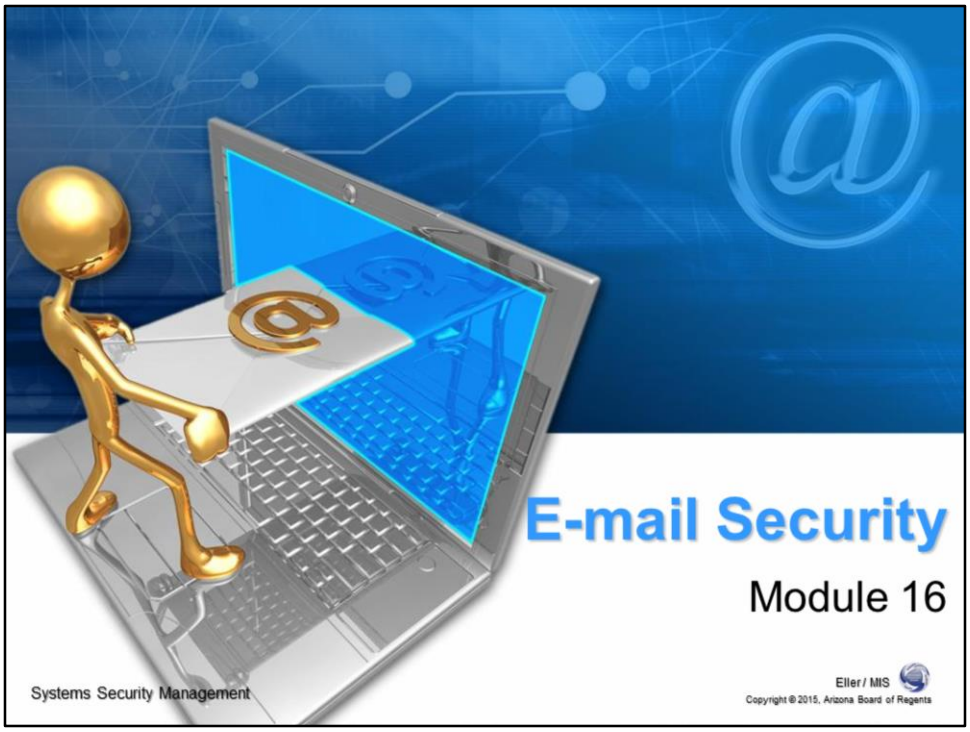
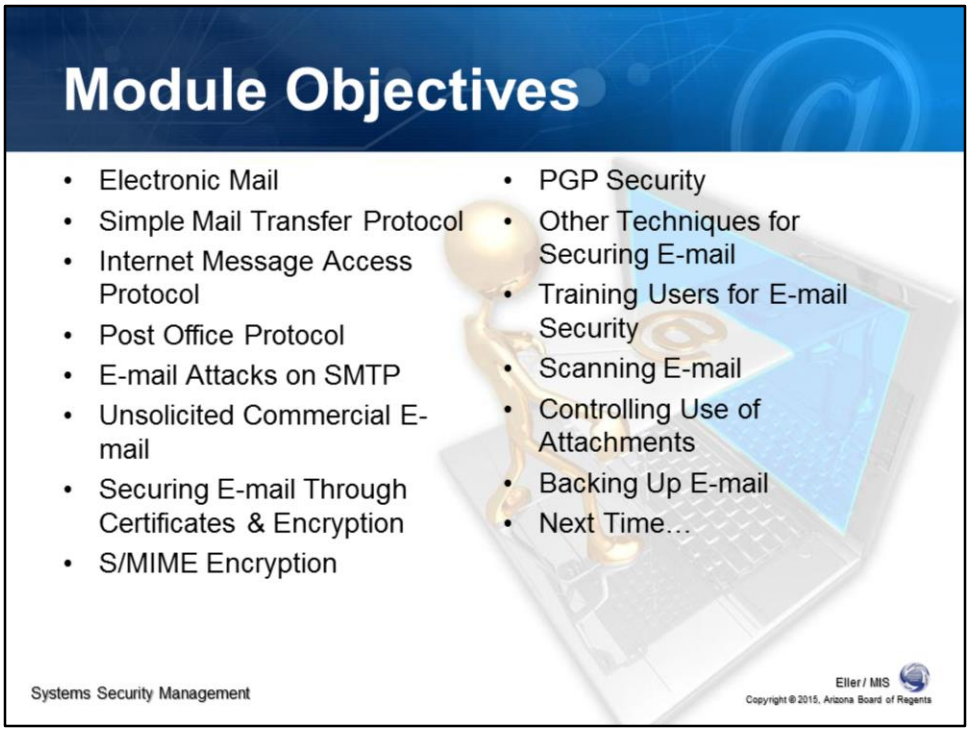


E-mail Security

Module 16

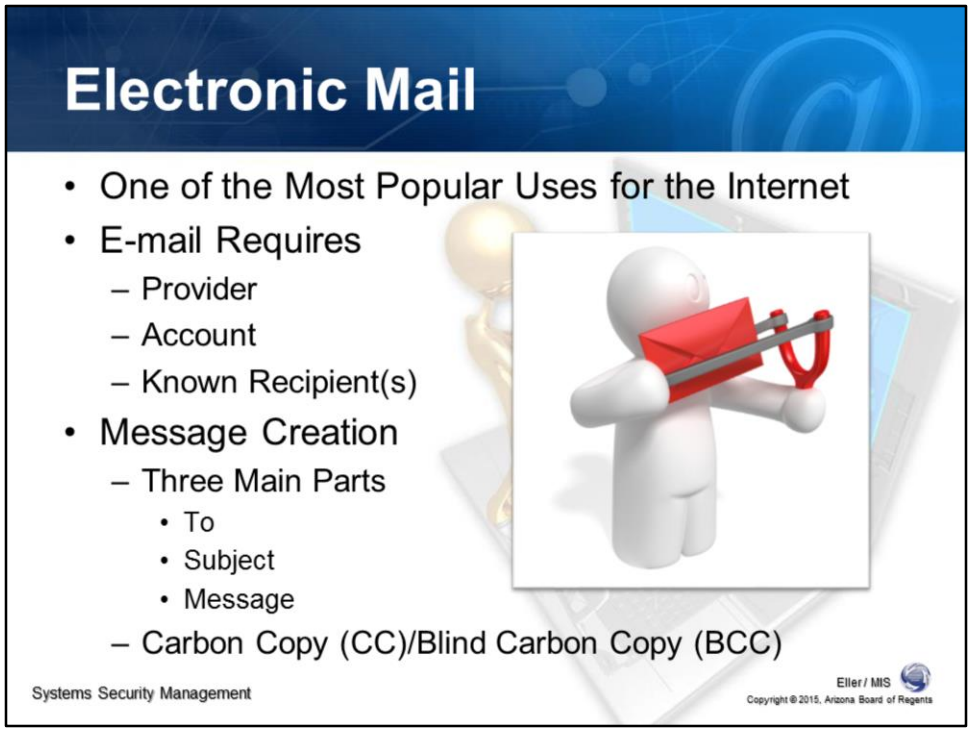
Systems Security Management

Eller / MIS



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

- Describe what electronic mail is and how it works.
- Understand how the simple mail transfer protocol works.
- Describe the differences between IMAP and POP.
- Understand how SMTP can be attacked.
- Understand what UCE is.
- Describe how to secure e-mail through the use of certificates and encryption.
- Understand different encryption options such as S/MIME and PGP and other techniques for securing e-mail.
- Understand how training users will help improve e-mail security.
- Understand how scanning e-mail and controlling the use of attachments are important pieces of e-mail security.
- Understand how backing up e-mail is one of the last lines of defense in e-mail security.



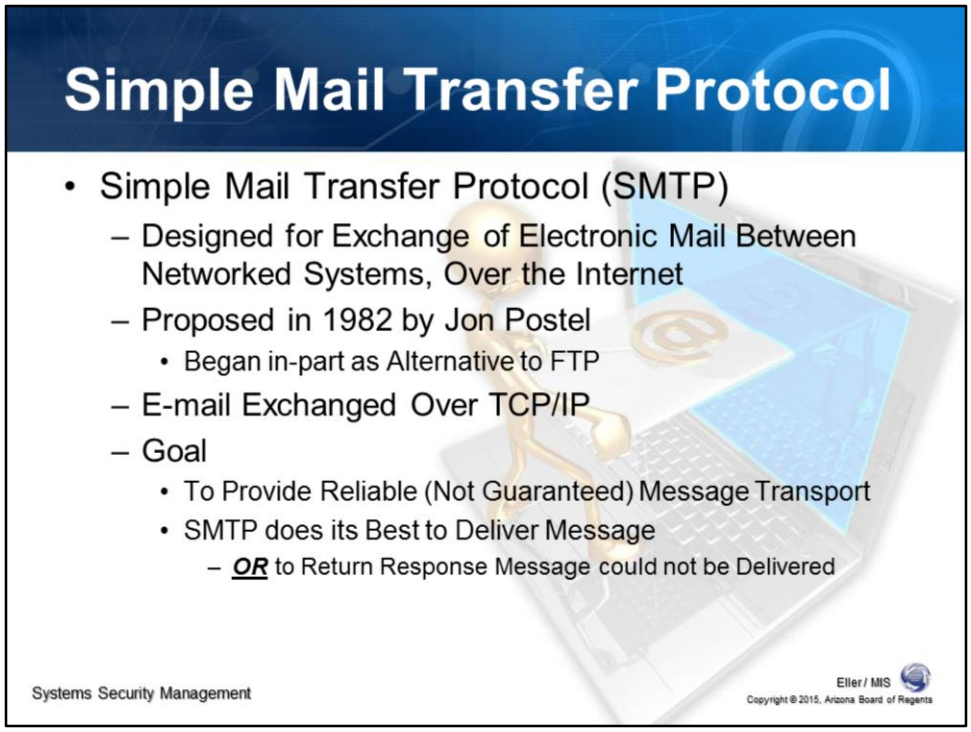
Electronic Mail

Electronic Mail, or E-mail, is one of the most popular uses for the Internet. Everyone taking this class has an e-mail account, so this is definitely something you should be familiar with.

In general, e-mail requires a provider, an account, and known recipients. You cannot send or receive e-mail without these three components. When it comes to message creation, there are three main parts:

To – Who are you sending a message to?
Subject – This is a short description of the message.
Message – What do you need to say?

In addition to these parts, you will also find a CC field (carbon copy) and BCC (blind carbon copy). In some e-mail applications, such as Microsoft Outlook, you will also find a From field which is used to change who the e-mail appears to be sent from. Note, this field will show the e-mail you enter as the sender; however, it will also note that the message is from that sender through you, unless you have "Send As" privileges (this is typically a feature of Microsoft Exchange).

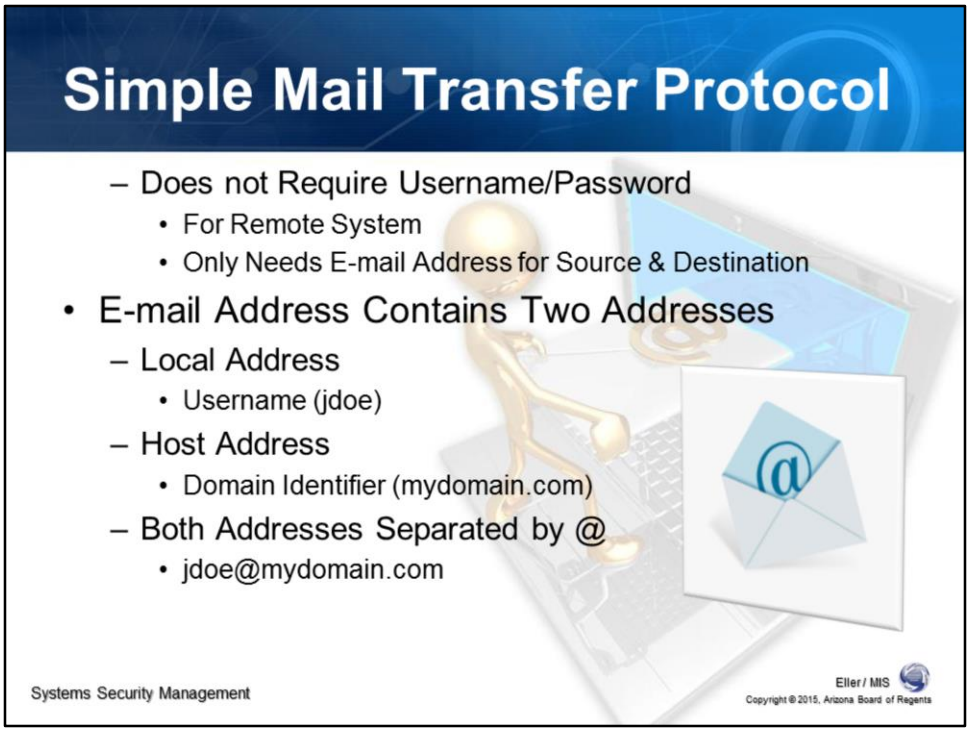


Simple Mail Transfer Protocol

The Simple Mail Transfer Protocol, or SMTP, was designed to facilitate the exchange of e-mail between networked systems over the Internet. In other words, SMTP is used when you send a message to someone. Your computer will take the message and pass it on to an SMTP server which sends it to another SMTP server and so on until it reaches its destination. SMTP was proposed in 1982 by Jon Postel as an alternative to FTP for sending files over the Internet.

