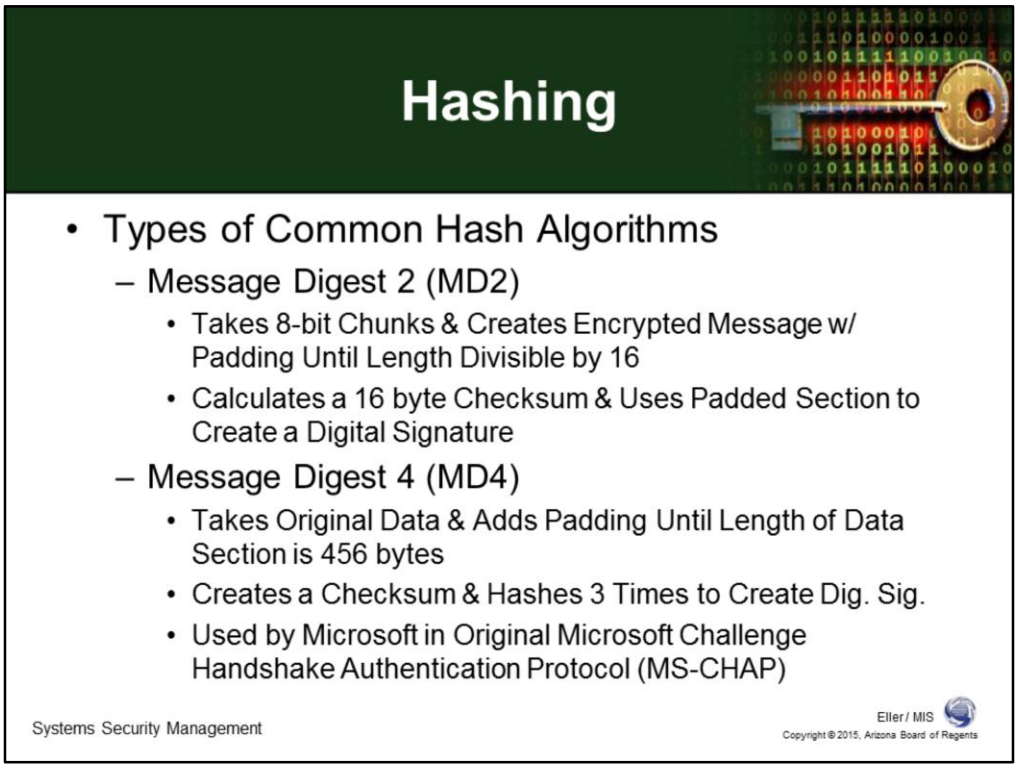


Hashing (continued)

Let's take a look at this example of hashing. Assume the password we want to hash is ar*d48!T. Translated into ASCII (American Standard Code for Information Interchange) code, this password will become 971144210052563384. In this example, a = 97, r = 114, * = 42, d = 100, 4 = 52, 8 = 56, ! = 33, and T = 84.

The first step to hashing this password is to multiply that original value by 84,218. This will reveal a string of numbers 81787823082206783073712, and is used as the hashed value of the actual password. Next a digital signature of the hashed value is created by inverting the value just calculated and removing the last four numbers. So, the signature would be 2173703876022803287. Now the hashed password is sent to the server and compared to the known hash.

Take note that this is just a very simple example of a hashed password. Actual hash calculations are much more complex.



Hashing (continued)

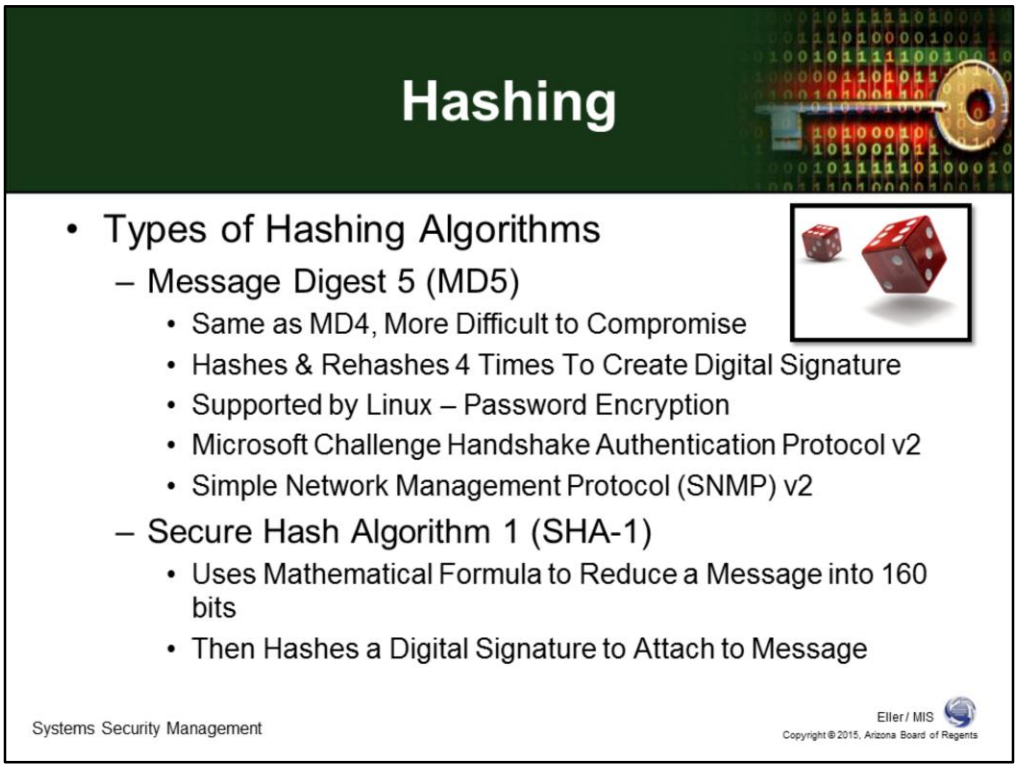
There are several common types of hash algorithms, including:

Message Digest 2 (MD2)

The MD2 hash takes 8-bit chunks out of a file or password and creates an encrypted message with extra padding until the total length of the hash is divisible by 16. MD2 then calculates a 16 byte checksum and uses the padded section to create a digital signature.

Message Digest 4 (MD4)

The MD4 hash takes the original data and adds padding until the length of the data section is 456 bytes. MD4 then creates a checksum and hashes the value three times to create the digital signature. MD4 was used by Microsoft in the original Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).



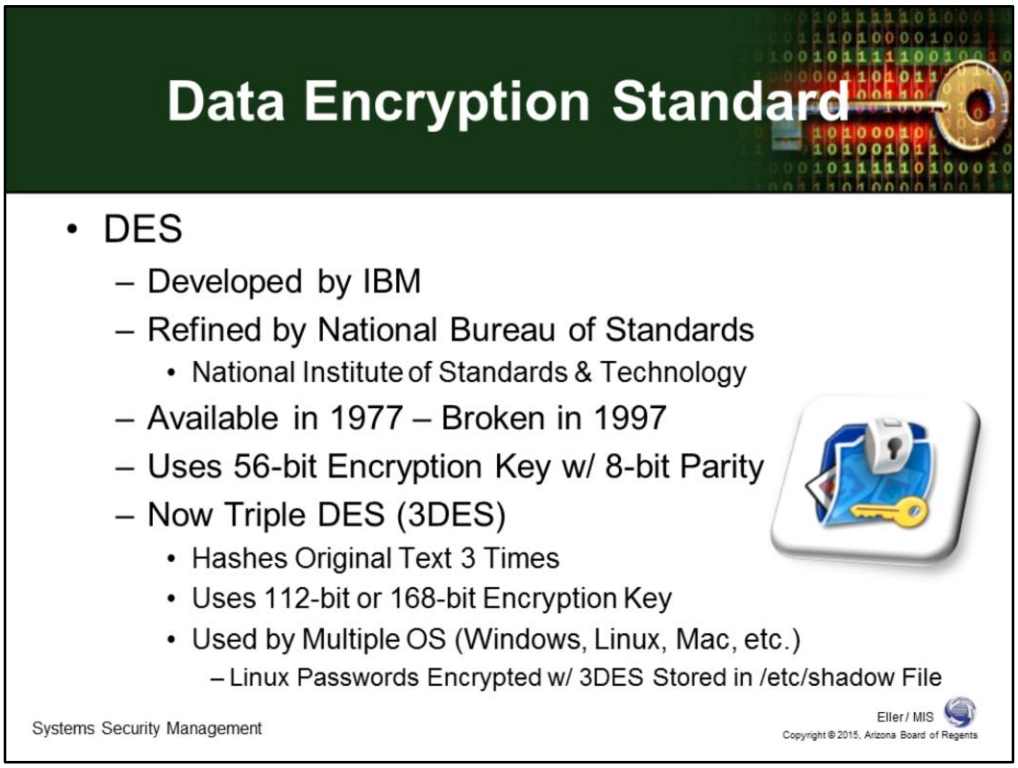
Hashing (continued)

Message Digest 5 (MD5)

MD5 uses the same algorithm as MD4; however, it is much more difficult to compromise. This is because MD5 hashes and rehashes four times to create the digital signature. MD5 is supported by Linux for password encryption. It is also supported by Microsoft for the Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2). In addition, MD5 is used by the Simple Network Management Protocol (SNMP) version 2 for communicating with network devices.

Secure Hash Algorithm 1 (SHA-1)

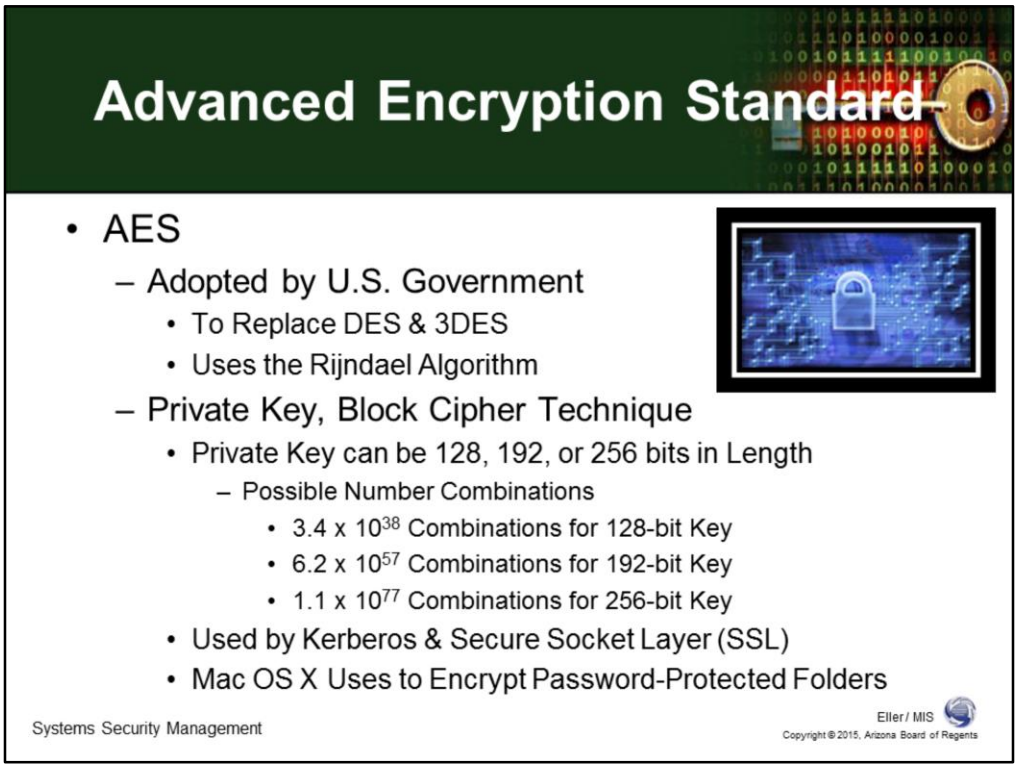
SHA-1 uses a mathematical formula to reduce a message into 160 bits, then hashes a digital signature to attach to the message.



Data Encryption Standard

The Data Encryption Standard, or DES, was developed by IBM and later refined by the National Bureau of Standards in the National Institute of Standards and Technology. DES was made available in 1977, but was ultimately broken in 1997, so it took 20 years for someone to crack the encryption employed with DES. DES used a 56-bit encryption key with an 8-bit parity (error correction) for encrypting files.

