National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-45
Version 2

Guidelines on Electronic Mail Security

Recommendations of the National Institute of Standards and Technology

Miles Tracy
Wayne Jansen
Karen Scarfone
Jason Butterfield

NIST Special Publication 800-45
Version 2

Guidelines on Electronic Mail Security

Recommendations of the National Institute of Standards and Technology

Miles Tracy, Wayne Jansen, Karen Scarfone, and Jason Butterfield

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2007

U .S. Department of Commerce

Carlos M. Gutierrez, Secretary

Technology Administration

Robert C. Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology

William Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-45 Version 2
Natl. Inst. Stand. Technol. Spec. Publ. 800-45 Version 2, 139 pages (Feb. 2007)

Acknowledgements, Version 2

The authors, Wayne Jansen and Karen Scarfone of NIST, Miles Tracy of Federal Reserve Information Technology, and Jason Butterfield of Booz Allen Hamilton, wish to express their thanks to colleagues at both organizations who reviewed drafts of this document. In particular, their appreciation goes to Linda Antil, Rick Ayers, Bill Burr, Tim Grance, and Tim Polk from NIST for their research, technical support, and written contributions to this version of the document. The authors would also like to express their thanks to all those who contributed input during the public comment period and who assisted with our internal review process.

Acknowledgements, Original Version

The authors, Wayne Jansen of NIST and Scott Bisker and Miles Tracy of Booz Allen Hamilton (BAH), wish to express their thanks to colleagues at both organizations who reviewed drafts of this document. In particular, their appreciation goes to John Wack, Murugiah Souppaya, and Tim Grance from NIST, and Steve Allison, Alexis Feringa, Jonathan Holleran, Kevin Kuhlkin, and Mark McLarnon from BAH, for their research, technical support, and written contributions to this document. The authors would also like to express their thanks to all those who contributed input during the public comment period and who assisted with our internal review process.

Table of Contents

Appendices

List of Tables and Figures

This page has been left blank intentionally.

Executive Summary

Electronic mail (email) is perhaps the most popularly used system for exchanging business information over the Internet (or any other computer network). At the most basic level, the email process can be divided into two principal components: (1) mail servers, which are hosts that deliver, forward, and store email; and (2) mail clients, which interface with users and allow users to read, compose, send, and store email. This document addresses the security issues of mail servers and mail clients, including Web-based access to mail.

Mail servers and user workstations running mail clients are frequently targeted by attackers. Because the computing and networking technologies that underlie email are ubiquitous and well-understood by many, attackers are able to develop attack methods to exploit security weaknesses. Mail servers are also targeted because they (and public Web servers) must communicate to some degree with untrusted third parties. Additionally, mail clients have been targeted as an effective means of inserting malware into machines and of propagating this code to other machines. As a result, mail servers, mail clients, and the network infrastructure that supports them must be protected. Examples of email security issues include the following:

- To exchange email with the outside world, a requirement for most organizations, it is allowed through organizations' network perimeter defenses. At a basic level, viruses and other types of malware may be distributed throughout an organization via email. Increasingly, however, attackers are getting more sophisticated and using email to deliver targeted zero-day attacks in an attempt to compromise users' workstations within the organization's internal network.
- Given email's nature of human to human communication, it can be used as a social engineering vehicle. Email can allow an attacker to exploit an organization's users to gather information or get the users to perform actions that further an attack.
- Flaws in the mail server application may be used as the means of compromising the underlying server and hence the attached network. Examples of this unauthorized access include gaining access to files or folders that were not meant to be publicly accessible, and being able to execute commands and/or install software on the mail server.
- Denial of service (DoS) attacks may be directed to the mail server or its support network infrastructure, denying or hindering valid users from using the mail server.
- Sensitive information on the mail server may be read by unauthorized individuals or changed in an unauthorized manner.
- Sensitive information transmitted unencrypted between mail server and client may be intercepted. All popular email communication standards default to sending usernames, passwords, and email messages unencrypted.
- Information within email messages may be altered at some point between the sender and recipient.
- Malicious entities may gain unauthorized access to resources elsewhere in the organization's network via a successful attack on the mail server. For example, once the mail server is compromised, an attacker could retrieve users' passwords, which may grant the attacker access to other hosts on the organization's network.
- Malicious entities may attack external organizations from a successful attack on a mail server host.