SMTP is a protocol in the TCP/IP suite, so e-mail is exchanged through this communications medium. The goal with SMTP is to provide a reliable, but not guaranteed, message transport for e-mail. SMTP does its best to deliver messages, or return a response message to the sender that the message could not be delivered.

NOTE – A common mnemonic device used to remember SMTP's function is that it's used to Send Mail To People.



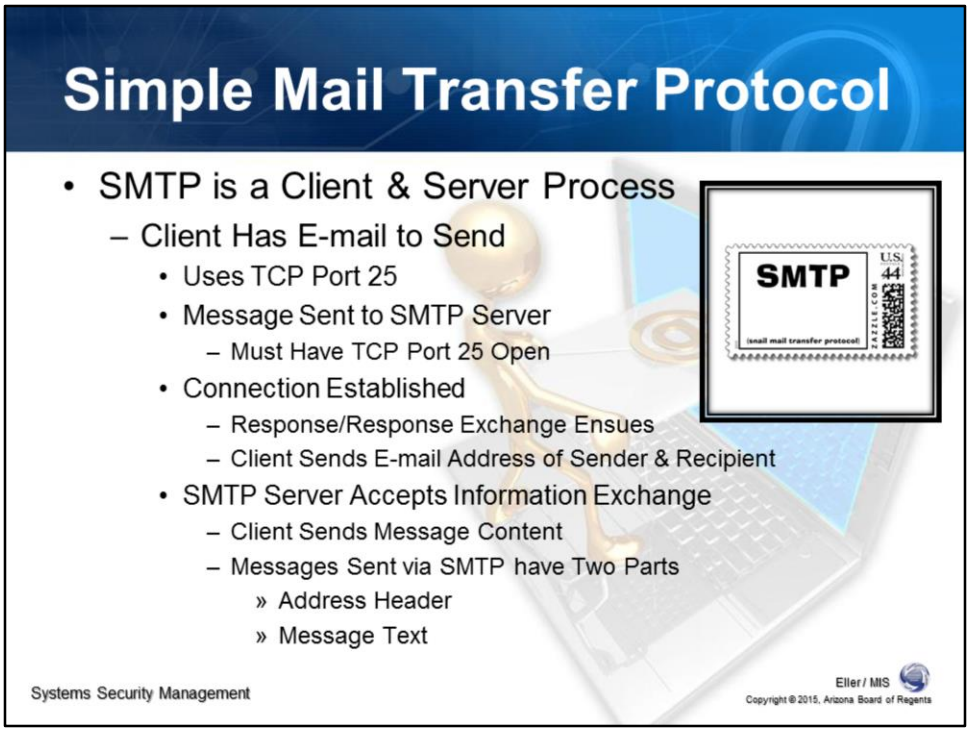
Simple Mail Transfer Protocol (continued)

SMTP servers generally do not require a username and password in order to send a message; however, many organizations are beginning to implement this as a means of preventing non-employees from using the server to send SPAM. Regardless, the SMTP server really only needs to know the email addresses of the sender and the recipient to pass the message along.

An E-mail address actually contains two different addresses: a local address and a host address.

- Local Address – this is your username in the e-mail address.
- Host Address – this is the domain identifier

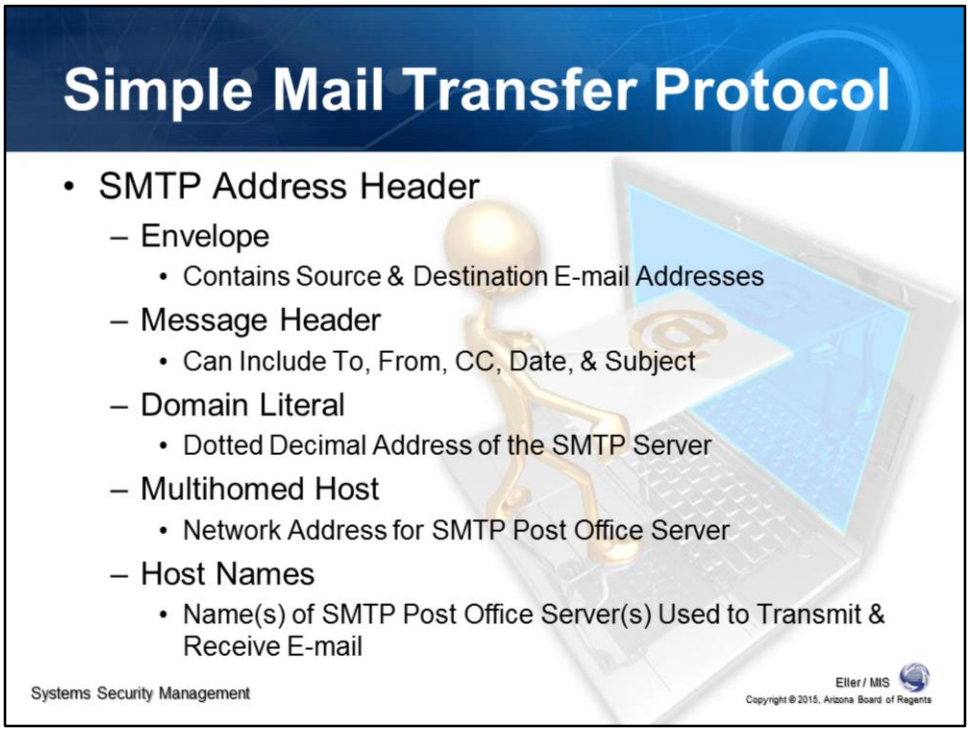
When you combine these two parts and separate them with the @ symbol, you have an e-mail address.



Simple Mail Transfer Protocol (continued)

SMTP is a client/server process. The client system has an e-mail that needs to be sent. The client will use TCP port 25 to send the message to the SMTP server. The server itself must also have TCP port 25 open and available in order to receive the message. Once the connection is established a response/response exchange ensues, where the client and server exchange information. The client will send the e-mail addresses of both the sender and recipient.

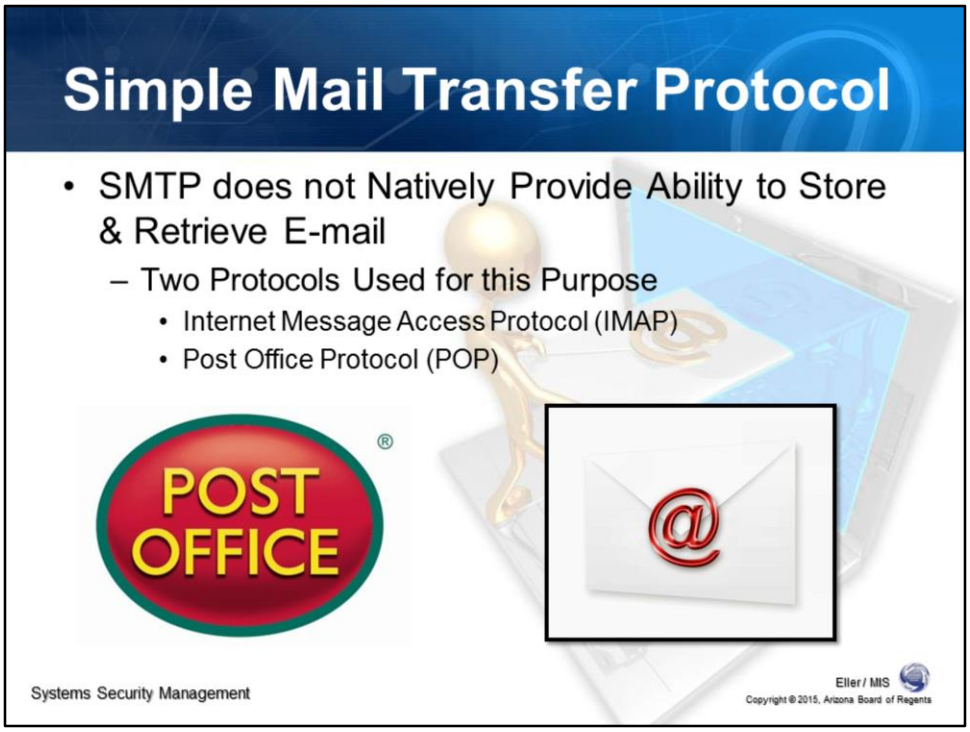
Once the SMTP server accepts the information exchange, the client will send the message content. Any messages sent via SMTP have two parts: an address header and the message text.



Simple Mail Transfer Protocol (continued)

The SMTP address header contains the following information:

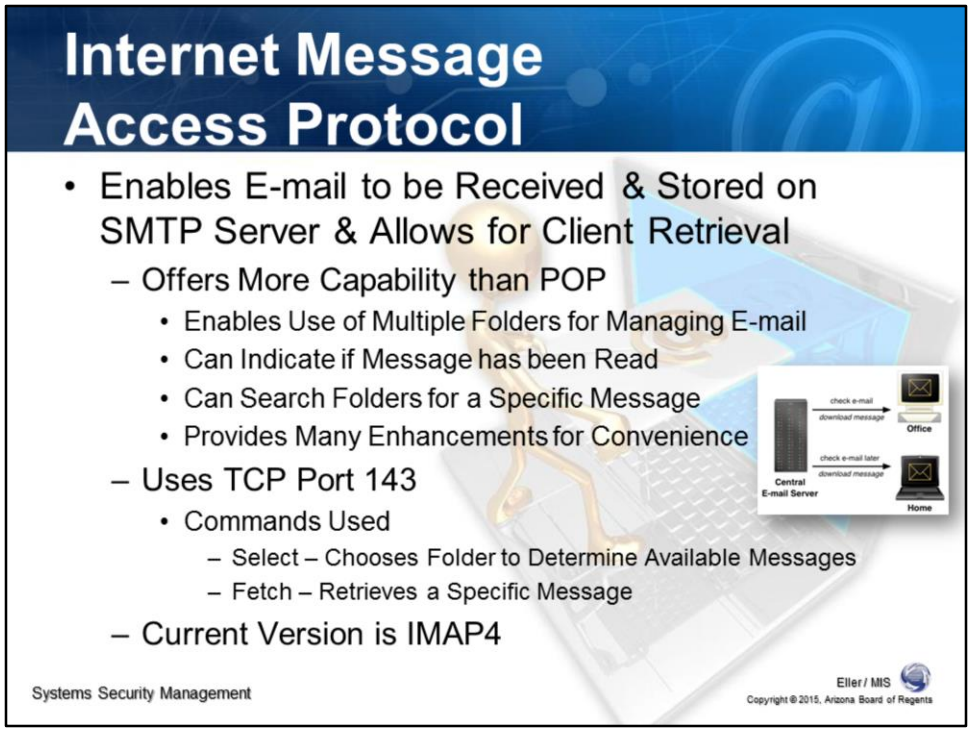
- **Envelope** – Contains Source & Destination E-mail Addresses
- **Message Header** – Can Include To, From, CC, Date, & Subject
- **Domain Literal** – Dotted Decimal Address of the SMTP Server
- **Multihomed Host** – Network Address for SMTP Post Office Server
- **Host Names** – Name(s) of SMTP Post Office Server(s) Used to Transmit & Receive E-mail