Since DES was broken in 1997, a new version emerged and is currently being used, called Triple DES, or 3DES. 3DES hashes the original text three times using a 112-bit or 168-bit encryption key. 3DES is used by multiple operating systems, including Windows, Linux, and Mac OS X. Linux passwords are encrypted using 3DES and stored in the /etc/shadow file.



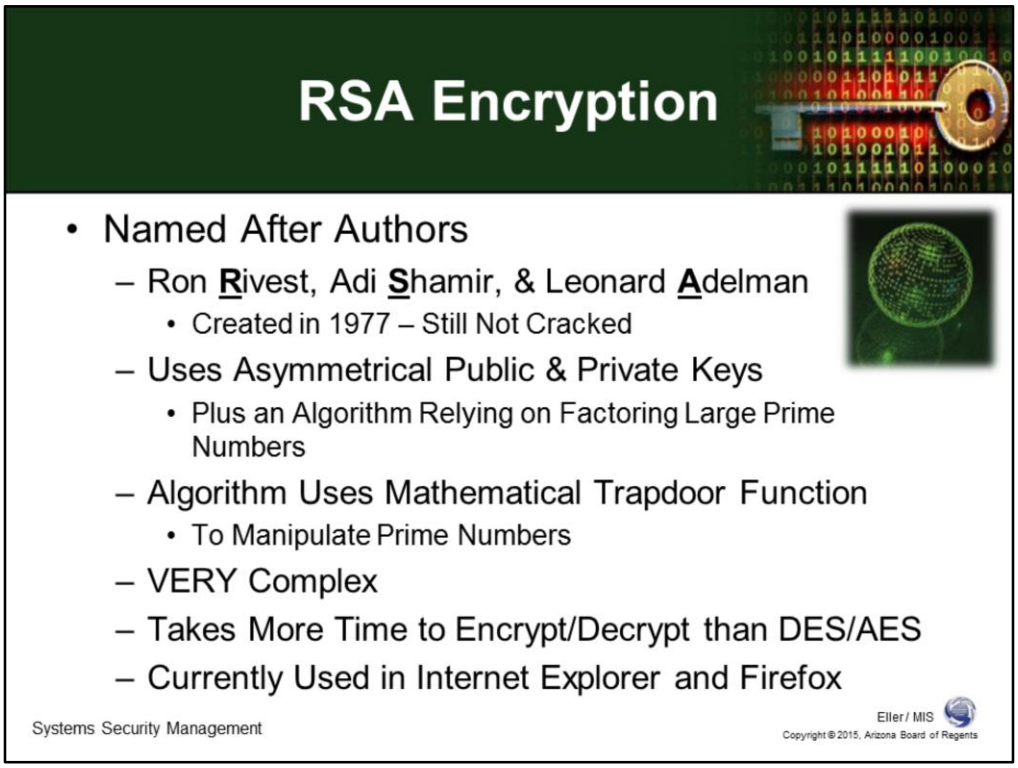
Advanced Encryption Standard

The Advanced Encryption Standard, or AES, was adopted by the United States Government in order to replace DES and 3DES. AES uses the Rijndael algorithm to encrypt files.

In general AES uses a private key, block cipher technique for encryption. The private key can be 128, 192, or 256-bits in length. Depending on the size of the key will determine the possible number combinations required in order to crack the algorithm. To give you an idea of how powerful AES is, consider this:

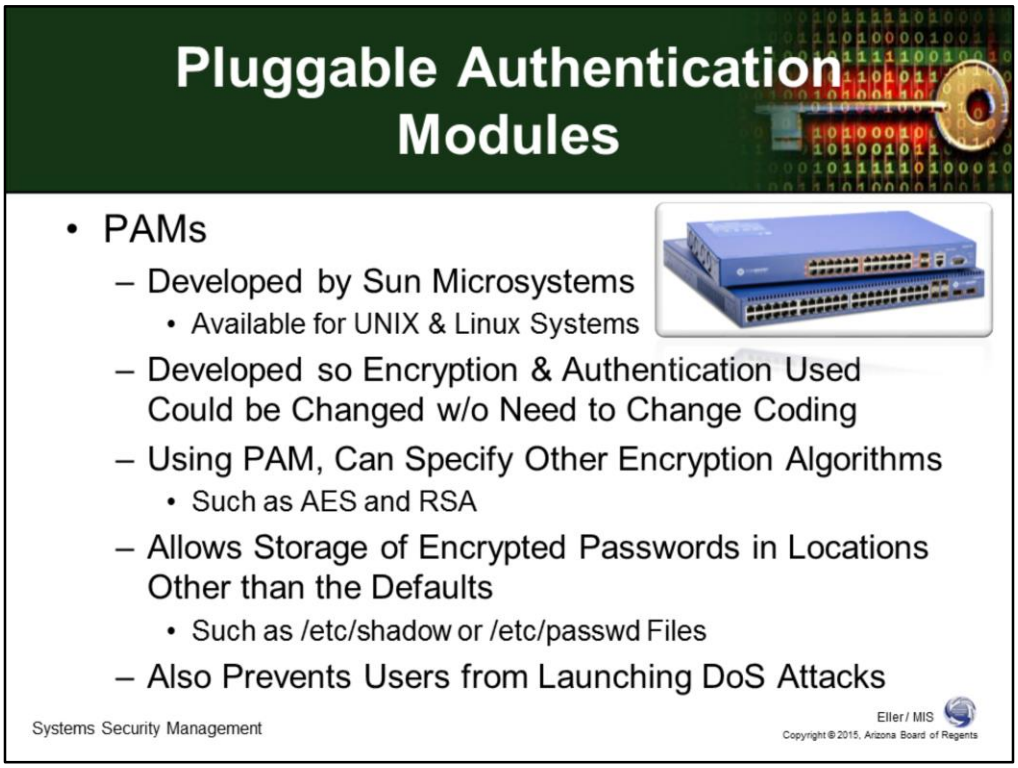
- 3.4×10^{38} Combinations for 128-bit Key
- 6.2×10^{57} Combinations for 192-bit Key
- 1.1×10^{77} Combinations for 256-bit Key

AES is also used by Kerberos and the Secure Sockets Layer (SSL) authentication techniques. In addition, the Mac OS X uses AES to encrypt password-protected folders.



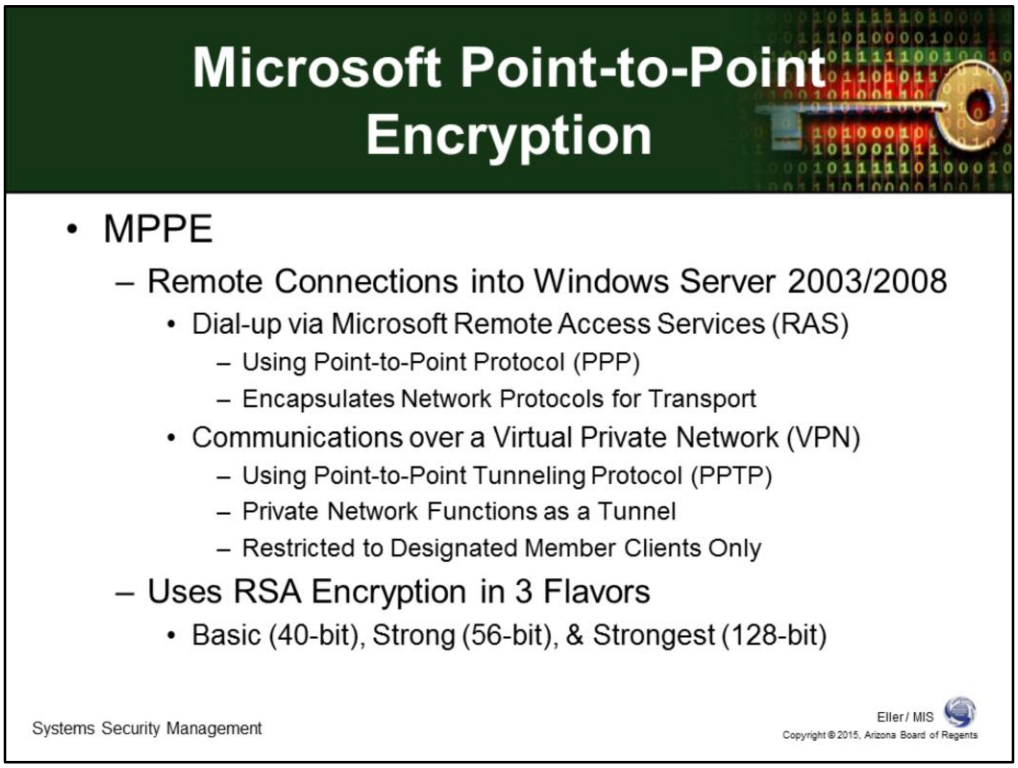
RSA Encryption

RSA encryption gets its name from its authors: Ron Rivest, Adi Shamir, and Leonard Adelman. RSA was created in 1977 and 30+ years later it still has not been cracked. RSA uses asymmetrical public and private keys plus an algorithm relying on factoring large prime numbers. The algorithm uses a mathematical trapdoor function to manipulate prime numbers, and because of this it is a very complex algorithm. RSA takes far more time to encrypt and decrypt a file than using DES or AES. Currently, RSA is commonly used in Internet Explorer and Mozilla Firefox.



Pluggable Authentication Modules

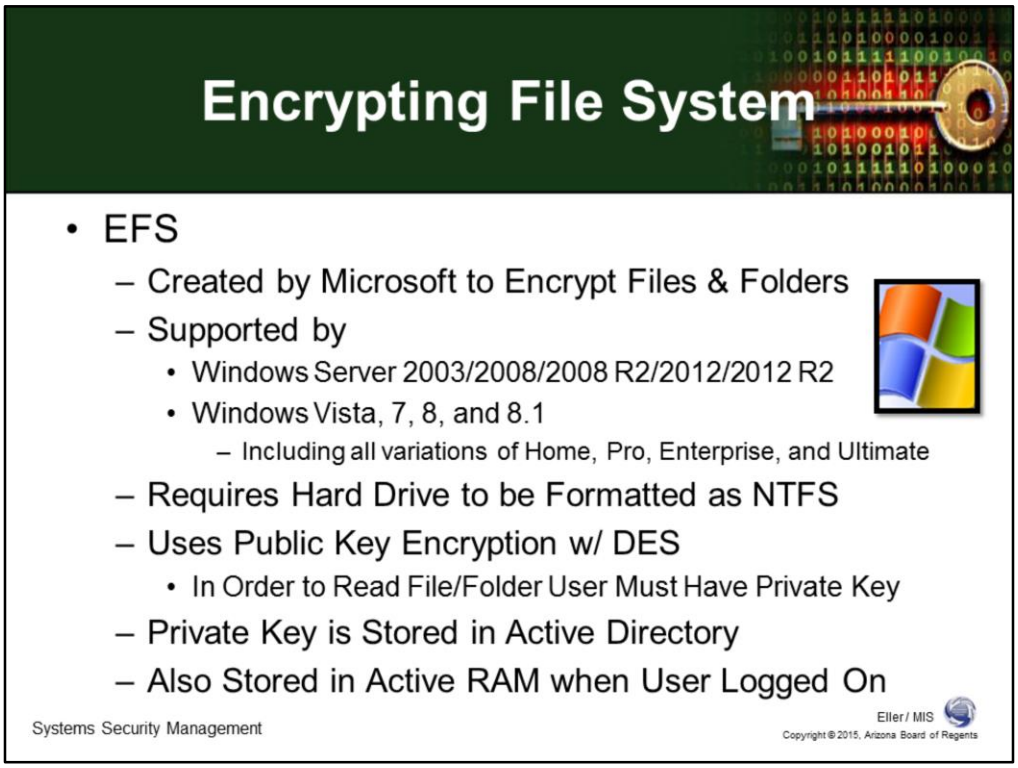
Pluggable Authentication Modules, or PAMs, are a technology that was developed by Sun Microsystems and is available for UNIX and Linux-based systems. PAMs were developed so encryption and the authentication used could be changed without the need to change system coding. Using PAMs, one can specify other encryption algorithms, including AES or RSA, and PAMs allow for the storage of encrypted passwords in locations other than the normal defaults, such as the /etc/shadow or /etc/passwd files. PAMs also help to prevent users from launching denial of service-type attacks.