- Misconfiguration may allow malicious entities to use the organization's mail server to send email-based advertisements (i.e., spam).
- Users may send inappropriate, proprietary, or other sensitive information via email. This could expose the organization to legal action.

This document is intended to assist organizations in installing, configuring, and maintaining secure mail servers and mail clients. More specifically, this document discusses the following items in detail:

- Email standards and their security implications
- Email message signing and encryption standards
- Planning and management of mail servers
- Securing the operating system underlying a mail server
- Mail server application security
- Email content filtering
- Email-specific considerations in the deployment and configuration of network protection mechanisms, such as firewalls, routers, switches, and intrusion detection and intrusion prevention systems
- Securing mail clients
- Administering the mail server in a secure manner, including backups, security testing, and log reviews.

The following key guidelines are recommended to Federal departments and agencies for maintaining a secure mail server.

Organizations should carefully plan and address the security aspects of the deployment of a mail server.

As it is much more difficult to address security once deployment and implementation have occurred, security should be considered from the initial planning stage. Organizations are more likely to make decisions about configuring computers appropriately and consistently when they develop and use a detailed, well-designed deployment plan. Developing such a plan will support mail server administrators in making the inevitable tradeoff decisions between usability, performance, and risk.

Organizations often fail to take into consideration the human resource requirements for both deployment and operational phases of the mail server and supporting infrastructure. Organizations should address the following points in a deployment plan:

- Types of personnel required (e.g., system and mail server administrators, network administrators, information systems security officers)
- Skills and training required by assigned personnel
- Availability of personnel.

Organizations should implement appropriate security management practices and controls when maintaining and operating a secure mail server.

Appropriate management practices are essential to operating and maintaining a secure mail server. Security practices entail the identification of an organization's information system assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines that help to ensure the confidentiality, integrity, and availability of information system resources.

To ensure the security of a mail server and the supporting network infrastructure, the following practices should be implemented:

- Organization-wide information system security policy
- Configuration/change control and management
- Risk assessment and management
- Standardized software configurations that satisfy the information system security policy
- Security awareness and training
- Contingency, continuity of operations, and disaster recovery planning
- Certification and accreditation.

Organizations should ensure that the mail server operating system is deployed, configured, and managed to meet the security requirements of the organization.

The first step in securing a mail server is securing the underlying operating system. Most commonly available mail servers operate on a general-purpose operating system. Many security issues can be avoided if the operating systems underlying mail servers are configured appropriately. Default hardware and software configurations are typically set by manufacturers to emphasize features, functions, and ease of use at the expense of security. Because manufacturers are not aware of each organization's security needs, each mail server administrator must configure new servers to reflect their organization's security requirements and reconfigure them as those requirements change. Using security configuration guides or checklists can assist administrators in securing systems consistently and efficiently. Securing an operating system would generally include the following steps:

- Patching and updating the operating system
- Removing or disabling unnecessary services and applications
- Configuring operating system user authentication
- Configuring resource controls
- Installing and configuring additional security controls, if needed
- Performing security tests on the operating system.

Organizations should ensure that the mail server application is deployed, configured, and managed to meet the security requirements of the organization.

In many respects, the secure installation and configuration of the mail server application mirrors the operating system process discussed above. The overarching principle, as before, is to install the minimal

mail server services required and eliminate any known vulnerabilities through patches or upgrades. If the installation program installs any unnecessary applications, services, or scripts, they should be removed immediately after the installation process completes. Securing the mail server application would generally include the following steps:

- Patch and upgrade the mail server application
- Remove or disable unnecessary services, applications, and sample content
- Configure mail server user authentication and access controls
- Configure mail server resource controls
- Test the security of the mail server application.

Organizations should consider the implementation of cryptographic technologies to protect user authentication and email data.