Simple Mail Transfer Protocol (continued)

Something else to remember, SMTP does not natively provide the ability to store and retrieve e-mail. SMTP is only used as a means of sending messages. There are two different protocols which are used for the purpose of storing and retrieving messages:

- Internet Message Access Protocol (IMAP)
- Post Office Protocol (POP)



Internet Message Access Protocol

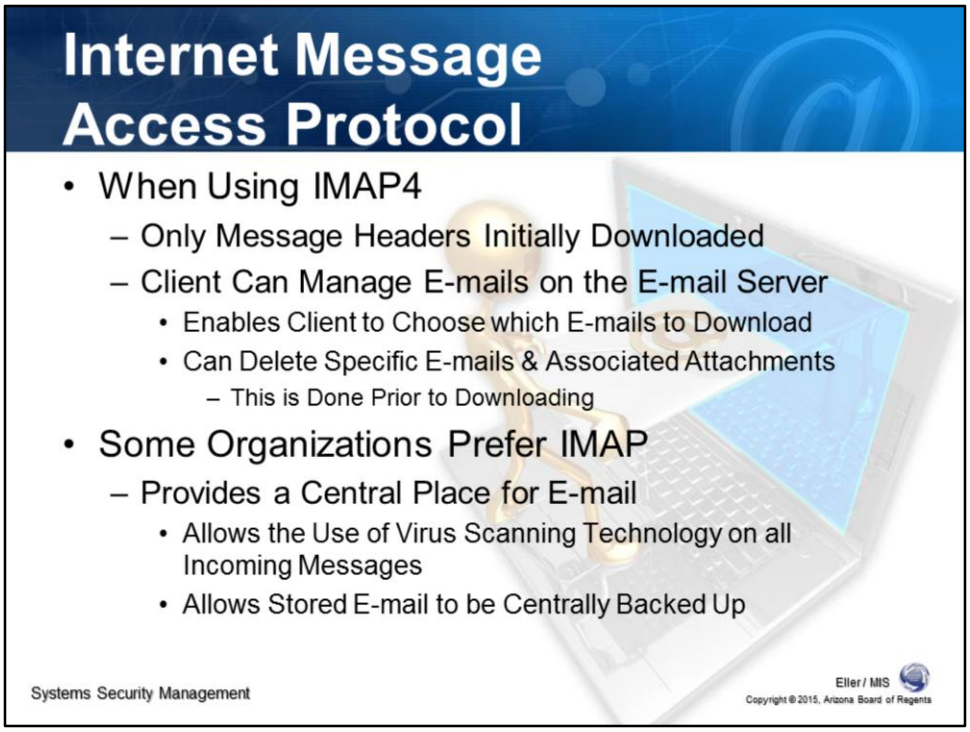
The Internet Message Access Protocol, or IMAP, enables e-mail to be received and stored on an SMTP server and allows for client retrieval through a web browser or client application. IMAP offers more capability than POP, which we will discuss in a moment. These capabilities include:

- Enables Use of Multiple Folders for Managing E-mail
- Can Indicate if Message has been Read
- Can Search Folders for a Specific Message
- Provides Many Enhancements for Convenience

IMAP uses TCP port 143 for accessing e-mail from the server. The commands used to access messages include:

- **Select** – Chooses Folder to Determine Available Messages
- **Fetch** – Retrieves a Specific Message

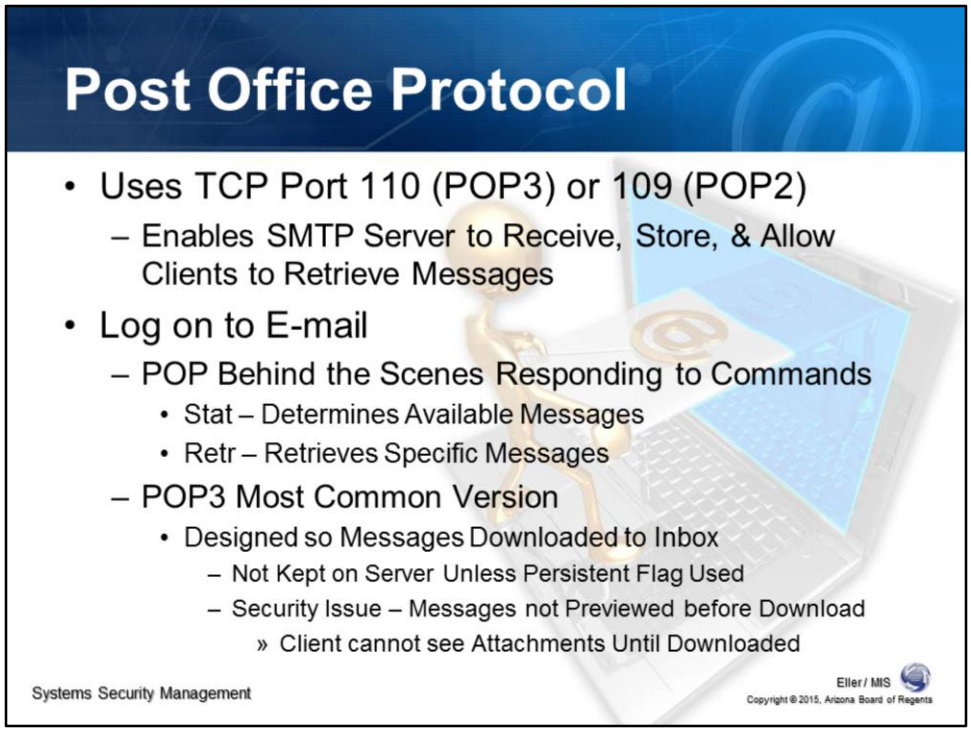
The current version of IMAP is IMAP4.



Internet Message Access Protocol (continued)

When using IMAP4 to retrieve messages, only the message headers will be downloaded to your client application. The client can then manage e-mails on the server itself. This allows the client to pick and choose which e-mails to download, and it allows for the added security feature where the client can delete specific e-mails and their associated attachments before they can be downloaded to the client system. This is a huge advantage that helps to prevent the spread of viruses, worms, and Trojan horses.

Some organizations prefer their employees to use IMAP for e-mail. The reason for this is the organization can provide a centralized location for e-mail storage, making it possible to retrieve e-mails from different locations when necessary. IMAP also allows organizations to make use of a virus scanning technology on all incoming messages, whether or not they originate from within the organization. IMAP also allows stored e-mail to be centrally backed up in the event a client accidentally, or intentionally in some cases, deletes one or more messages.

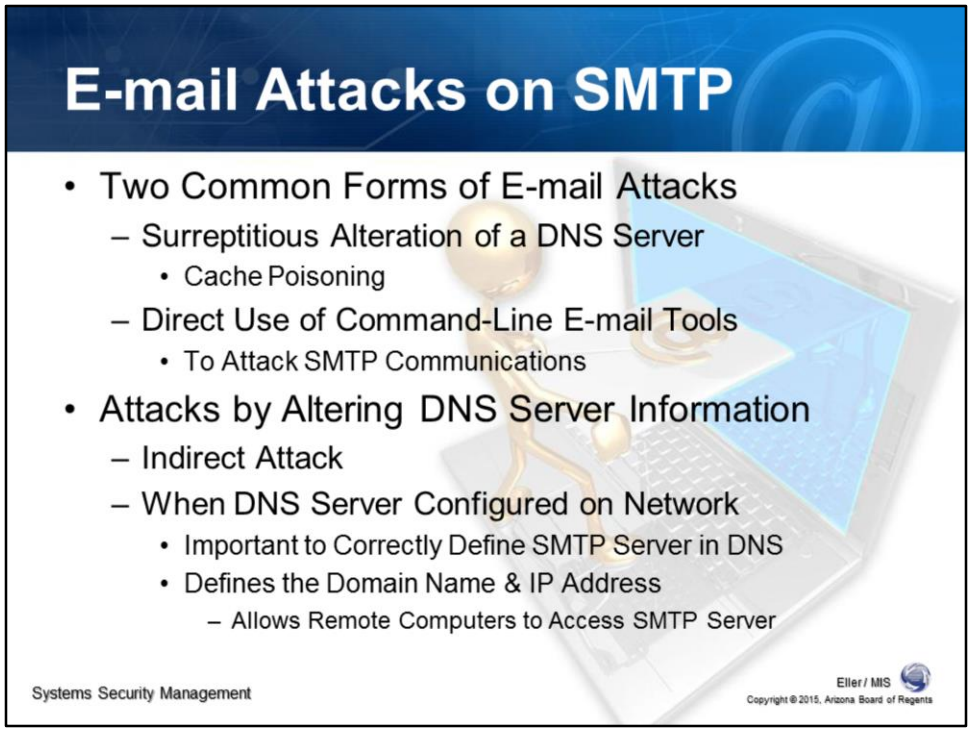


Post Office Protocol

The Post Office Protocol, or POP, makes use of TCP port 110 when using POP3, or TCP port 109 when using POP2. POP enables the SMTP server to receive, store, and allow clients to retrieve messages. When accessing your e-mail using POP, the client application will use the following commands:

- **Stat** – Determines Available Messages
- **Retr** – Retrieves Specific Messages

POP version 3 is the most common, and most recent, version of the protocol, and it is designed so all messages are downloaded from the server to a client application inbox. E-mail is not kept on the server unless the client application has been configured to leave the messages on the server. There is a security issue with regard to POP. Whereas you could preview messages in IMAP and delete them before downloading, POP does not allow you to preview and delete until you actually download the message to your client application.

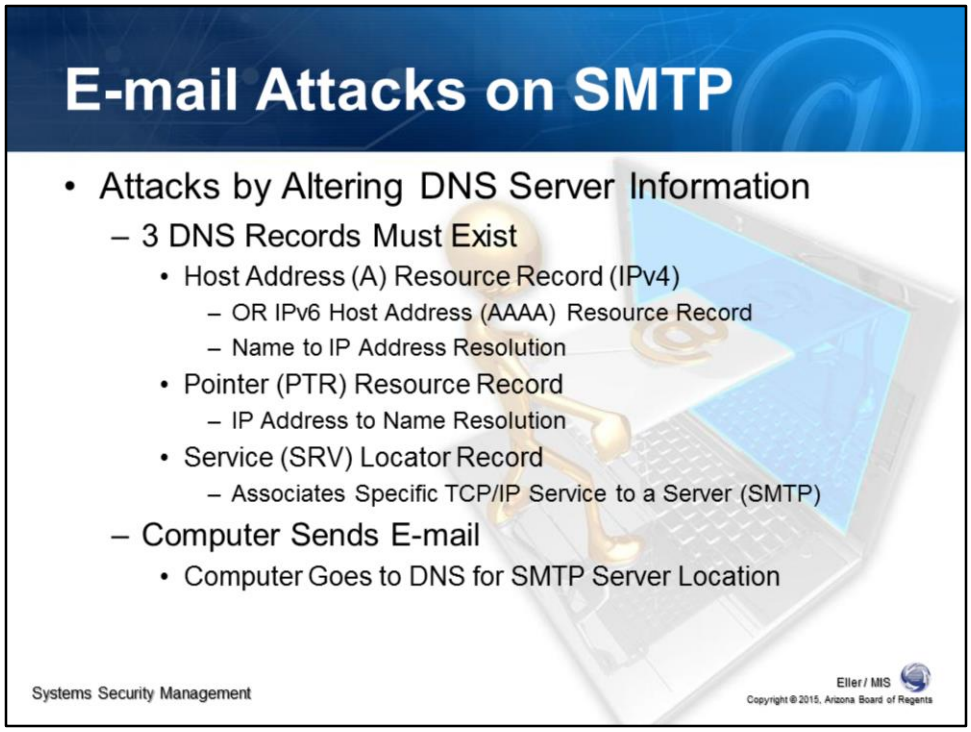


E-Mail Attacks on SMTP

There are two common forms of e-mail attacks that are used by attackers. These attacks include:

Surreptitious Alteration of a DNS Server – Cache Poisoning
Direct Use of Command-Line E-mail Tools – To Attack SMTP Communications

When an attacker chooses to launch an attack by altering DNS server information, this is considered to be an indirect attack because they are not actually attacking their target. Let me explain. When a DNS server is configured on the network, it is very important to correctly define the SMTP server within DNS. This involves defining the domain name and IP address, which in-turn allows remote computers to access the SMTP server.