Microsoft Point-to-Point Encryption

Microsoft's Point-to-Point Encryption (MPPE) was developed to be used for remote connections into Windows Server 2003 and 2008. MPPE is used when a remote user uses a dial-up connection to the server via Microsoft Remote Access Services (RAS). RAS uses the point-to-point protocol (PPP) and encapsulates entire network protocols for transport over the connection. Communications with the Windows Servers are achieved over a Virtual Private Network (VPN) using the point-to-point tunneling protocol (PPTP). This private network functions as a tunnel from the remote computer to the server through the Internet or other networks. This kind of access is restricted to designated member clients only, so the user must have an account on the server itself.

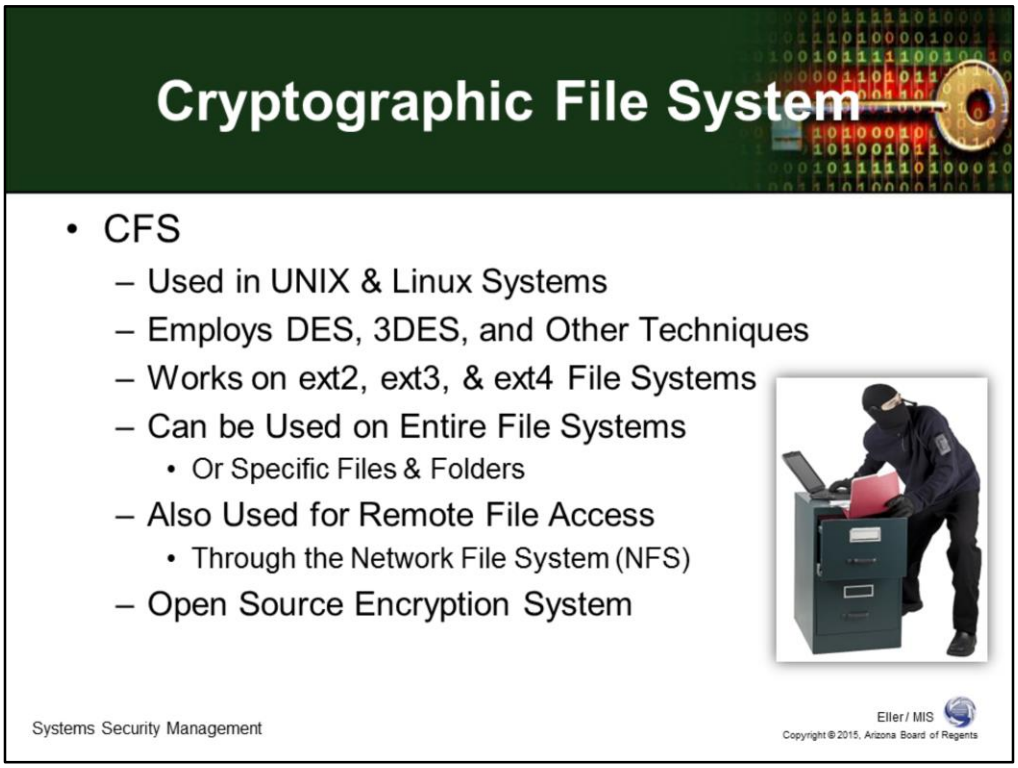
MPPE makes use of RSA encryption in three different flavors: basic (40-bit), strong (56-bit) and strongest (128-bit).



Encrypting File System

The Encrypting File System, or EFS, was created by Microsoft to allow for the encryption of files and folders on Windows servers. Currently EFS is supported by Windows Server 2003, Windows Vista (Business, Enterprise, and Ultimate), Windows 7 (Professional, Enterprise, and Ultimate), and Windows Server 2008 and 2008 R2, Windows 8 and 8.1 Pro and Enterprise editions, and Windows Server 2012. EFS requires that the hard drive you want to encrypt is formatted using the NTFS file system. We will discuss NTFS in more detail in Module 11.

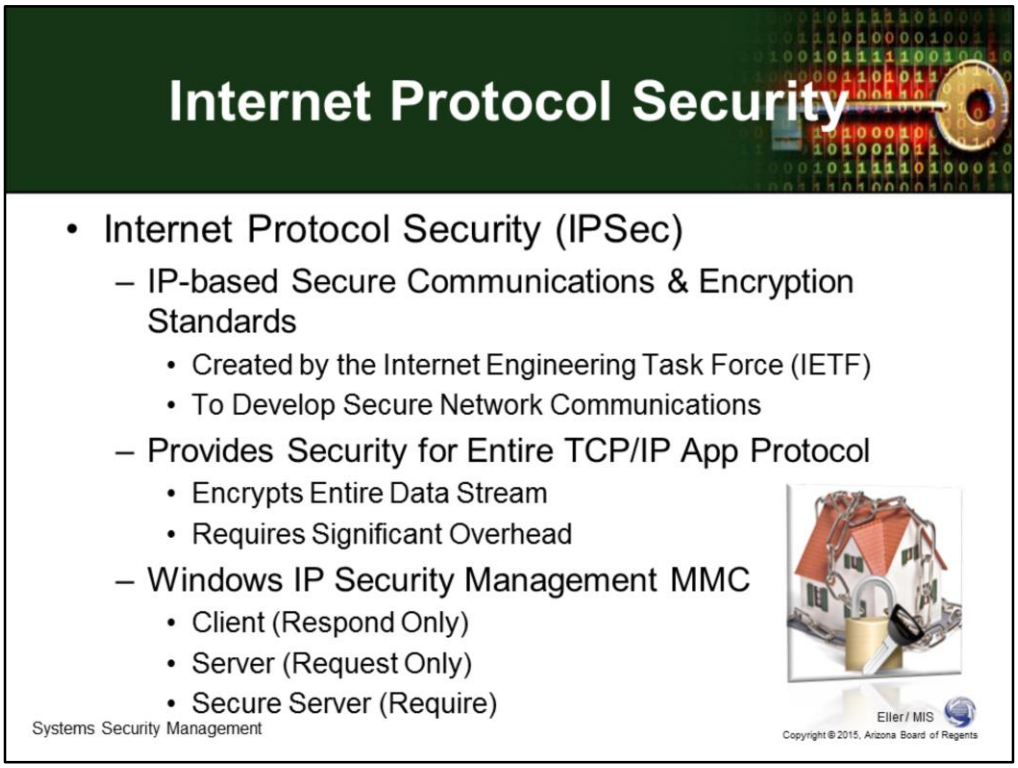
EFS uses public key encryption with DES to encrypt files and folders. In order to read the files or folders, the user must have the private key. In an Windows network, the private key is stored in Active Directory. This way if the client system fails the data can still be recovered. The private key is also stored in active memory (RAM) while the user is logged on. This is so the user can easily interact with the files while they are still encrypted.



Cryptographic File System

The Cryptographic File System, or CFS, is used on UNIX and Linux systems. CFS makes use of DES, 3DES, and other techniques for encryption and it works on the ext2, ext3, and ext4 file systems. We will discuss these file systems in more detail in Module 11.

CFS can be used to encrypt the entire file system, or just specific files or folders. CFS is also used for remote file access through the use of the Network File System (NFS). The interesting part of CFS is since it is a UNIX and Linux-based encrypting file system, CFS itself is an open source encryption system.

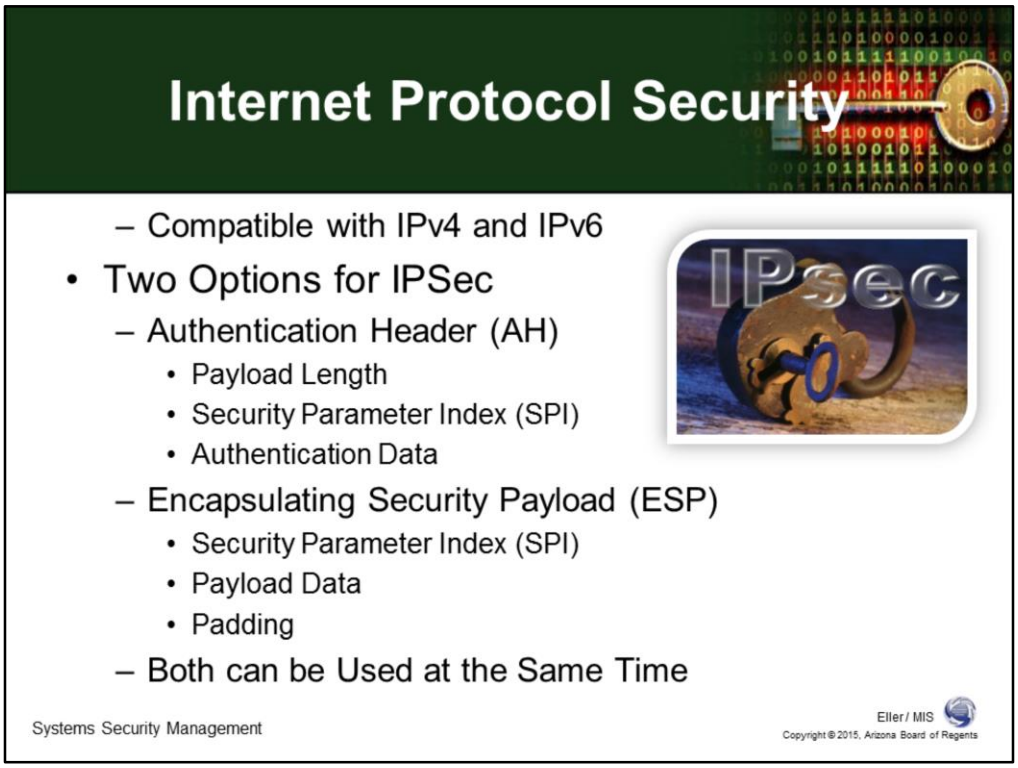


Internet Protocol Security

Internet Protocol Security (IPSec) is an IP-based secure communications and encryption standard created by the Internet Engineering Task Force (IETF). IPSec was developed in order to help secure network communications. In order to accomplish this, IPSec provides security for the entire TCP/IP application protocol. This means IPSec encrypts the entire data stream. The problem with this is that it requires significant overhead as everything sent across the network needs to be processed in order to encrypt and decrypt on either end of the communication. Imagine that process times 100 or 1000 or more and you have a significant network bottleneck.

In Windows you can enable IPSec as a means of securing communications between clients and servers. IPSec is Disabled by default; however, it can be enabled easily using one of the following three settings:

1. Client (Respond only) Means 'I will speak IPSec if you wish'.
2. Server (Request Security) Means 'I would like to speak IPSec, but if you cannot comprehend IPSec then I will speak normally.
3. Secure Server (Require Security) Means 'I will only speak with clients who understand IPSec'.



Internet Protocol Security (continued)

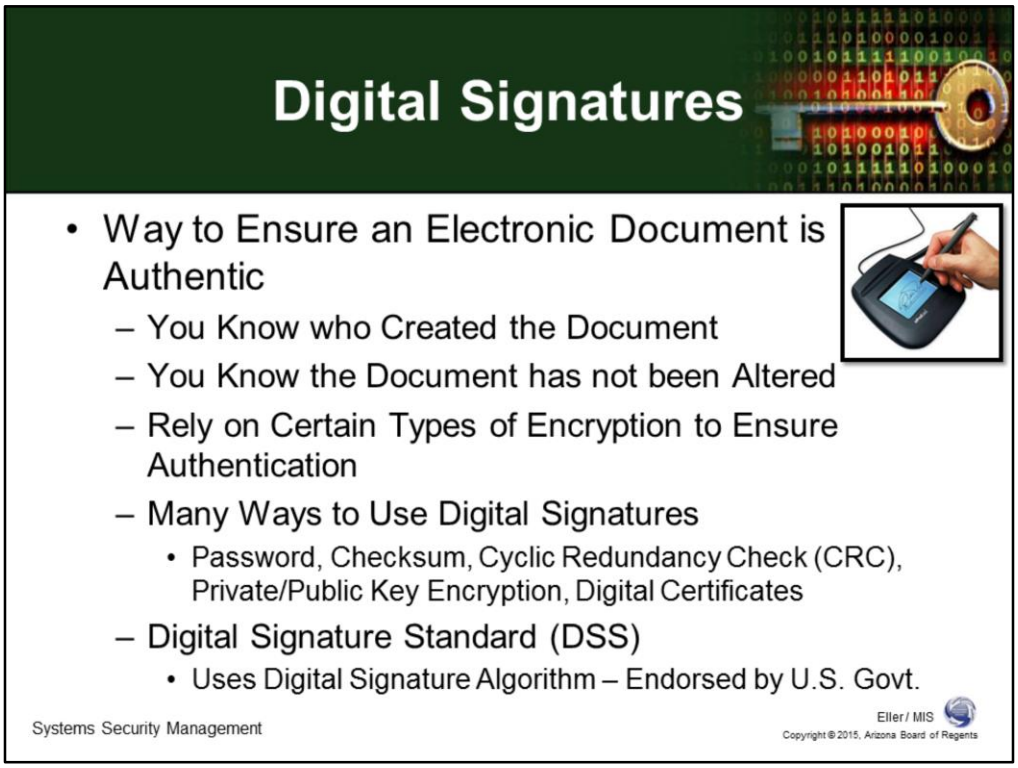
IPSec is compatible with both IP version 4 and version 6, so it can continue to be used into the near future.