Most standard email protocols default to unencrypted user authentication and send email data in the clear (unencrypted). Sending this data in the clear may allow an attacker to easily compromise a user account and/or intercept and alter unencrypted emails. At a minimum, most organizations should encrypt the user authentication session even if they do not encrypt the email data itself. Encrypted user authentication is now supported by most standard and proprietary mailbox protocols.

The issues involved with encrypted and signed email data are more complex. Encrypting and signing email places a greater load on the organization's network infrastructure, may complicate malware scanning and email content filtering, and often requires significant administrative overhead. However, for many organizations the benefits of email encryption and signatures will outweigh the costs.

Organizations should employ their network infrastructure to protect their mail server(s).

The network infrastructure (e.g., firewalls, routers, intrusion detection systems) that supports the mail server plays a critical role in the security of the mail server. In most configurations, the network infrastructure will be the first line of defense between the Internet and a mail server. Network design alone, however, cannot protect a mail server. The frequency, sophistication, and variety of mail server attacks perpetrated today support the idea that mail server security must be implemented through layered and diverse protection mechanisms.

Organizations should ensure that the mail clients are deployed, configured, and used properly to meet the security requirements of the organization.

In many respects, the client side of email represents a greater risk to security than the mail server. Numerous issues need to be carefully considered and addressed to provide an appropriate level of security for mail clients. Securely installing, configuring, and using mail client applications would generally include the following steps:

- Patch and upgrade the mail client applications
- Configure mail client security features, such as disabling automatic opening of messages and enabling anti-spam and anti-phishing features
- Configure mailbox authentication and access

- Secure the client host's operating system.

Maintaining the security of a mail server is an ongoing process.

Maintaining a secure mail server requires constant effort, resources, and vigilance from an organization. Securely administering a mail server on a daily basis is an essential aspect of mail server security. Maintaining the security of a mail server will usually involve the following steps:

- Configuring, protecting, and analyzing log files
- Backing up data frequently
- Protecting against malware (e.g., viruses, worms, Trojan horses)
- Establishing and following procedures for recovering from compromise
- Testing and applying patches in a timely manner
- Testing security periodically.

This page has been left blank intentionally.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

The purpose of the *Guidelines on Electronic Mail Security* is to recommend security practices for designing, implementing, and operating email systems on public and private networks. While intended as recommended guidance for Federal departments and agencies, it may be used in the private sector on a voluntary basis.

Mail servers are frequently targeted by attackers. Various types of email content and attachments have also proven to be effective in introducing viruses and other malware into networks through mail clients. Email is extensively used as a vector to deliver attacks that exploit vulnerabilities in users' workstations or use social engineering methods to trick users. These attacks often lead to the compromise of the user workstation or the release of sensitive information even when the email client is securely configured. This document may be used by organizations interested in enhancing security on existing and future mail systems to reduce the number and frequency of email-related security incidents. This document presents generic principles that apply to all systems.

This guideline does not cover the following aspects relating to securing a mail server:

- Securing other types of network servers
- Firewalls and routers used to protect mail servers beyond a basic discussion in Section 7.2.1
- Special considerations for high traffic mail servers with multiple hosts
- Securing backend servers that may support the mail server (e.g., syslog hosts, file servers)
- Security of the X.400 standard messaging protocol.

1.3 Audience and Assumptions

The document, while technical in nature, provides the background information to help readers understand the topics that are discussed. The intended audience for this document includes the following:

- Users when setting up mail clients and accessing email
- System engineers and architects when designing and implementing mail systems
- System administrators when administering or upgrading mail systems
- Program managers and information technology (IT) security officers to ensure that adequate security measures have been considered for all phases of the system's life cycle.

The practices recommended in this document are designed to help mitigate the risks associated with email and other known security problems. They build on and assume the implementation of practices described in other NIST guidelines listed in Appendix E.

1.4 Document Organization

The remainder of this document is organized into the following eight major sections:

- Section 2 includes background information and standards relating to email.
- Section 3 contains information on protecting email messages by signing and encrypting them.
- Section 4 discusses the planning and management of a mail server.
- Section 5 presents an overview of securing the underlying operating system of a mail server.
- Section 6 discusses securing a mail server application, protecting messages traversing the server, and securing access to mailboxes.
- Section 7 addresses protecting a mail server through the supporting network infrastructure.
- Section 8 provides information regarding mail client security.
- Section 9 discusses the basics of securely administering a mail server on a daily basis.