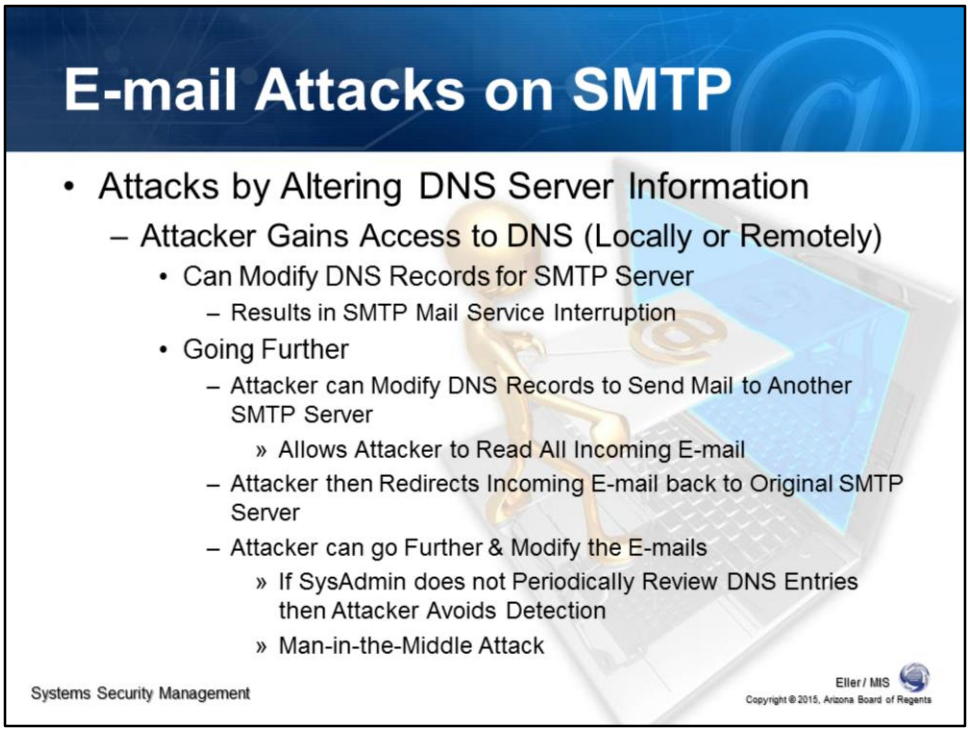


E-Mail Attacks on SMTP (continued)

So, attacks that are designed to alter DNS information means the attacker wants to change the DNS records which point to the correct SMTP server in order to redirect e-mail to their own systems. In DNS there are three records which must exist to ensure proper communication:

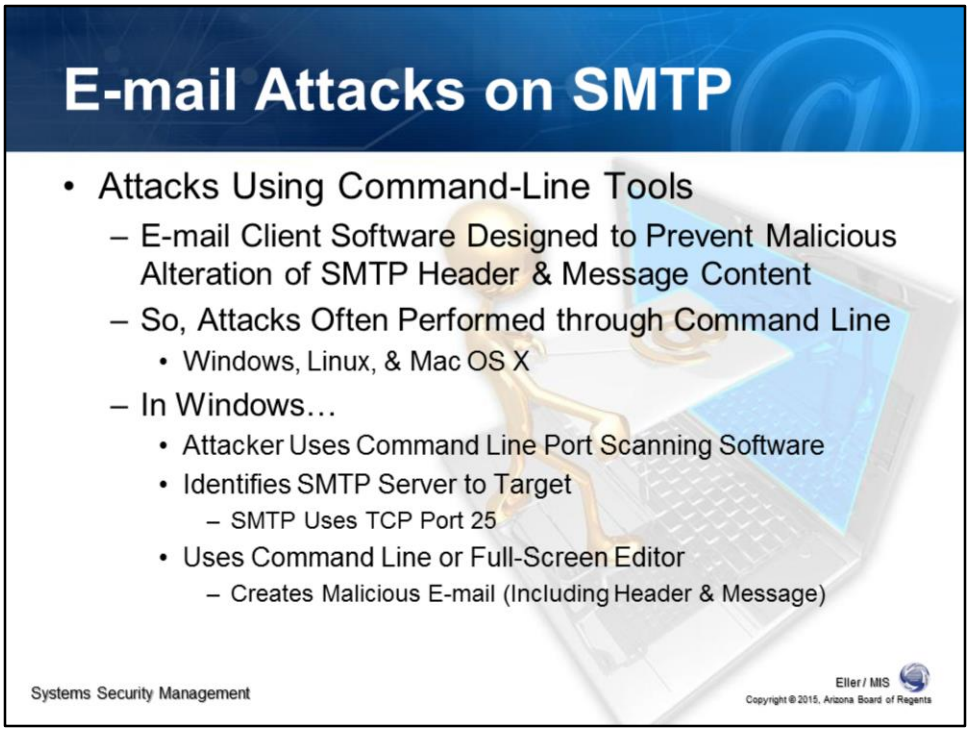
- **Host Address (A) Resource Record (IPv4) OR IPv6 Host Address (AAAA) Resource Record** – Name to IP Address Resolution
- **Pointer (PTR) Resource Record** – IP Address to Name Resolution
- **Service (SRV) Locator Record** – Associates Specific TCP/IP Service to a Server (SMTP)

When a computer sends an e-mail, the client computer asks the DNS server for the SMTP server location. This is why the attacker is looking to make a change to the DNS.



E-Mail Attacks on SMTP (continued)

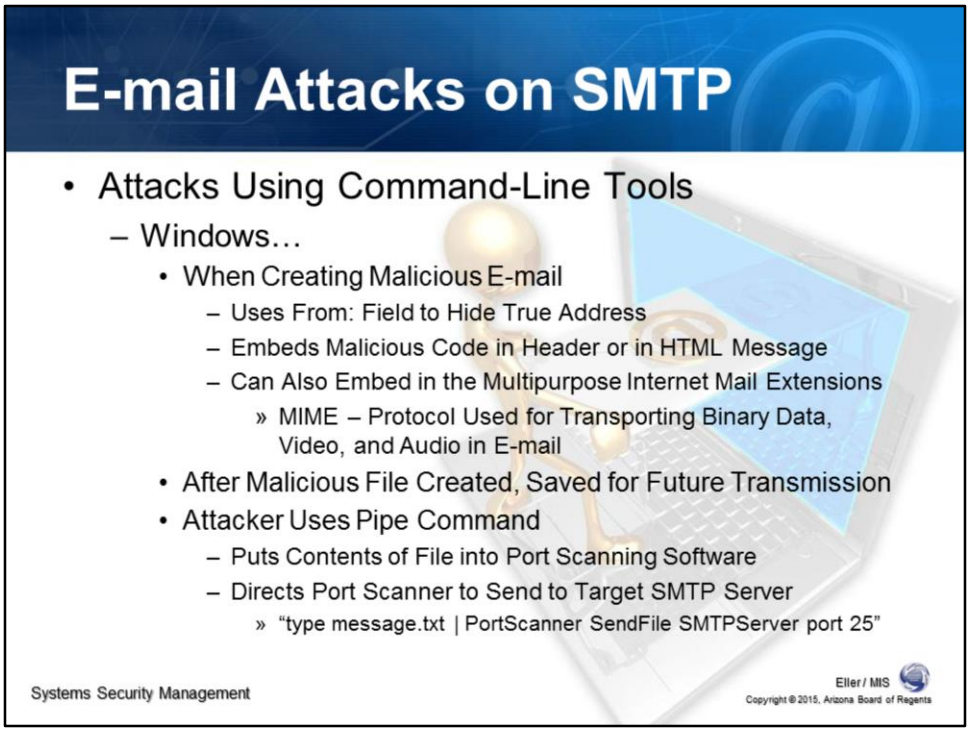
In order to perpetrate this type of attack, the attacker gains access to the DNS server, either locally or remotely and modifies the DNS records for the SMTP server. This will result in SMTP mail service disruption for the victim organization. Taking this one step further, the attacker can modify the DNS records in order to send all mail to another SMTP server of their choosing. This allows the attacker to read all incoming e-mail, which as you might expect can be a major problem. The attacker will then generally redirect their SMTP server to point back to the organization's SMTP server so the e-mail will continue on to its expected destinations with no one the wiser. Going even further, the attacker can take the e-mails as they arrive on his or her system and modify them before sending them on their way. If the SysAdmin does not periodically review their DNS entries, the attacker will avoid detection. This is an example of a man-in-the-middle attack.



E-Mail Attacks on SMTP (continued)

Another type of attack on an SMTP server would involve the attacker making use of command line tools. E-mail client software is designed to prevent malicious alteration of the SMTP header and message content, so attacks are often performed through the command line in Windows, Linux, and the Mac OS X.

In Windows, the attacker will use command line port scanning software to identify the SMTP server to target. This is possible since all SMTP servers will use TCP port 25 by default. By using the command line or a full-screen editor, the attacker can create a malicious e-mail, including the header and message.

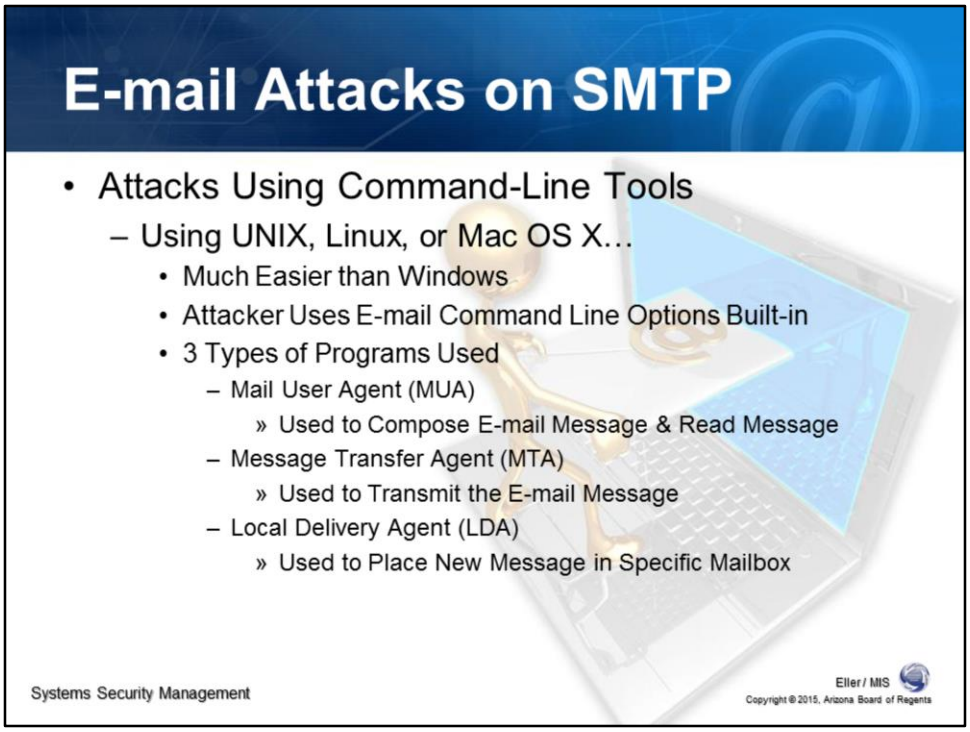


E-Mail Attacks on SMTP (continued)

When the attacker creates a malicious e-mail they use the From: field to hide the true address of the source. They then embed malicious code in the header or in an HTML message. The attacker can also embed the malicious code in the Multipurpose Internet Mail Extensions, or MIME, which as you remember is a protocol used for transporting binary data, video, and audio files in e-mail.