There are two options when configuring IPSec: the Authentication Header (AH) and the Encapsulating Security Payload (ESP).

The Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams. The AH allows you to configure settings for payload length, the security parameter index, and authentication data, among others.

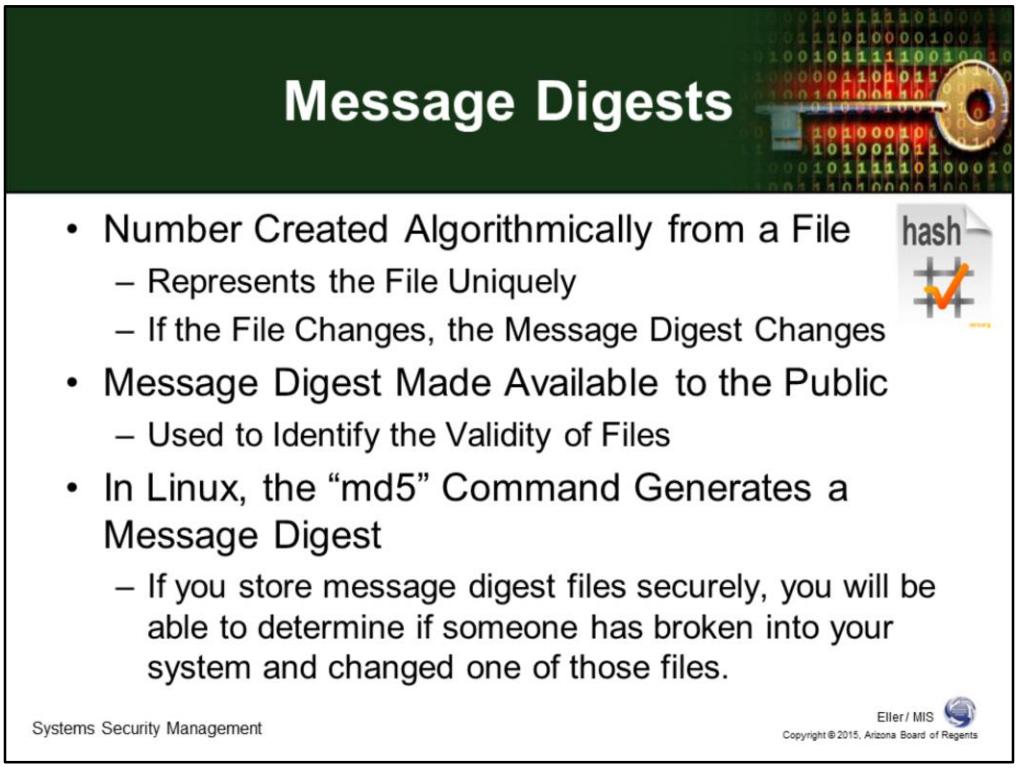
Encapsulating Security Payload (ESP) is used to provide confidentiality, data origin authentication, connectionless integrity, and limited traffic flow confidentiality. ESP allows you to configure settings for security parameter index, payload data, and padding.

It is important to note that IPSec can use both of these options at the same time to increase security.



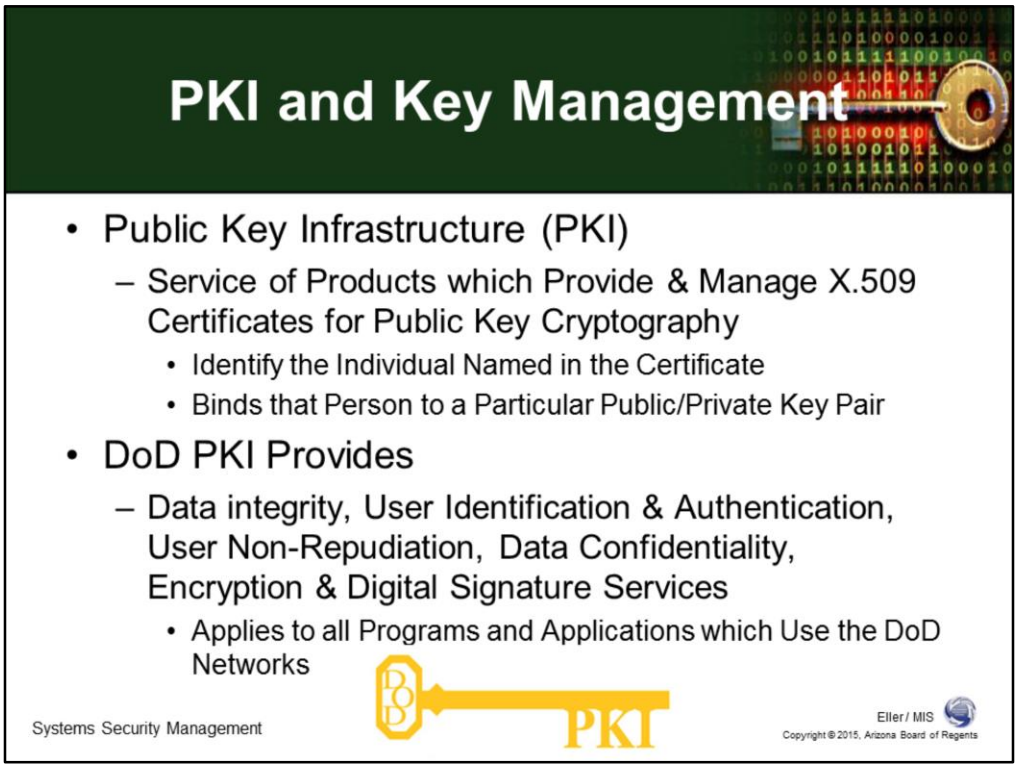
Digital Signatures

Throughout the discussion on encryption we have mentioned digital signatures several times. To officially define it, a digital signature is a way to ensure an electronic document is authentic. This authenticity is achieved because you know who created the document and you know the document has not been altered in any way during transmission. Digital Signatures will rely on certain types of encryption to help ensure proper authentication. There are many ways to use digital signatures, including passwords, checksums, cyclic redundancy checks (CRCs), private/public key encryption, and digital certificates. The Digital Signature Standard, or DSS, uses a Digital Signature algorithm that is endorsed by the U.S. Government.



Message Digests

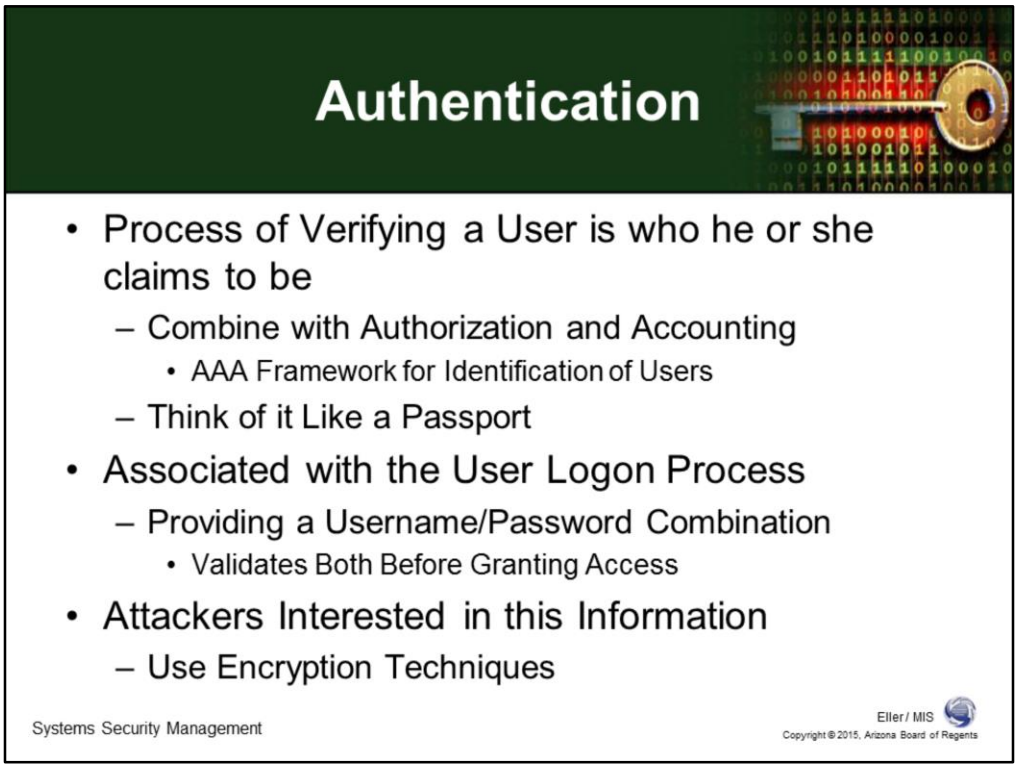
We touched upon message digests when we discussed hashing; however, here we can get into a little more detail. A message digest is a number created algorithmically from a file. The message digest represents the file uniquely, so if the file changes the message digest will change with it. Message digest was made available to the public as a means of identifying the validity of files. In the Linux OS, the md5 command generates a message digest for a specific file. This way, if you store message digest files securely, you will be able to determine if someone has broken into your system and changed one of those files. This is commonly used on websites to verify download file integrity to ensure that you don't have a file that has been altered in some way, perhaps by malware or a Trojan.



PKI and Key Management

The Public Key Infrastructure, or PKI, is a service of products which provide and manage X.509 certificates used for public key cryptography. The PKI is used to identify the individual named in the certificate and binds that person to a particular public/private key pair.

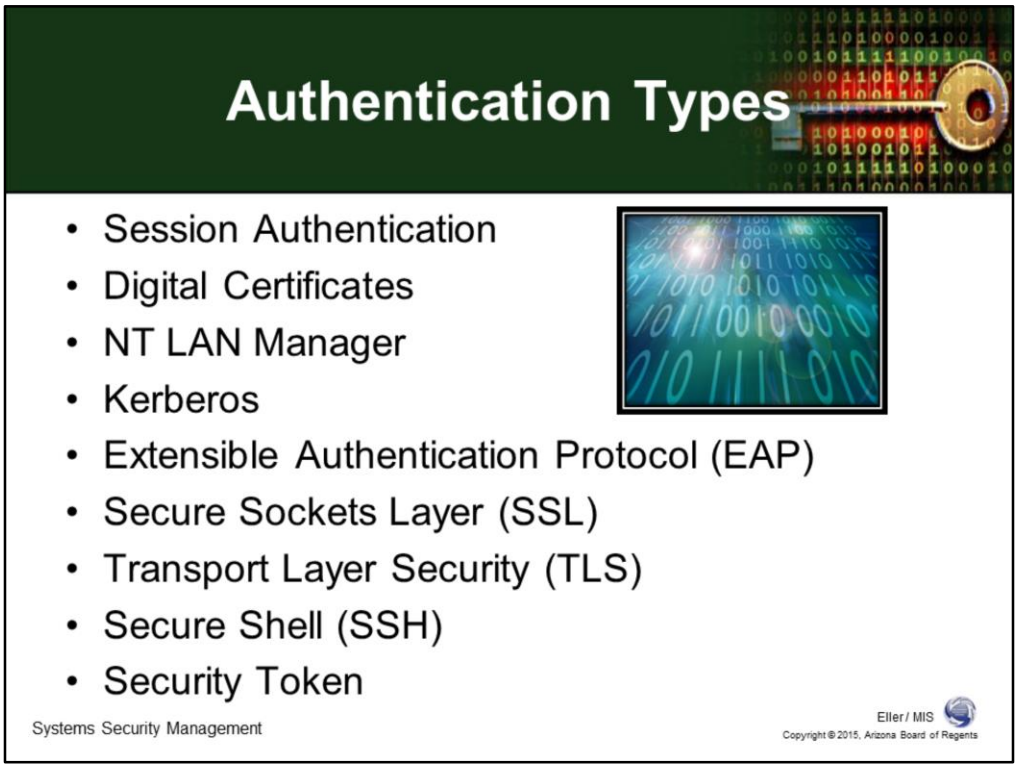
The Department of Defense operates its own PKI, which provides data integrity, user identification and authentication, user non-repudation, data confidentiality, encryption, and digital signature services. The DoD PKI applies to all programs and applications which use DoD networks.