After the malicious e-mail is created, it is saved for future transmission. The attacker will then make use of the pipe command in order to put the contents of the file into the command line port scanning software. This directs the port scanner to send the message to the target SMTP server. So, for example, the command line code might look as follows:

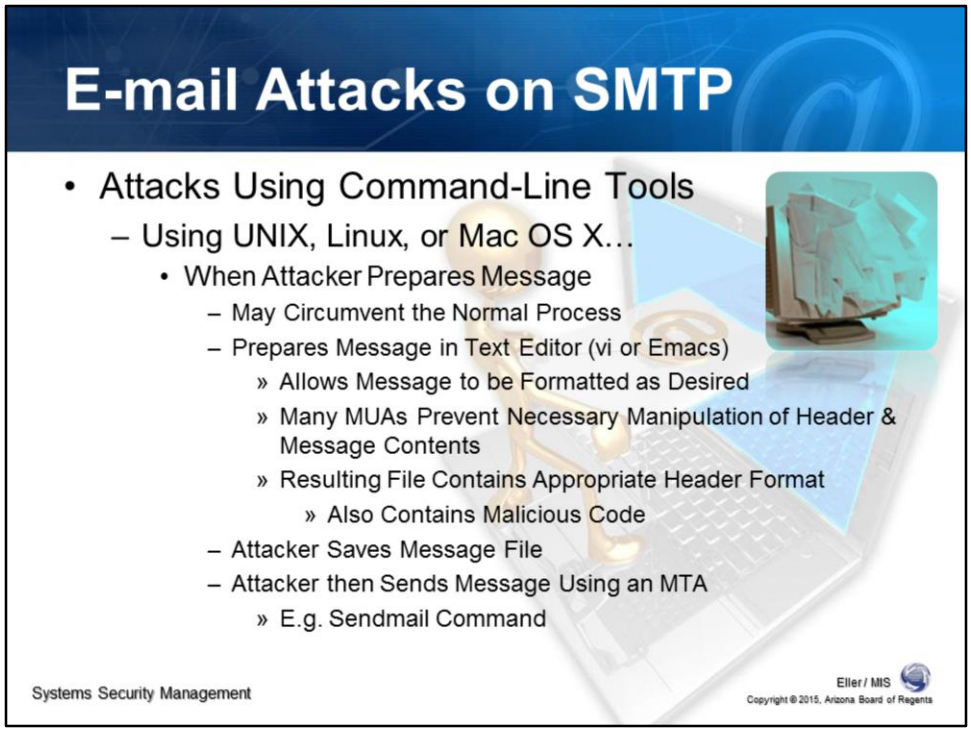
"type message.txt | PortScanner SendFile SMTPServer port 25"



E-Mail Attacks on SMTP (continued)

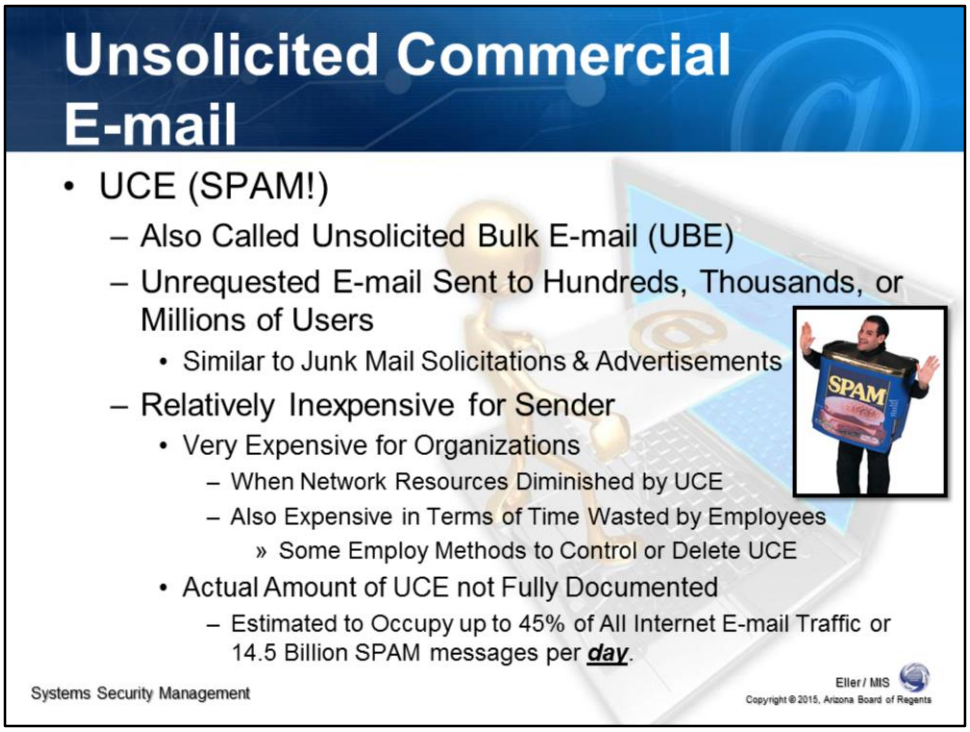
If an attacker chooses to use a Linux or Mac OS X system to initiate an attack using command line tools, they will find it to be easier to accomplish than in Windows. The attacker can use e-mail command line options that are built-in to the operating systems. There are three types of programs that are used:

- **Mail User Agent (MUA)** – Used to Compose E-mail Message & Read Message
- **Message Transfer Agent (MTA)** – Used to Transmit the E-mail Message
- **Local Delivery Agent (LDA)** – Used to Place New Message in Specific Mailbox



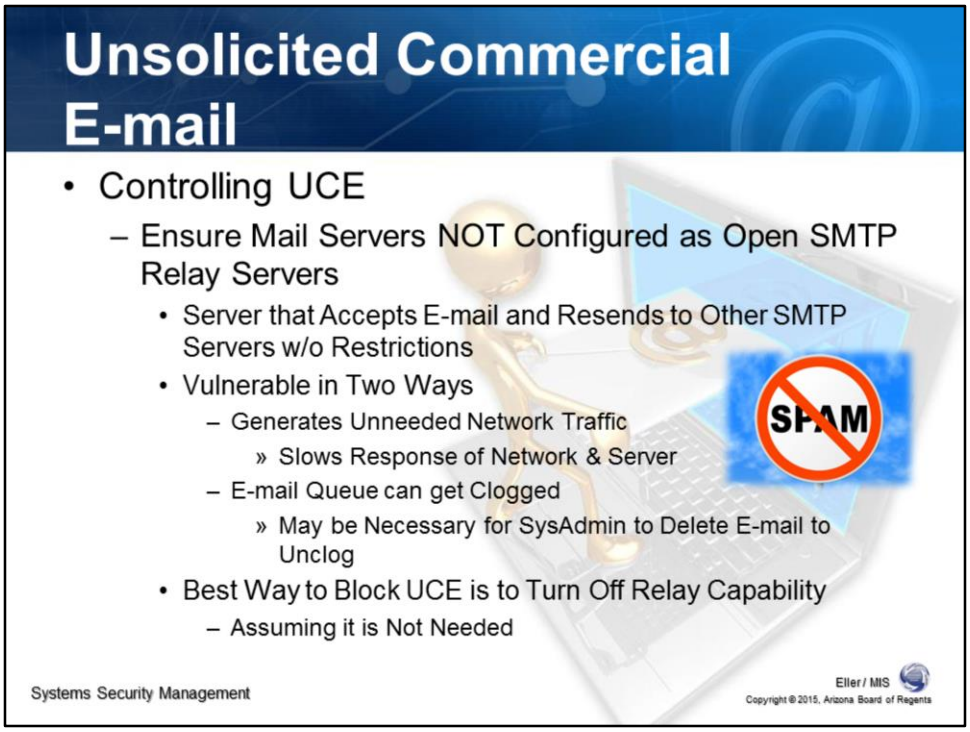
E-Mail Attacks on SMTP (continued)

When the attacker prepares the message, they may circumvent the normal process. The attacker can prepare the message in a text editor, such as vi or emacs, which allows the message to be formatted as desired. Many of the MUAs in both operating systems will prevent the necessary manipulation of the header and message contents required by the attacker; however, by using a text editor, the resulting file will contain the appropriate header format and the malicious code. The attacker can then save the message file and send it using an MTA, for example, using the sendmail command.



Unsolicited Commercial E-mail

All of you should be familiar with unsolicited commercial e-mail, or UCE, because it is also known as unsolicited bulk e-mail (UBE), or SPAM. UCE is simply unrequested e-mail that is sent to hundreds, thousands, or millions of users, and this is similar to junk mail solicitations and advertisements you might receive in your real mailbox. UCE is relatively inexpensive for the sender; however, it can be very expensive for organizations, especially when network resources are diminished by processing UCE. UCE is also expensive in terms of the time wasted by employees downloading and opening these messages, so some organizations employ different methods to try and control or delete SPAM. While the actual amount of UCE transmitted on a regular basis is not fully documented, experts estimate that SPAM accounts for up to at least 45% of all Internet e-mail traffic. This means there are approximately 14.5 billion unsolicited emails sent each ***day*** ("Spam Statistics and Facts," 2015).

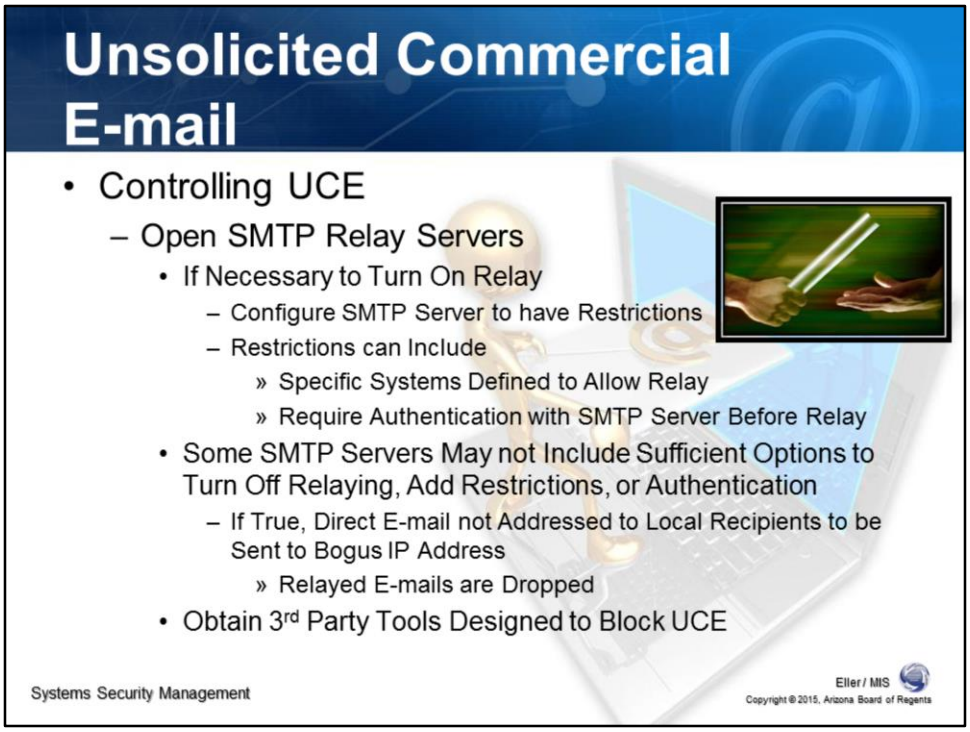


Unsolicited Commercial E-mail (continued)

When attempting to control UCE, the SysAdmin will need to ensure the SMTP servers are NOT configured as Open SMTP Relay Servers. An open SMTP relay server is a server that accepts e-mail and resends it to other SMTP servers without restrictions. This makes an SMTP server vulnerable in two ways:

- **Generates Unneeded Network Traffic** – Slows Response of Network & Server
- **E-mail Queue can get Clogged** – May be Necessary for SysAdmin to Delete E-mail to Unclog

The best way to block SPAM senders is to turn off the relay capability of SMTP, assuming it is not necessary for some specific reason.

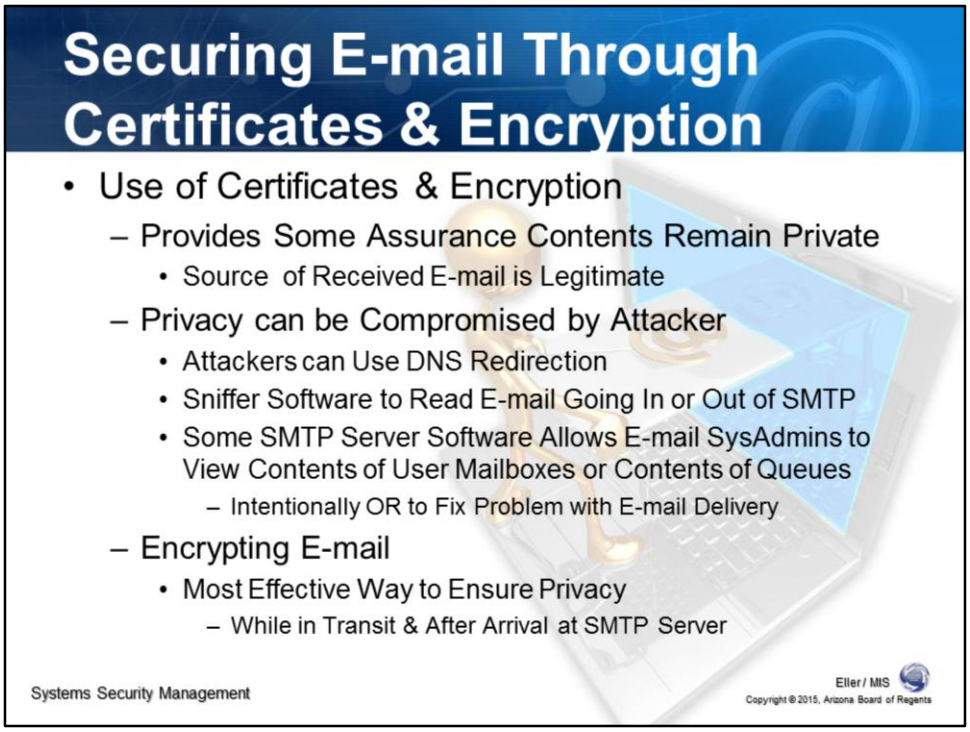


Unsolicited Commercial E-mail (continued)

If it is necessary to maintain an open SMTP relay server, the SysAdmin needs to configure the server to have restrictions, including:

- Only Specific Systems are Defined to Allow Relay
- Require Authentication with SMTP Server Before Relay

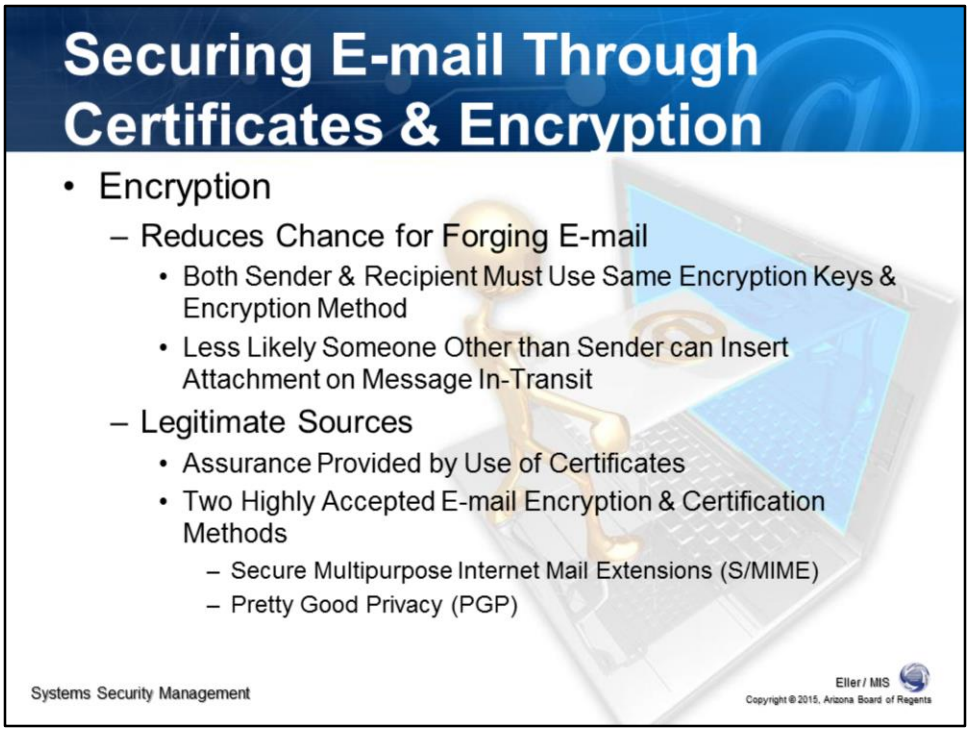
Depending on the type of SMTP server your organization deploys, they may find there are not enough options available to turn off relaying, add restrictions, or require authentication. If this is the case, then direct e-mail not addressed to local recipients should be sent to a bogus IP address. The relayed e-mails are then dropped by the SMTP server and never arrive at their destination. The SysAdmin can alternatively obtain third party tools designed to help block UCE from being relayed.



Securing E-mail Through Certificates and Encryption

One way to secure e-mail is through the use of certificates and encryption. This helps to provide some assurance the contents of the e-mail remain private and the source of the message is legitimate. Remember, privacy can be compromised by an attacker through DNS redirection, sniffer software, or in some cases the SysAdmin has software that allows him or her to view the contents of user mailboxes or the contents when e-mail is in a queue waiting to be sent. This software can be legitimate for fixing problems with e-mail delivery; however, it can also be used for spying.

In order to prevent these attacks, the contents of your messages can be encrypted in order to ensure privacy while in transit and after arrival at the SMTP server.

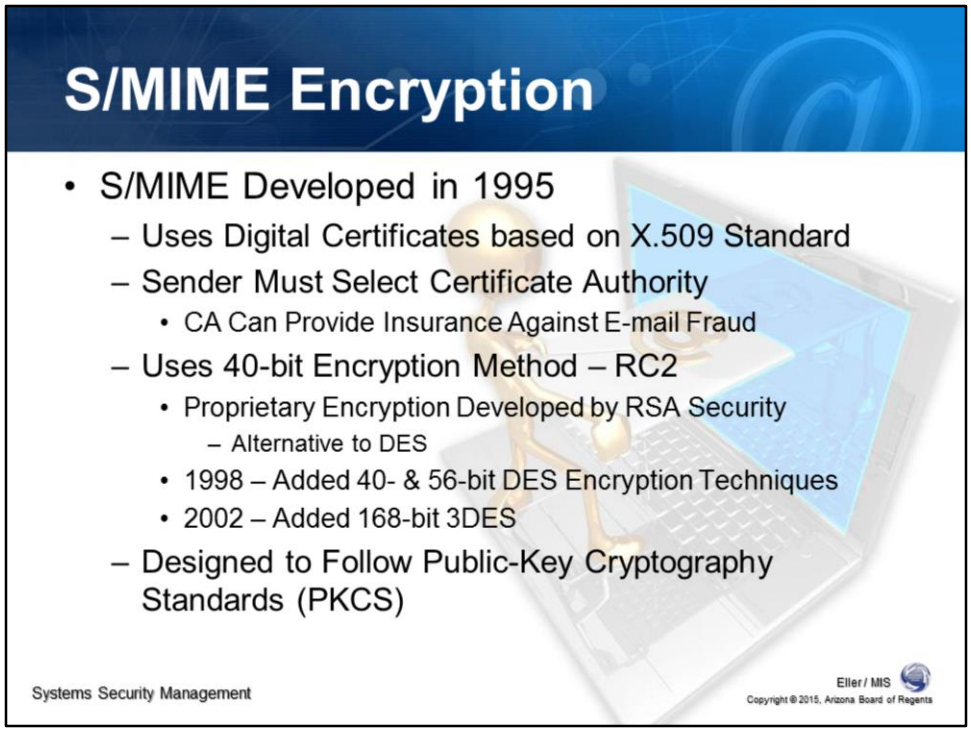


Securing E-mail Through Certificates and Encryption (continued)

Encryption also reduces the chance for forging e-mail, since both the sender and receiver must use the same encryption keys and encryption method in order to read the message. This makes it less likely someone other than the sender can insert attachments on a message in-transit.

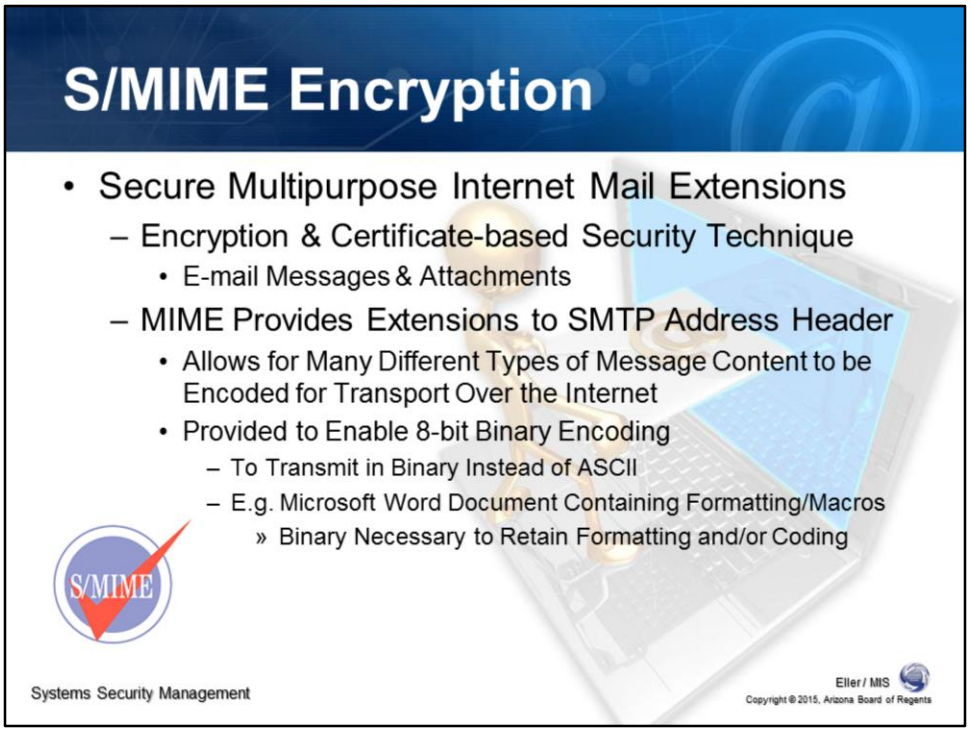
Legitimate sources will provide some assurance through the use of certificates. There are two highly accepted e-mail encryption and certification methods in use today:

- Secure Multipurpose Internet Mail Extensions (S/MIME)
- Pretty Good Privacy (PGP)



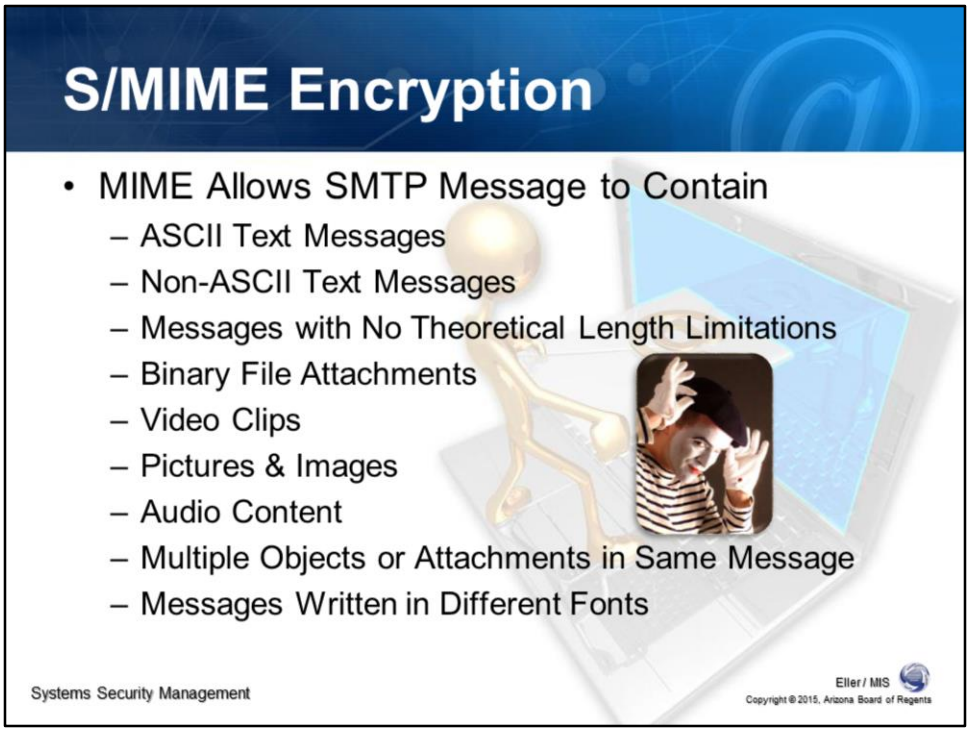
S/MIME Encryption

Secure MIME, or S/MIME, was developed in 1995 and uses digital certificates based on the X.509 standard. The sender must select a certificate authority, or CA, which can provide insurance against e-mail fraud. S/MIME uses a 40-bit encryption method called RC2, which is a proprietary encryption method developed by RSA security as an alternative to DES. Since its inception, S/MIME has been modified twice: in 1998 and again in 2002. In 1998, S/MIME added the ability to encrypt messages using either a 40-bit or 56-bit DES encryption technique. In 2002, S/MIME added a 168-bit 3DES encryption technique. S/MIME has been designed to follow the public-key cryptography standards, or PKCS.