Authentication

Authentication is the process of verifying a user is who he or she claims to be. Couple this with authorization, which determines whether the user is allowed to access specific resources, and accounting, which logs access requests and whether or not they were successful, and you have the commonly used AAA framework for identification of users. Think of it as similar to the process of using a passport to enter (or leave in some cases) a country. Authentication is generally associated with the user logon process, where a user is asked to provide a username and password combination which must be validated before the user is granted access to the system.

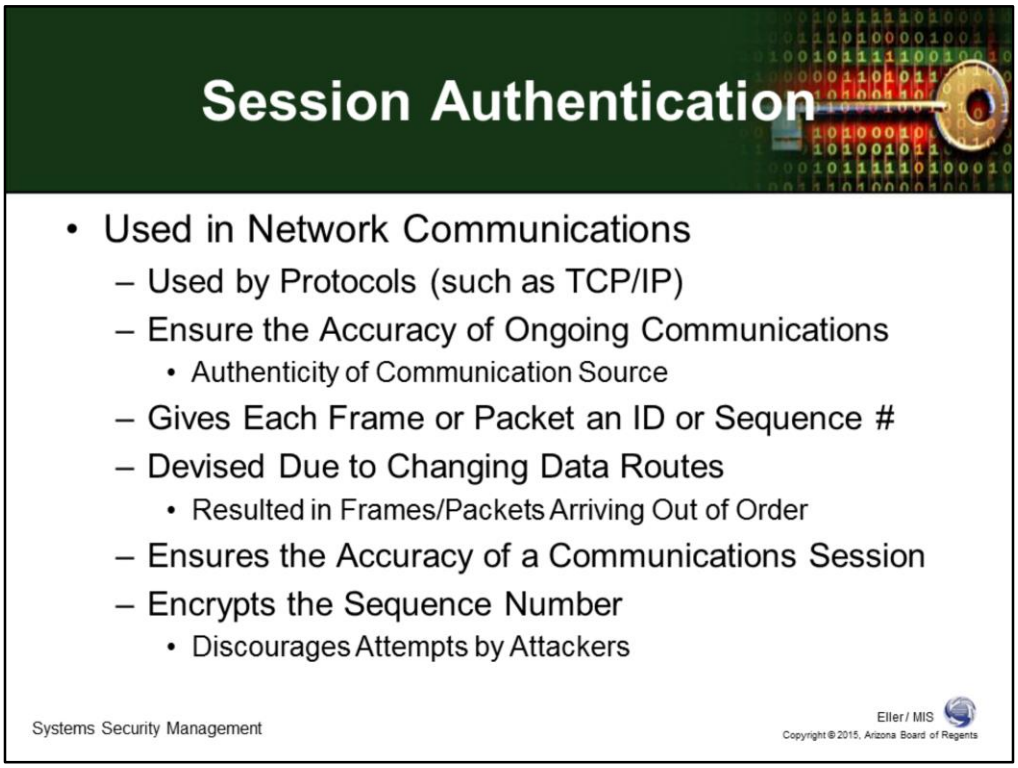
Attackers are very interested in obtaining this kind of information, so many authentication methods use different encryption techniques to try and prevent an attacker from intercepting the information. There are many different forms of authentication available to choose from.



Authentication Types

There are many different methods available for authentication, including:

- Session Authentication
- Digital Certificates
- NT LAN Manager
- Kerberos
- Extensible Authentication Protocol (EAP)
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- Secure Shell (SSH)
- Security Token



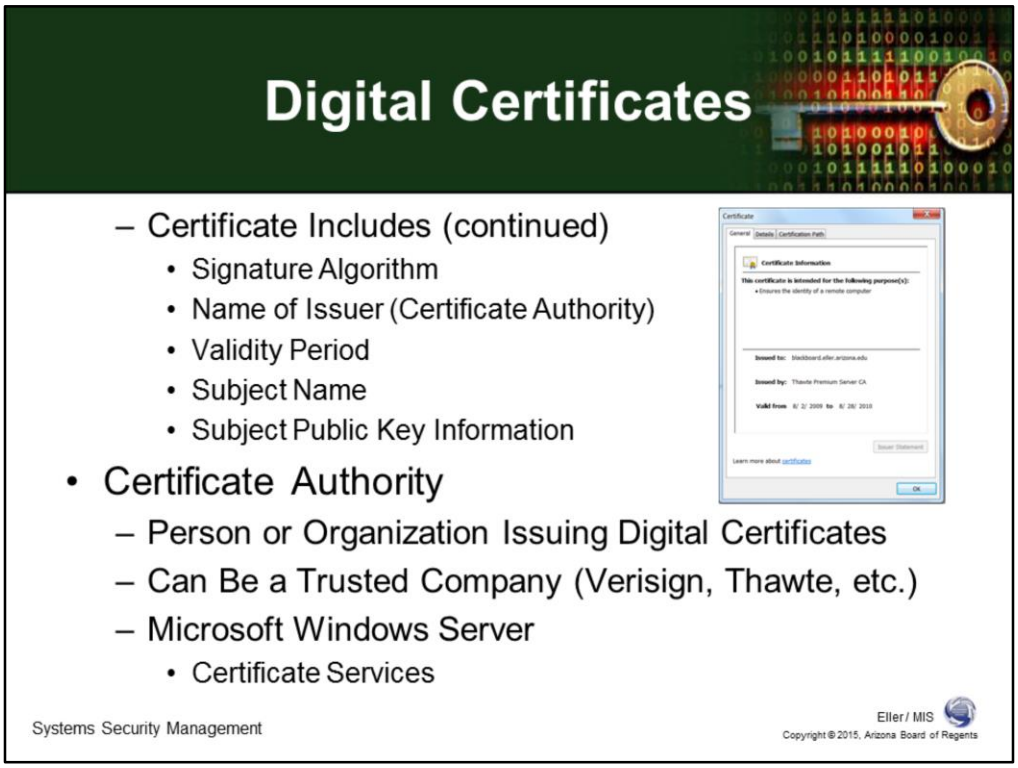
Session Authentication

Session Authentication is used in network communications protocols such as TCP/IP to ensure the accuracy of ongoing communications and the authenticity of the communication source. Session Authentication gives each network frame or packet an ID or sequence number because data routes will constantly change during a communications session. This can result in frames and packets arriving out of the proper order at the destination. These IDs or sequence numbers allow the receiving end to put them back together in order. This ensures the accuracy of a communications session, and by encrypting the sequence number, this discourages attempts by attackers to try and intercept and rebuild the data properly.

Digital Certificates

Digital Certificates provide a set of unique identifying information that is placed at the end of a file and associated with computer communication. Digital certificates are encrypted with a private key and decrypted using a public key, so they use asymmetrical encryption techniques. Digital Certificates are created in the International Organization for Standardization (ISO) X.509 format. Certificates will include the following information:

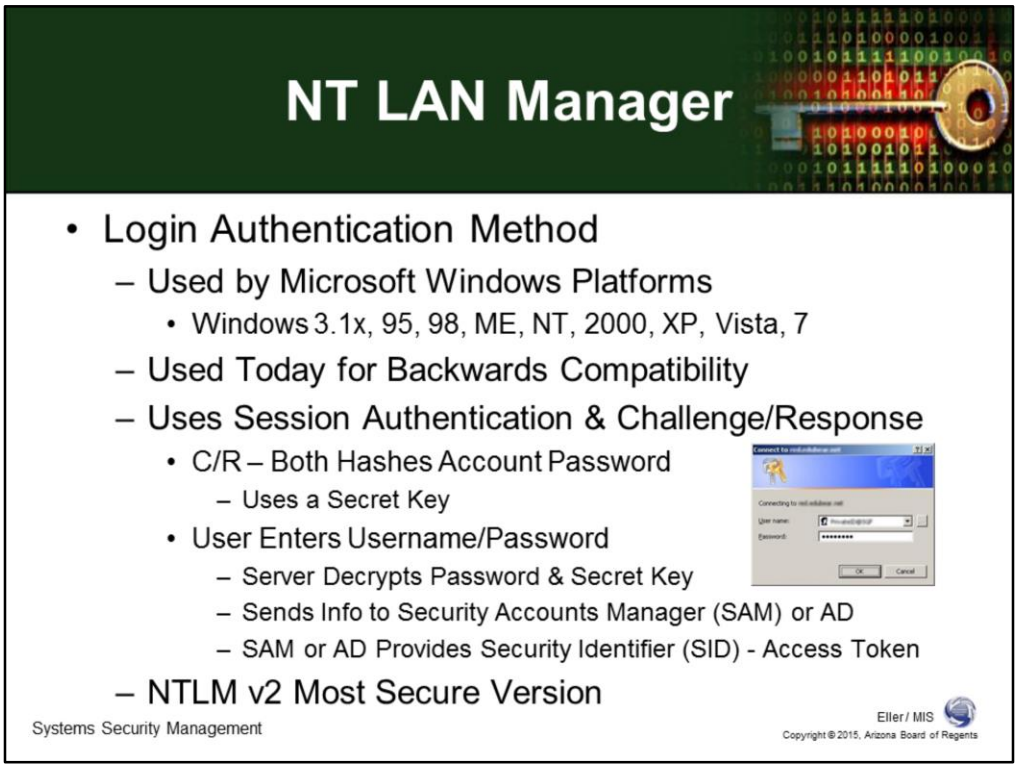
- Version of X.509 Standard Used
- Certificate Serial Number



Digital Certificates (continued)

- Signature Algorithm
- Name of Issuer (Certificate Authority)
- Validity Period
- Subject Name
- Subject Public Key Information

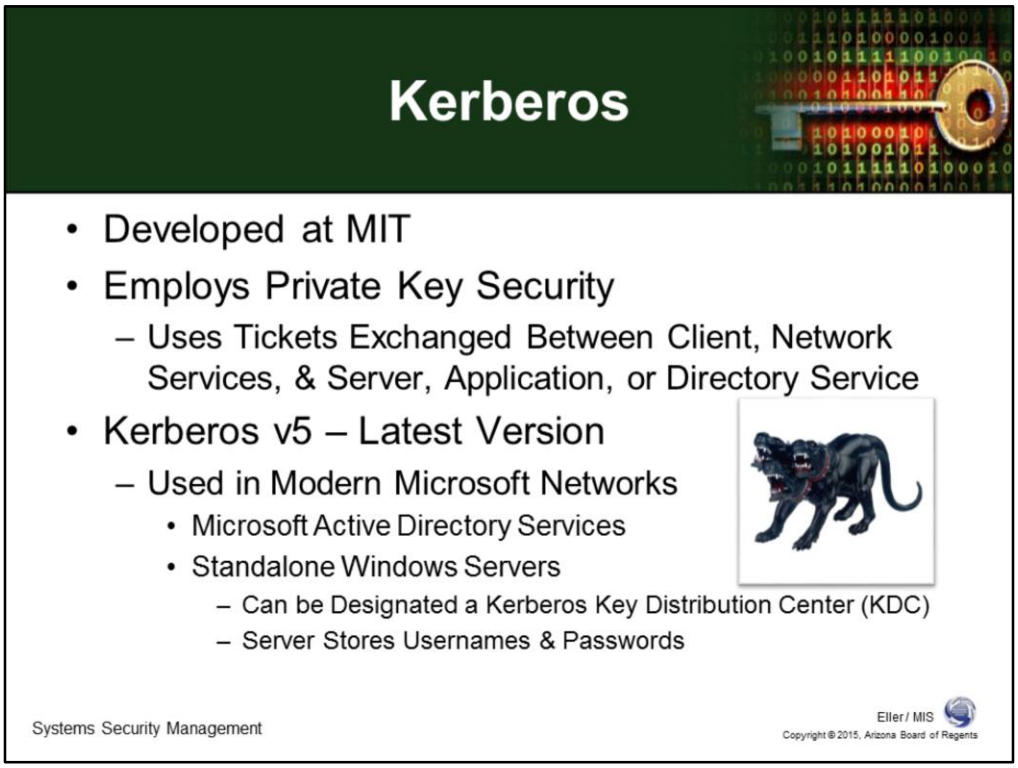
A Certificate Authority (CA) is a person or organization that issues digital certificates. This can be a trusted company such as Verisign or Thawte; however, it can also be a local server in the organization. Microsoft's Windows Server offers Certificate Services for this purpose.



NT LAN Manager

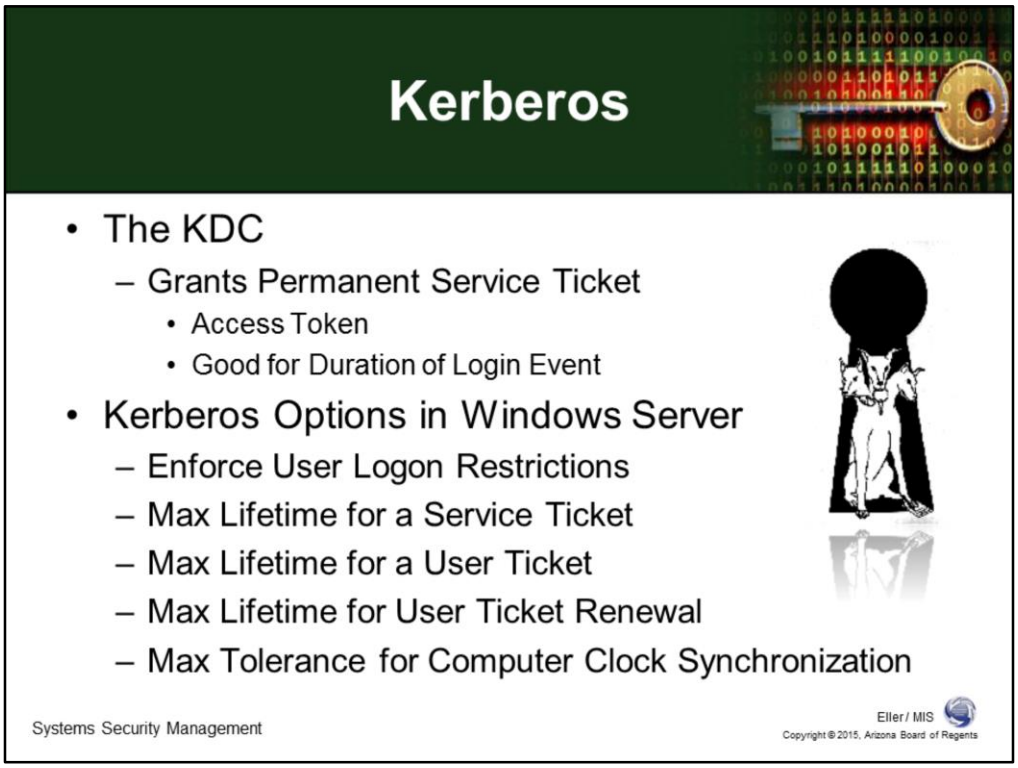
The NT LAN Manager (NTLM) is an authentication method supported by all versions of Windows including Windows 3.1x, 95, 98, ME, NT, 2000, XP, Vista, and Windows 7. Today the NT LAN Manager is used mostly for backwards compatibility with older versions of Windows.

NTLM uses session authentication with challenge/response. The challenge/response both hash the user's account password using a secret key. The user enters a username and password and the server decrypts the password and the secret key. The server then sends this information to the Security Accounts Manager (SAM) or Active Directory. The SAM or AD provides a security identifier (SID) access token validating the authentication attempt. The most current version (NTLM v2) is the most secure version available.



Kerberos

The Kerberos authentication protocol was developed at MIT and employs private key security using tickets exchanged between clients, network services, and the server, application, or directory service. Kerberos v5 is the latest version of the protocol and has been adopted for use in modern Microsoft networks including Microsoft Active Directory Services. Standalone Windows servers can be designated as a Kerberos Key Distribution Center (KDC), where Kerberos can store usernames and passwords.

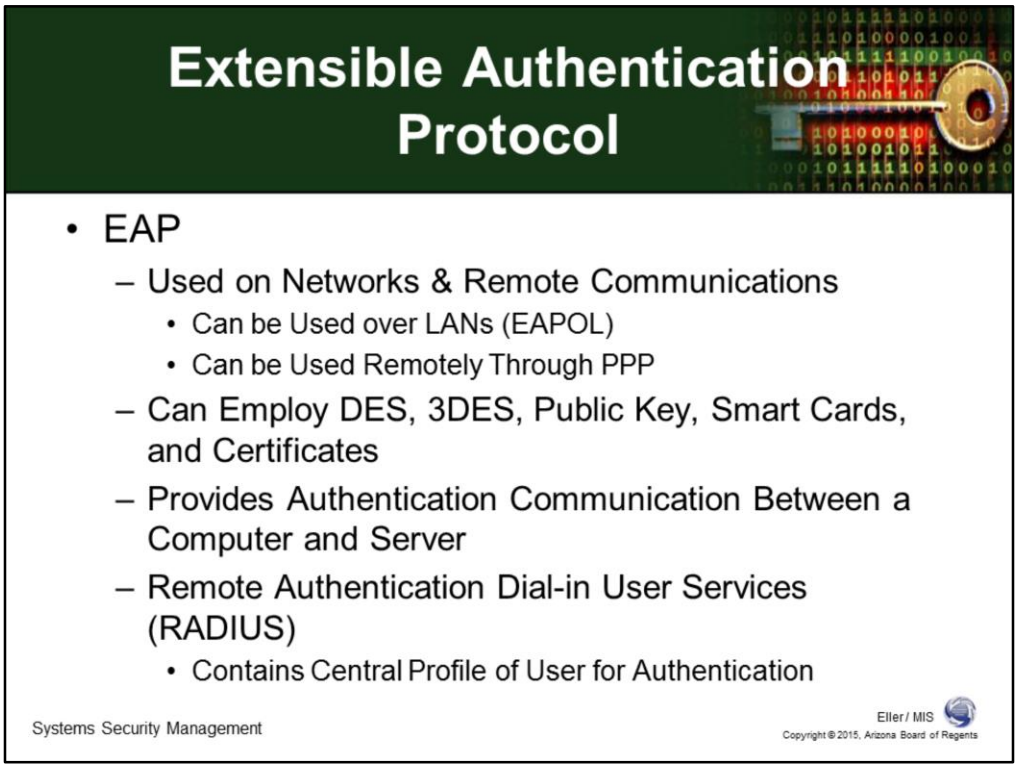


Kerberos (continued)

The Kerberos Distribution Center also grants permanent service tickets which act as access tokens and are good for the duration of a login event.

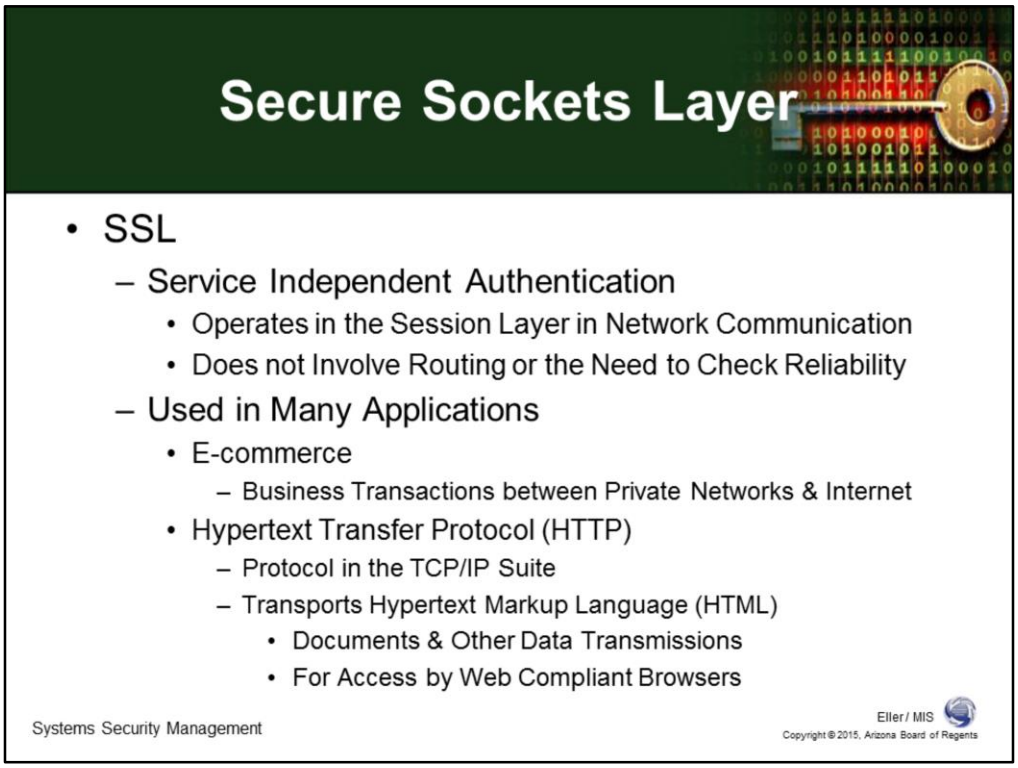
In Windows Server there are several options related to the Kerberos protocol including:

- **Enforce User Logon Restrictions** – This option enforces any restrictions that exist for a user when logged on.
- **Max Lifetime for a Service Ticket** – This option defines how long a service ticket is valid for.
- **Max Lifetime for a User Ticket** – This option defines how long a user ticket is valid for.
- **Max Lifetime for User Ticket Renewal** – This option defines how long between user ticket renewal requests.
- **Max Tolerance for Computer Clock Synchronization** – This option defines how much of a difference can exist between the clock on a client system and the Kerberos server.



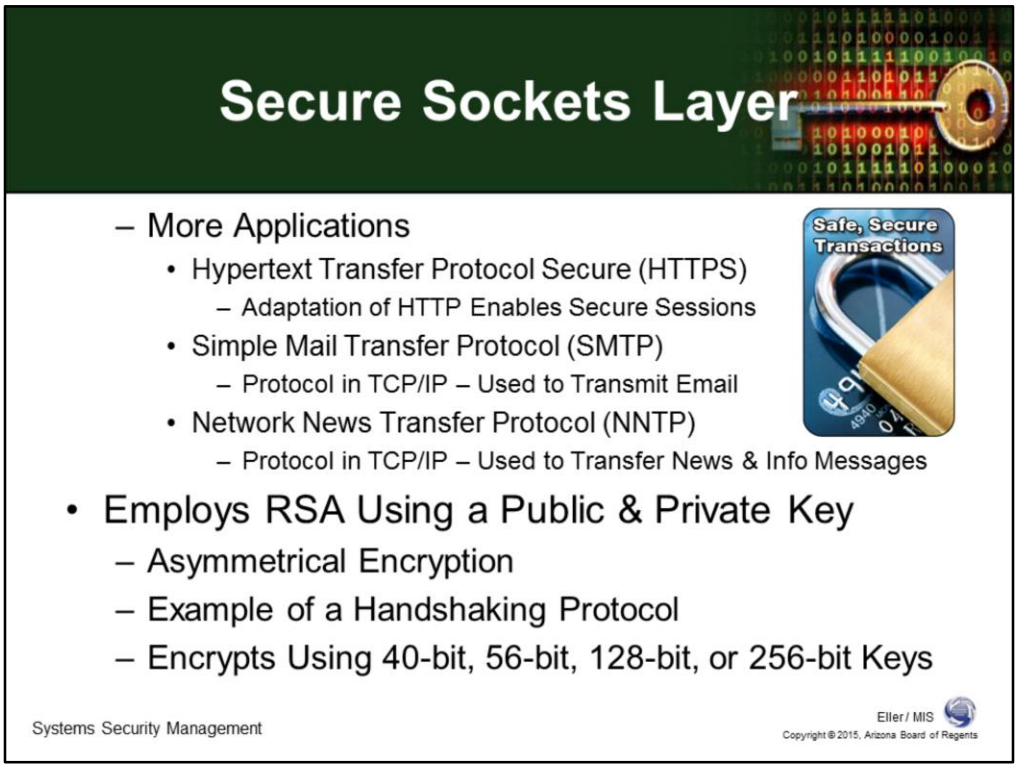
Extensible Authentication Protocol

The Extensible Authentication Protocol, or EAP, is an authentication mechanism able to be used on both networks and remote communications. EAP can be used over LANs (EAPOL) or can be used remotely through a point-to-point protocol (PPP). Because of EAP's flexibility, it can employ DES, 3DES, Public Key, Smart Cards, and Certificates for encrypted communications. EAP also provides authentication communication between a computer and server. EAP is commonly used with the Remote Authentication Dial-In User Services (or RADIUS), which contains a central profile of the user for authentication.