S/MIME Encryption (continued)

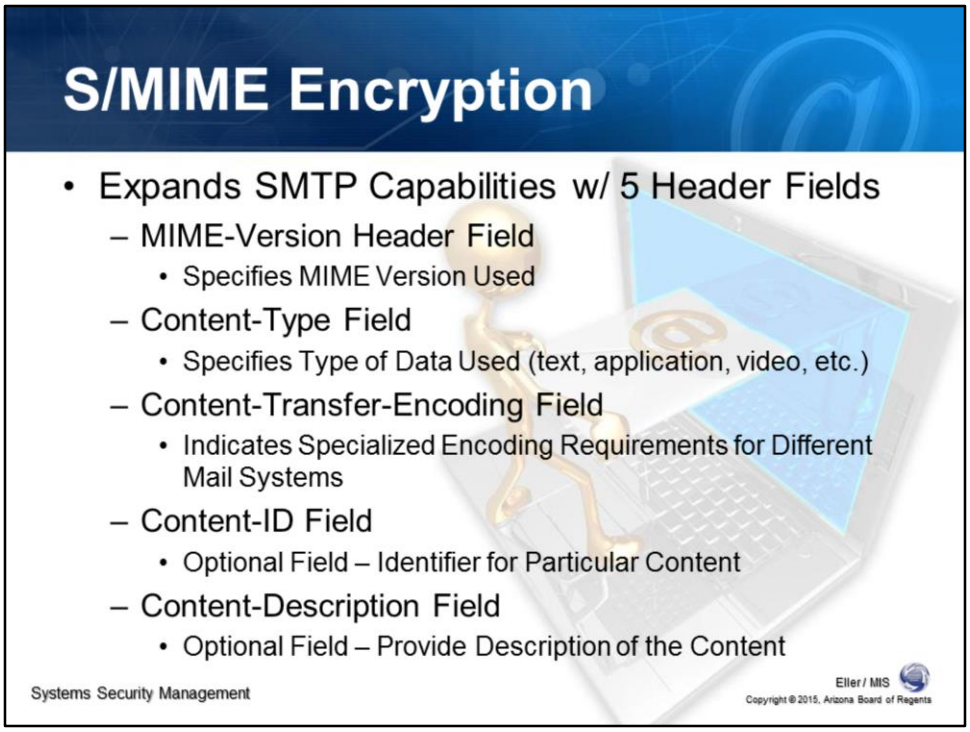
So, the Secure Multipurpose Internet Mail Extensions are both an encryption and certificate-based security technique for e-mail messages and attachments. MIME provides extensions to the SMTP address header which allows for many different types of message content to be encoded for transport over the Internet. MIME was provided to enable 8-bit binary encoding so attachments could be transmitted in binary instead of ASCII. So, for example, a Microsoft Word document containing formatting or macros will require binary in order to retain the formatting and coding.



S/MIME Encryption (continued)

MIME and S/MIME will allow an SMTP message to contain:

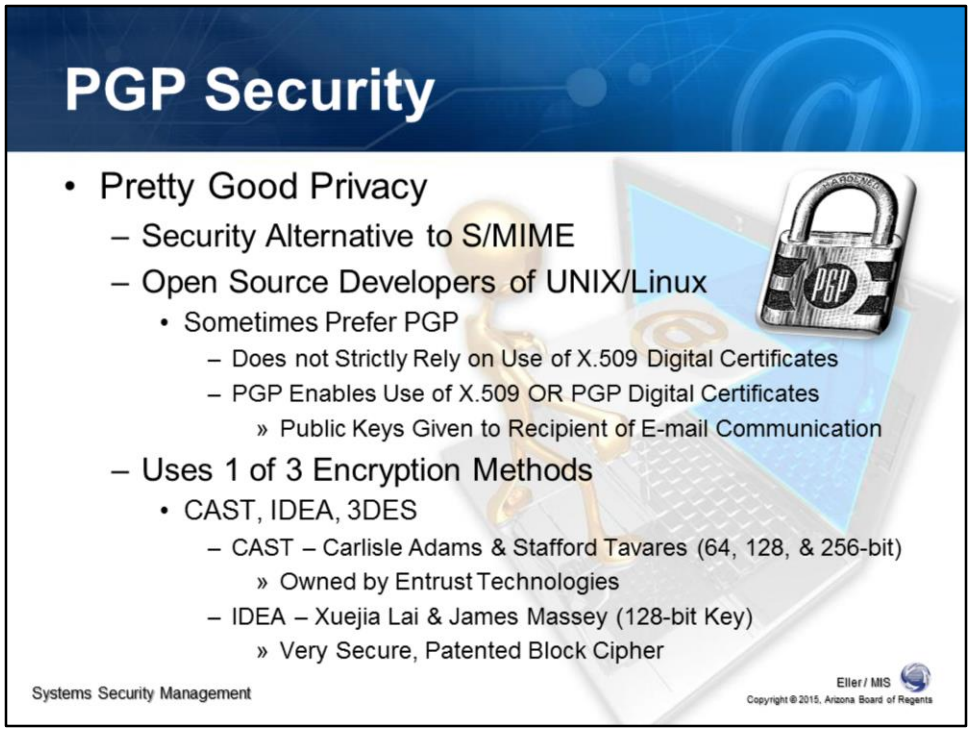
- ASCII Text Messages
- Non-ASCII Text Messages
- Messages with No Theoretical Length Limitations
- Binary File Attachments
- Video Clips
- Pictures & Images
- Audio Content
- Multiple Objects or Attachments in Same Message
- Messages Written in Different Fonts



S/MIME Encryption (continued)

MIME and S/MIME expand SMTP capabilities with the addition of 5 header fields:

- **MIME-Version Header Field** – Specifies MIME Version Used
- **Content-Type Field** – Specifies Type of Data Used (text, application, video, etc.)
- **Content-Transfer-Encoding Field** – Indicates Specialized Encoding Requirements for Different Mail Systems
- **Content-ID Field** – Optional Field – Identifier for Particular Content
- **Content-Description Field** – Optional Field – Provide Description of the Content

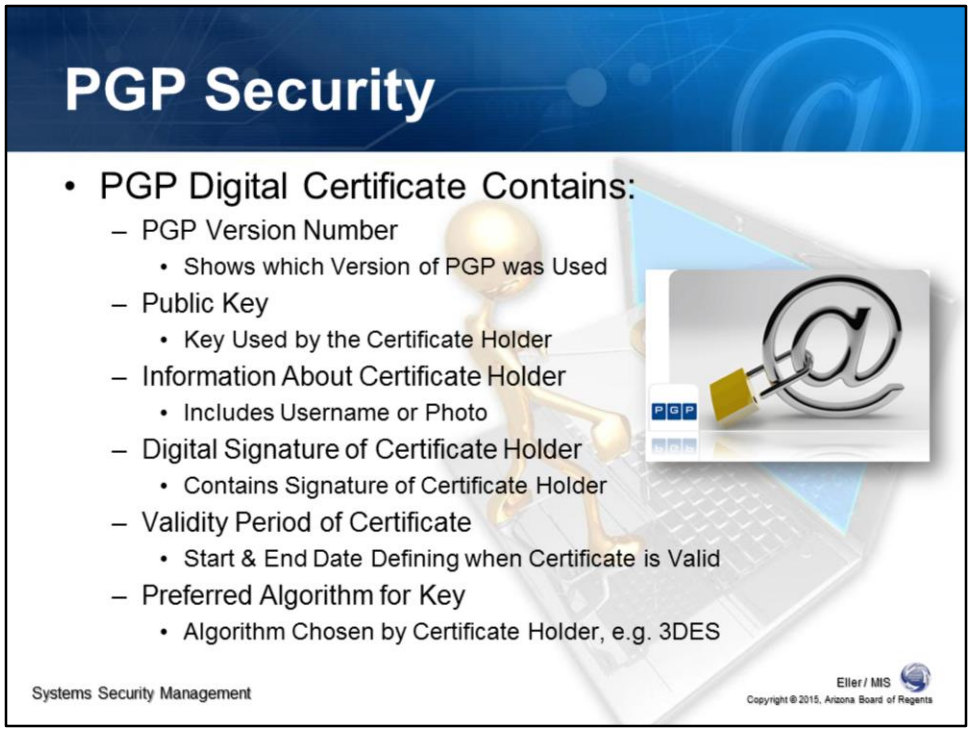


PGP Security

Pretty Good Privacy, or PGP, is a security alternative to S/MIME. PGP is one of the preferred methods for secure e-mail by the open source developers working on UNIX and Linux systems. This is because PGP does not strictly rely on the use of X.509 digital certificates, as it allows the user to choose whether to use X.509 or use PGP digital certificates. Public keys will be given to the recipients of any e-mail communication.

PGP uses one of three different encryption methods: CAST, IDEA, and 3DES.

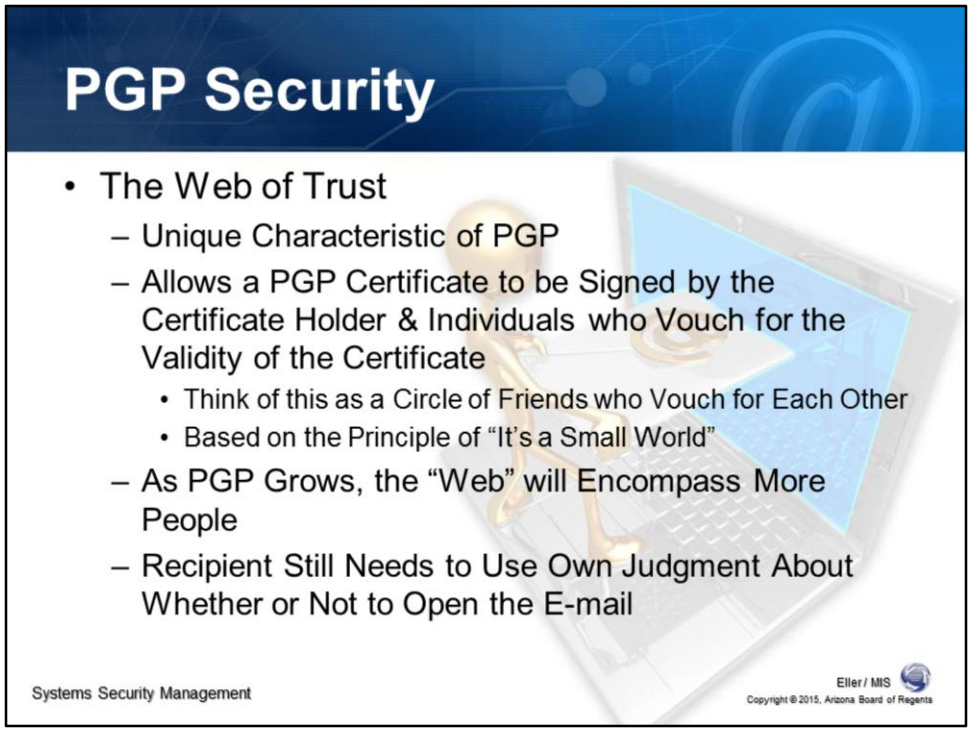
- **CAST** – Carlisle Adams & Stafford Tavares (64, 128, & 256-bit) – Owned by Entrust Technologies
- **IDEA** – Xuejia Lai & James Massey (128-bit Key) – Very Secure, Patented Block Cipher