Secure Sockets Layer

Secure Sockets Layer (or SSL) is commonly used to secure web sites with encryption. SSL is a service independent authentication mechanism that operates in the session layer during network communications and does not involve routing or the need to check the reliability of the network connection. SSL is used in many applications, especially e-commerce applications to secure business transactions between private networks and the Internet. SSL is also a part of the Hypertext Transfer Protocol (HTTP) in the TCP/IP suite, allowing for the secure transport of the Hypertext Markup Language (HTML). This allows documents and other data transmissions to be accessed securely by web compliant browsers.

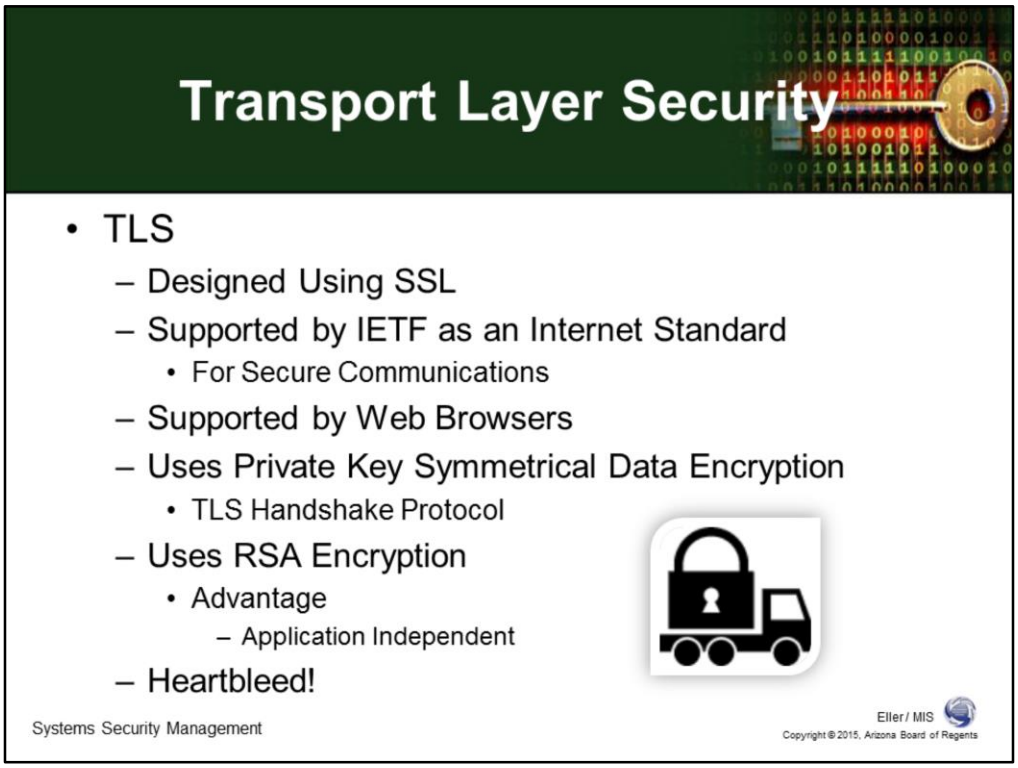


Secure Sockets Layer (continued)

Other applications that use SSL include the Hypertext Transfer Protocol Secure (HTTPS) which is an adaptation of HTTP that enables secure sessions automatically. The Simple Mail Transfer Protocol (SMTP), another protocol in the TCP/IP suite, uses SSL to allow secure transmission of e-mail. Another application protocol called the Network News Transfer Protocol (NNTP) is another TCP/IP protocol which can use SSL to transfer news and information messages securely.

SSL employs RSA encryption using a public and private key system for asymmetrical encryption. SSL is also an example of a handshaking protocol and allows sessions to be encrypted with 40-bit, 56-bit, 128-bit, or 256-bit keys.

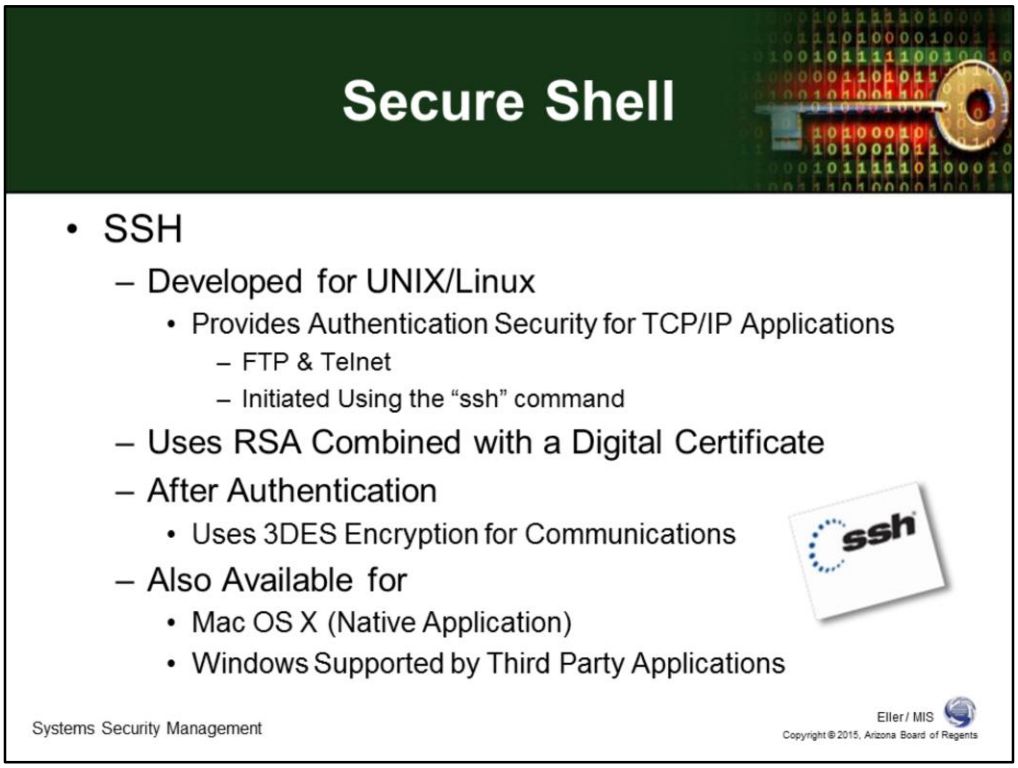
SSL versions 1 and 2 are currently deprecated in favor of SSL version 3 (SSLv3). There have been numerous major vulnerabilities found in previous versions, and even the current version is susceptible to the recently publicized POODLE vulnerability. Because of these vulnerabilities, more servers are trying to get users to use TLS, described in the next slide, to increase the security of web transactions.



Transport Layer Security

Transport layer security, or TLS, was designed using secure sockets layer and is supported by the Internet Engineering Task Force as an Internet standard technology for secure communications. TLS is supported by all major web browsers for encrypted communications. TLS makes use of private key symmetrical data encryption for initiating communications using the TLS handshake protocol. Further communications use RSA encryption solely because RSA is application independent.

In the news: In April of 2014, a major vulnerability dubbed “Heartbleed” was discovered in the OpenSSL implementation of TLS. Forbes cybersecurity columnist Joseph Steinberg wrote, "Some might argue that [Heartbleed] is the worst vulnerability found (at least in terms of its potential impact) since commercial traffic began to flow on the Internet." (Steinberg, 2014)



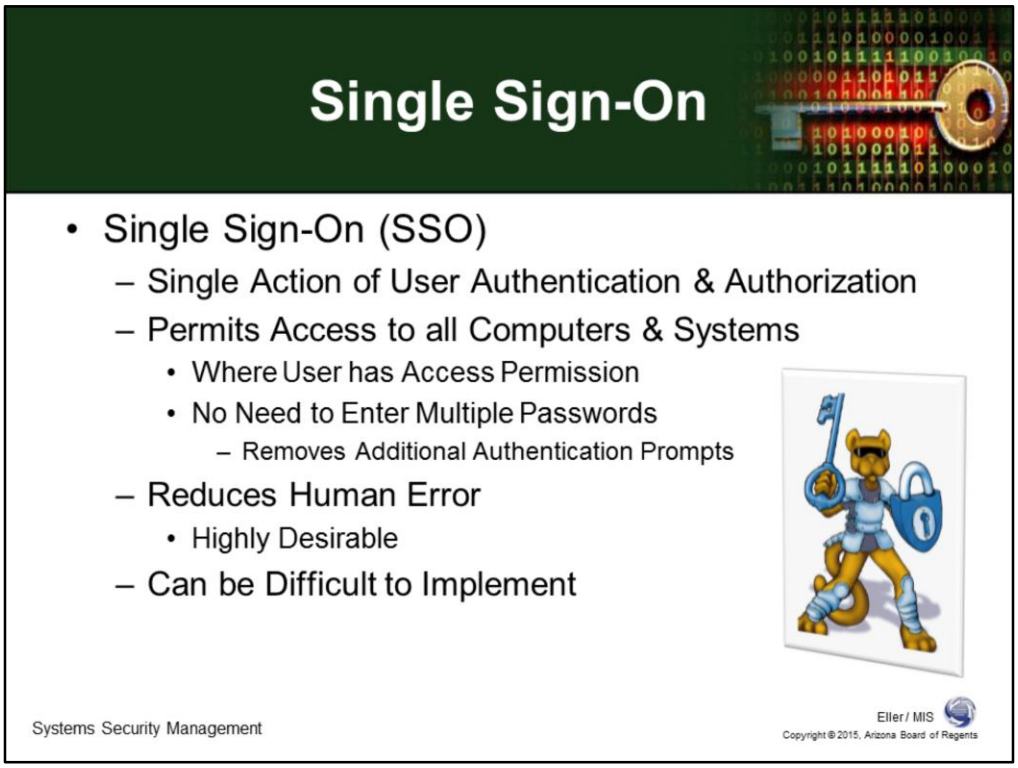
Secure Shell

Secure Shell, or SSH, was developed for UNIX and Linux platforms to provide authentication security for TCP/IP applications such as FTP and telnet. Using this software is as easy as typing "ssh" at a the command line. Secure shell uses RSA encryption combined with a digital certificate in order to initiate a secured connection with a server. After authentication has occurred, secure shell uses 3DES encryption for the communication session. Secure shell is also a native application in the Mac OS X and third parties have made SSH software available for Windows systems.

Security Token

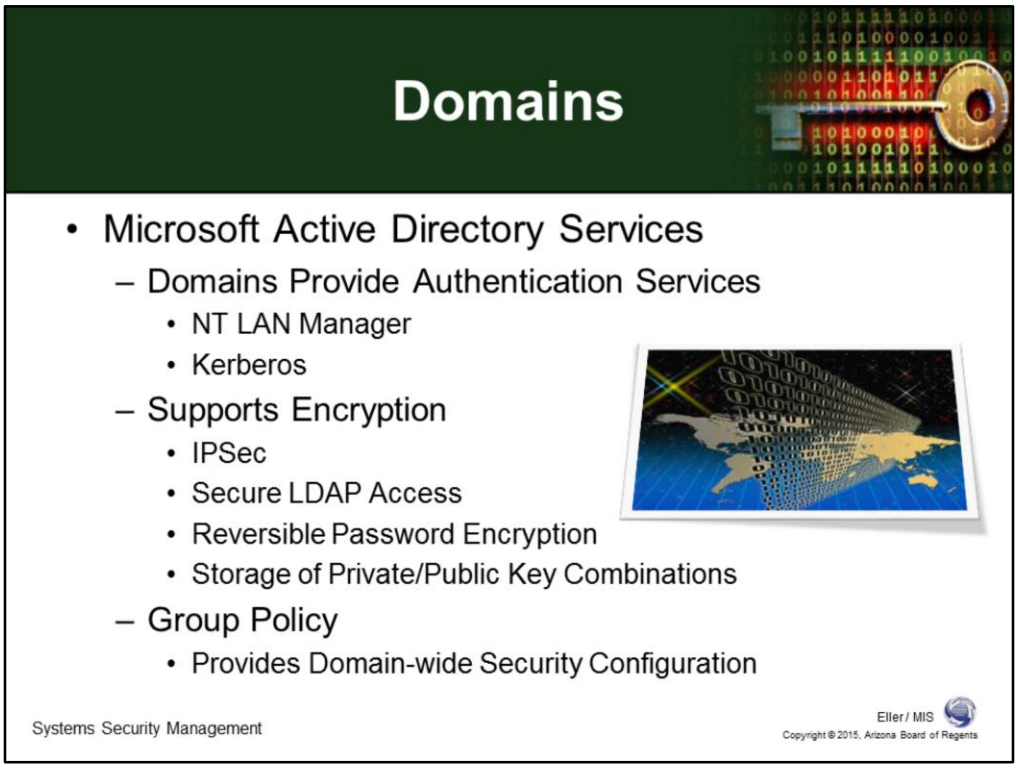
A security token is a physical device used for authentication purposes and resembles a credit card or keyfob. The token is usually inserted into a computer and communicates with an authentication server, allowing it to generate a password for secure authentication. The password is then displayed on the token's small LCD display and can be used for the duration of the logon event, meaning once you log off the password is no longer valid. The advantages for using a security token is that the user does not need to remember a password since it changes constantly and is displayed on the token itself. Also, if the password is intercepted by a third party, it is only valid for as long as the communication session lasts, so the amount of time a system is breached is minimal.