PGP Security (continued)

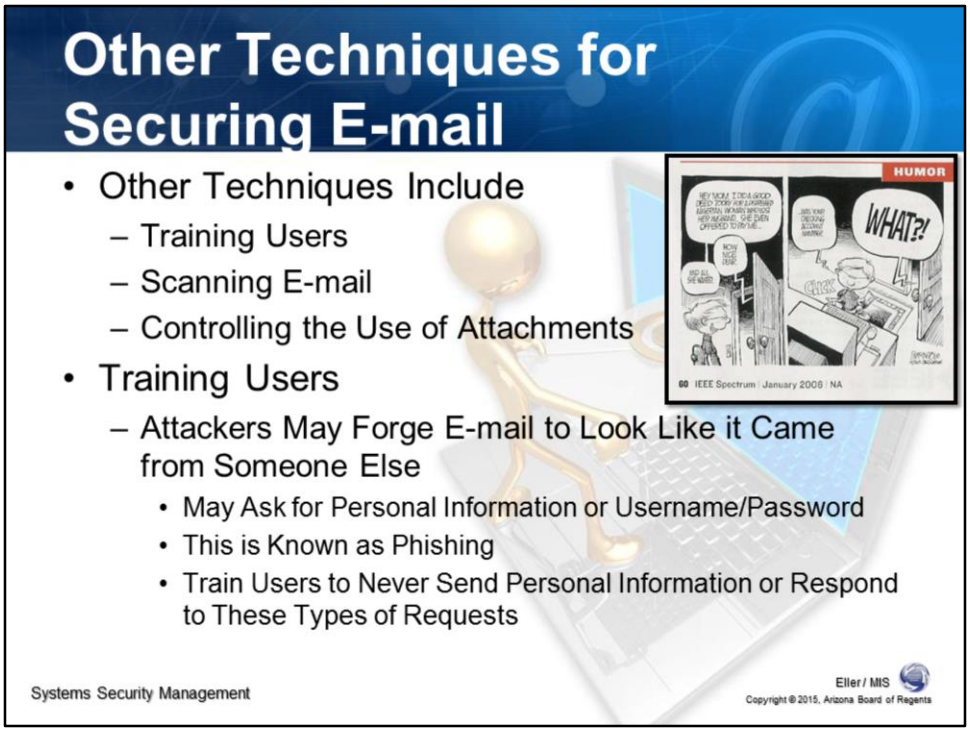
A PGP digital certificate contains the following information:

- **PGP Version Number** – Shows which Version of PGP was Used
- **Public Key** – Key Used by the Certificate Holder
- **Information About Certificate Holder** – Includes Username or Photo
- **Digital Signature of Certificate Holder** – Contains Signature of Certificate Holder
- **Validity Period of Certificate** – Start & End Date Defining when Certificate is Valid
- **Preferred Algorithm for Key** – Algorithm Chosen by Certificate Holder, e.g. 3DES



PGP Security (continued)

PGP is designed around the concept of a "web of trust." This is a unique characteristic of PGP, which allows the PGP certificate to be signed by the certificate holder and individuals who vouch for the validity of the certificate. This is like a circle of friends who each vouch for one another and is based on the principle of "it's a small world." As PGP use grows, the "web of trust" will encompass more people. However, the recipient will still need to use their own judgment about whether or not to open an e-mail.

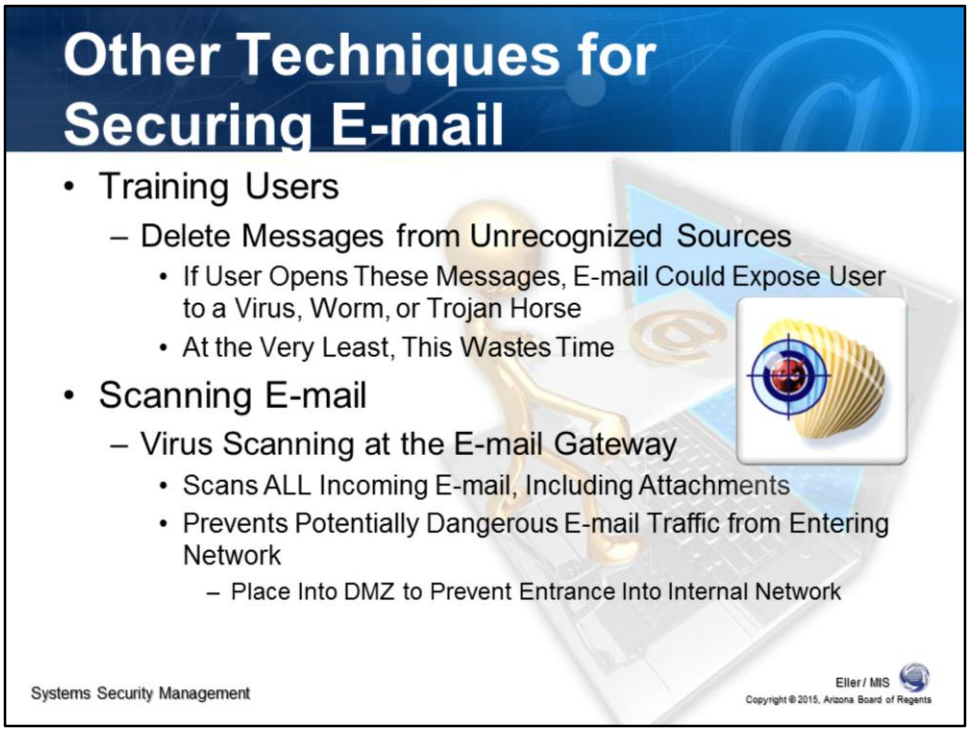


Other Techniques for Securing E-mail

Other techniques for securing e-mail include training users, scanning e-mail, and controlling the use of attachments.

Training Users

User training can be one of the most cost-effective ways of guarding against e-mail attacks. Since an attacker may forge e-mail to look like it came from someone else, these messages may ask for personal information or a username and password. This is known as phishing, and users should to trained to recognize these types of messages. They will also need to understand why they should never send personal information or respond to these types of requests.



Other Techniques for Securing E-mail (continued)

Training Users (continued)

Users should also be trained to delete messages from unrecognized sources. If a user opens these messages, the e-mail could expose the user to a virus, worm, or Trojan horse; however, at the very least, opening these messages just wastes time.

Scanning E-Mail

Some organizations choose to deploy a device on the network designed to scan all incoming e-mail and attachments for viruses before forwarding the messages to the e-mail gateway. This type of system helps to prevent potentially dangerous e-mail traffic from entering the network. SysAdmins should deploy these systems in a DMZ, assuming the network is configured with one, in order to prevent the malicious e-mail from entering into the private network.

Other Techniques for Securing E-mail (continued)

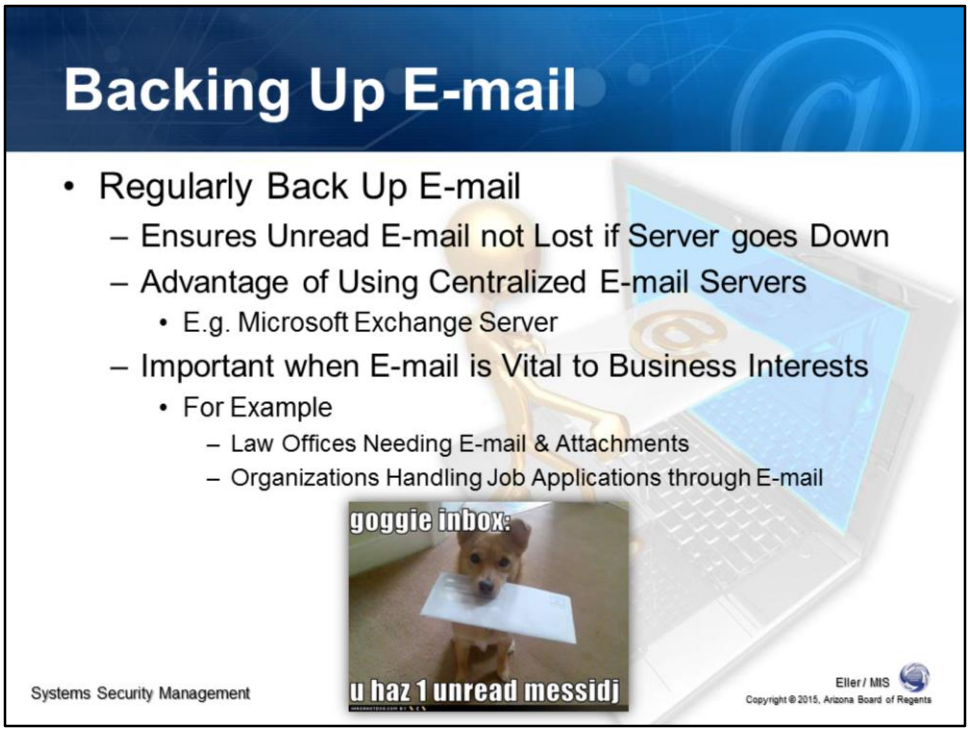
Some of these types of virus scanners are designed to strip specific attachment types, such as executable programs or scripts, from e-mail. These systems should have frequent virus definition updates, and attachments should be placed into a quarantine area on the scanner system, just in case they were removed due to a false positive trigger. Virus scanners should be able to scan compressed (.zip) files to ensure they do not contain any malware, and they should be very fast, otherwise the e-mail system will slow down considerably.

Other Techniques for Securing E-mail (continued)

One final technique for securing e-mail involves controlling the use of attachments, since attachments offer many opportunities to spread malware. Attachments can be executables, scripts, or be designed to point a web browser to malicious sites that contain malware. There are several immediate ways for users to protect themselves, including:

- Delete Attachments from Unknown Sources
- Never Configure Clients to Immediately Open Attachments
- Avoid Using HTML Format for Opening E-mail
- Use a Virus Scanner on Received E-mail
- Place Attachments in Quarantined Area

One suggestion would be to instruct users to not send file attachments. Instead they should send the network location where the file can be accessed by the recipient.



Backing Up E-Mail

Finally, one of the most important things the SysAdmin and users can do is backup e-mail regularly. This ensures that unread e-mails are not lost if the server itself goes offline. The advantage for an organization using a centralized system such as Microsoft's Exchange Server is the organization can backup the server during its regular backup schedule.

Backing up e-mail is extremely important when e-mail is vital to the organization's business interests. For example:

- Law Offices Needing E-mail & Attachments
- Organizations Handling Job Applications through E-mail

There are many other examples. The point here is if e-mail is important to the organization, then all e-mail should be backed up regularly to prevent the loss of data and productivity that can occur.

In the next module we will discuss Disaster Recovery, Business Continuity, and Incident Response, including:

- Disasters
- Uninterruptable Power Supplies
- Hardware Redundancy & Fault Tolerance
- Multiprocessor Systems and Clustering Services
- Placing Servers in Different Locations
- Data Warehousing
- Redundant Array of Independent Disks
- Backups including Remote vs. Local Backups and Media Rotation
- Business Continuity
- Vendor Cooperation
- Law Enforcement
- Intrusion Detection
- Isolation & Mediation
- Incident & Violation Responses
- Corrective Actions

References

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

Spam statistics and facts. (2015). *SPAM Laws*. Retrieved from http://www.spamlaws.com/spam-stats.html.

What is Electronic Mail? (2010). *Dave's Beginners Guide to the Internet*. Retrieved from http://www.davesite.com/webstation/inet101/mail01.shtml.