In order to accomplish this kind of security with a hardware device, the token is assigned a unique identification number which never changes, this way the system always knows who is logging in with a particular token.



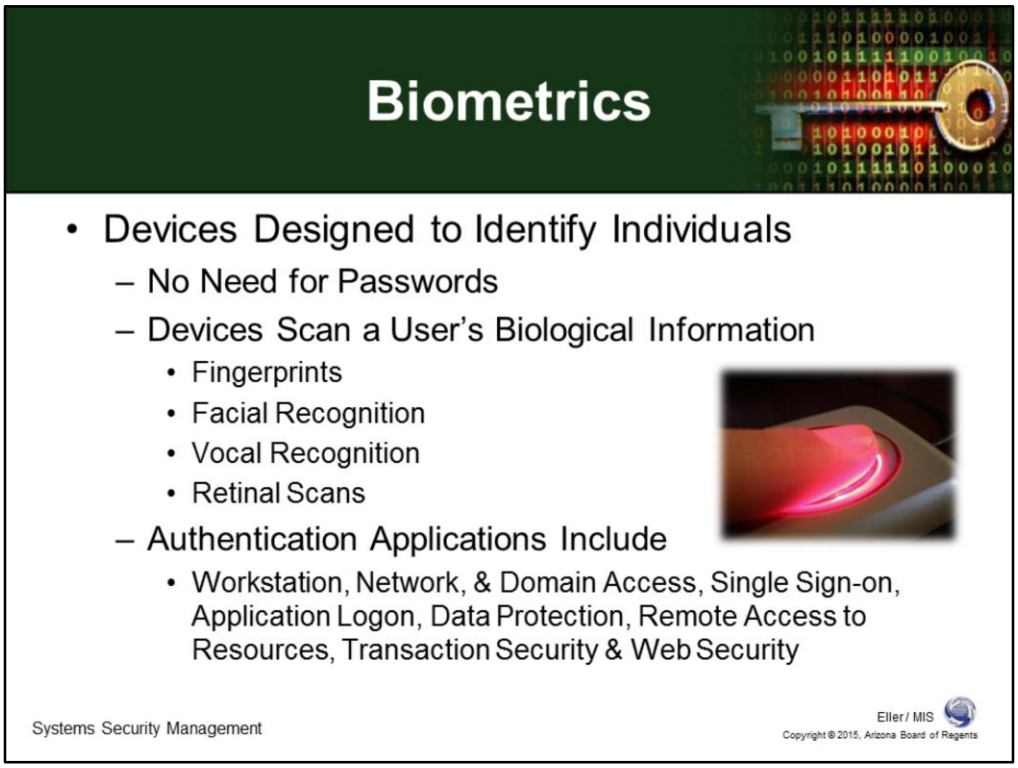
Single Sign-On

Single Sign-On is a feature available when an organization has adopted a centralized authentication system. This feature allows a single action of user authentication and authorization to occur in order to allow access to all computers and systems where the user has access permissions. It removes the need to enter multiple passwords and removes additional authentication prompts. As you can imagine, this greatly reduces human error and is highly desirable. One thing to keep in mind, however, is this can be difficult to implement, especially when technology groups or technology solutions are decentralized or third party applications do not provide methods of using existing authentication methods.



Domains

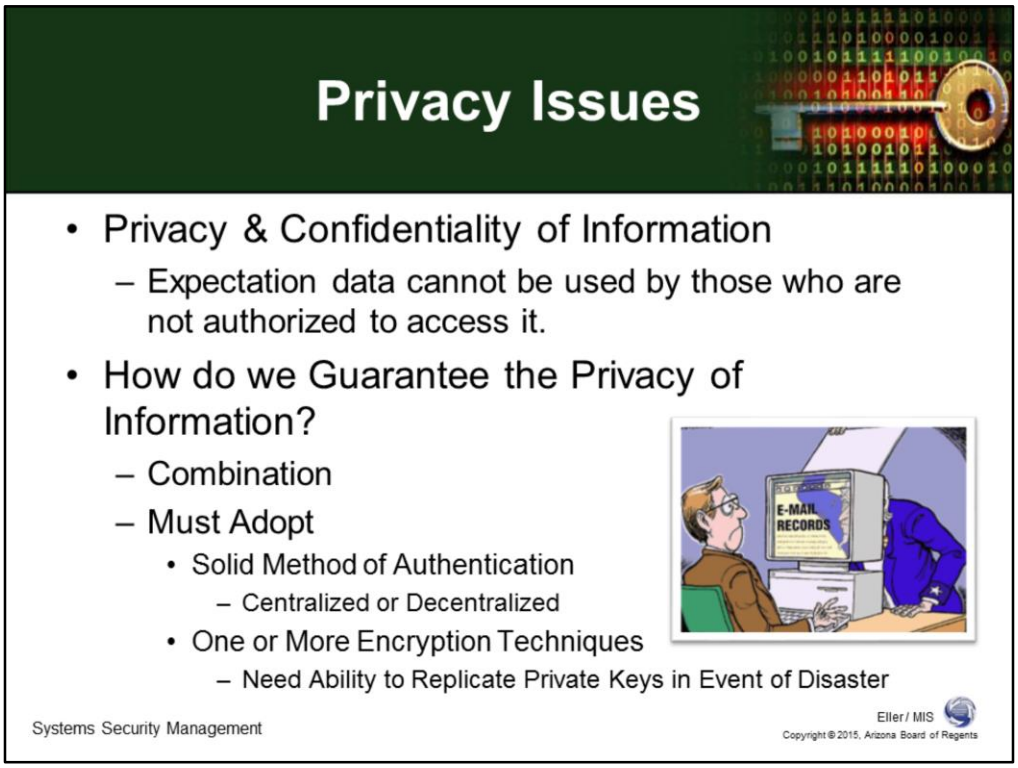
Domains are a primary component of Microsoft's Active Directory Services. We will be discussing Active Directory in depth in Module 10. Domains are used to provide centralized authentication services on a Windows-based network. Authentication is provided through either the NT LAN Manager or the Kerberos protocols. Domains support several encryption types including IPSec, secure LDAP access through SSL, reversible password encryption, and the storage of private and public key combinations. In addition, Microsoft has provided a tool called Group Policy which allows SysAdmins to provide domain-wide security configurations.



Biometrics

Biometrics are hardware devices designed to positively identify an individual using physical attributes instead of passwords. The devices will scan a user's biological information and use it to grant or deny access to systems and data. Some of the more well known forms of biometrics include fingerprint scanners, video cameras capable of facial recognition, vocal recognition, and retinal scanners.

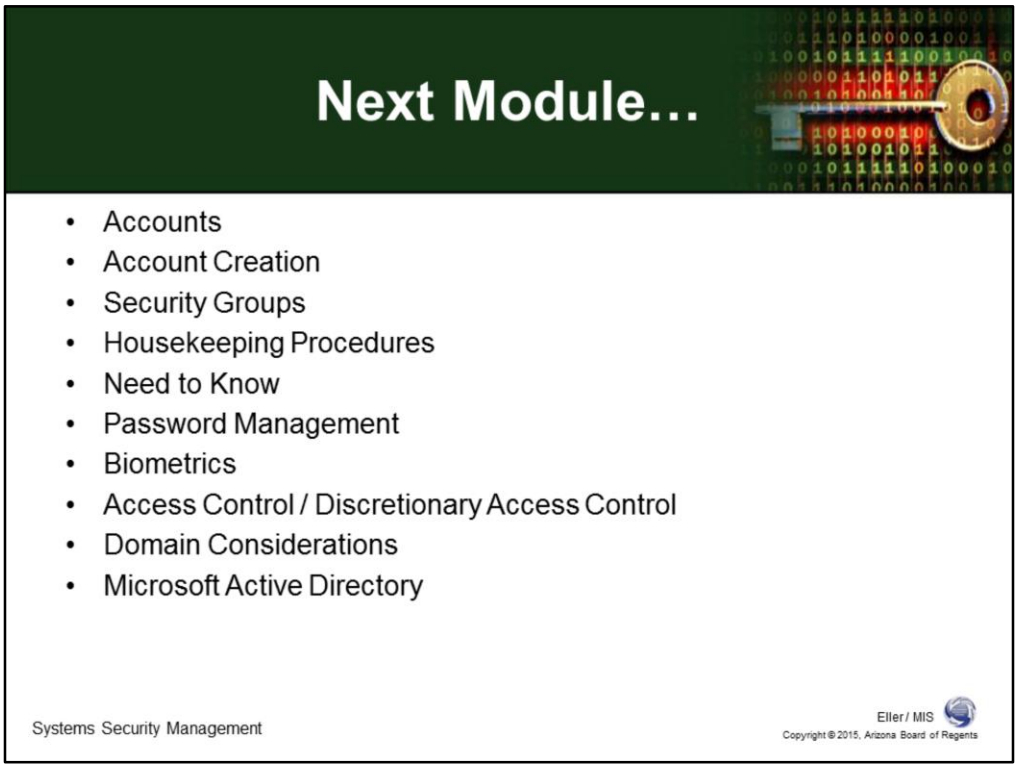
Biometric devices are designed to work with a wide variety of authentication applications, including workstation, network, & domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and web security. Biometrics are also being used to allow physical access to secure rooms in buildings.



Privacy Issues

When it comes to privacy we all have our individual comfort levels with regard to how much information we feel free to share. With information security, privacy and confidentiality go hand-in-hand as the expectation is that our data cannot be used by those who are not authorized to access it. So, how then do we guarantee the privacy of our information? Well the answer is a combination of factors. We must adopt a solid method of authentication so we know who is accessing our data. This can be either a centralized or decentralized solution. The other factor is using one or more encryption techniques in order to guarantee the data is unintelligible should someone without authorization tries to access it. Going along with encryption is a need to replicate and backup our private encryption keys, just in case there is a disaster that destroys the original keys.

Privacy is a complex issue when it comes to information security; however, a combination of authentication and encryption will help to keep our data safe from prying eyes.



In the next module we will be discussing Account-based Security, including:

- Accounts & Account Creation
- Security Groups
- Housekeeping Procedures
- Need to Know
- Password Management
- Biometrics
- Access Control / Discretionary Access Control
- Domain Considerations
- An introduction to Microsoft Active Directory

References

Introduction to Biometrics. (2010). The Biometrics Consortium. Retrieved from http://www.biometrics.org/introduction.php.

IPSec in Windows Server 2003. (2009). Computer Performance LTD. Retrieved from http://www.computerperformance.co.uk/w2k3/Security_IPSec.htm.

Message Digest. (2010). Top Bits. Retrieved from http://www.topbits.com/message-digest.html.

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

Public Key Infrastructure. (2009, September 18). *Information Assurance Support Environment: Department of Defense*. Retrieved from http://iase.disa.mil/pki/.

Single Sign-On. (2009). *The Open Group*. Retrieved from http://www.opengroup.org/security/sso/.

Steinberg, J. (2014, April). Massive Internet Security Vulnerability - Here's What You Need To Do. *Forbes*. Retrieved from http://www.forbes.com/sites/josephsteinberg/2014/04/10/massive-internet-security-vulnerability-you-are-at-risk-what-you-need-to-do/.