The document also contains several appendices with supporting material:

- Appendix A defines terms used in this document.
- Appendix B lists relevant Request for Comment (RFC) documents.
- Appendix C lists references used in this document.
- Appendix D identifies email security tools and applications.
- Appendix E lists online email security resources.
- Appendix F presents a set of mail server and client security checklists.
- Appendix G lists the acronyms used throughout the document.
- Appendix H contains the index for the document.

2. Background and Standards

As of January 2007, the estimated number of Internet users worldwide exceeded one billion.[1] Most of these users have electronic mail (email) accounts on one or more mail systems, which is a huge leap from its inception in 1971, when Ray Tomlinson, a Department of Defense (DoD) researcher, sent the first ARPANET email message to himself. The ARPANET, precursor to the Internet, was a United States (U.S.) Advanced Research Project Agency (ARPA) project intended to develop a set of communications protocols to transparently connect computing resources in various geographical locations. Messaging applications were available on ARPANET systems; however, they could only be used for sending messages to users with local system accounts. Tomlinson modified the existing messaging system so that users could send messages to users on other ARPANET connected systems. After Tomlinson's modification was available to other researchers, email quickly became the most heavily used application on the ARPANET.

As the ARPANET evolved into the Internet, email remained one of the most heavily used applications for personal and business users. Since the ARPANET was initially a small and trusted community, there was little need for security. The growth in the popularity of the Internet greatly increased the need for security. Unfortunately, the needed security was lacking because early email standards and implementations placed little emphasis on security. Maintaining compatibility with these standards presents a great challenge in securing email today.

2.1 Background

An understanding of how email messages are composed, delivered, and stored is helpful in understanding email security. For most email users, once a message is composed and sent, it leaves the computer and magically appears in the intended recipient's inbox. This may seem simple but the handling and delivery of an email message can be as complex as that involving physical mail, with processing and sorting occurring at several intermediary locations before arriving at the final destination.

The process starts with message composition. The most basic mail clients typically ask the user to provide the following: subject line, message content, and intended recipients. When these fields are completed and the user sends the message, the message is transformed into a specific standard format specified by Request for Comments (RFC) 2822, *Internet Message Format*. At the most basic level, the two primary message sections are the header and the body. The header section contains the vital information about the message including origination date, sender, recipient(s), delivery path, subject, and format information. The body of the message contains the actual content of the message.[2]

Once the message is translated into an RFC 2822 formatted message, it can be transmitted. Using a network connection, the mail client, referred to as a mail user agent (MUA), connects to a mail transfer agent (MTA) operating on the mail server. After initiating communication, the mail client provides the sender's identity to the server. Next, using the mail server commands, the client tells the server who the intended recipients are. Although the message contains a list of intended recipients, the mail server does not examine the message for this information. Only after the complete recipient list is sent to the server does the client supply the message. From this point, message delivery is under control of the mail server.

---

1 World Internet Usage and Population Statistics, http://www.internetworldstats.com/stats.htm.

2 Refer to RFC 2822 for additional information on message headers. Appendix B contains a comprehensive list of email-related RFCs that includes the URLs for many mail-related RFCs. It also indicates which RFCs are considered standards and which are informational, standards in progress, or best current practices (BCP).

Once the mail server is processing the message, several events occur: recipient server identification, connection establishment, and message transmission. Using Domain Name System (DNS) services, the sender's mail server determines the mail server(s) for the recipient(s). Then, the server opens up a connection(s) to the recipient mail server(s) and sends the message employing a process similar to that used by the originating client. At this point, one of two events could occur. If the sender's and recipient's mailboxes are located on the same mail server, the message is delivered using a local delivery agent (LDA). If the sender's and recipient's mailboxes are located on different mail servers, the send process is repeated from one MTA to another until the message reaches the recipient's mailbox.

When the LDA has control of the message, a number of possible events may occur. Depending on the configuration, the LDA could deliver the message or process the message based on a predefined message filter before delivery (filtering can be based on a number of message properties and is discussed in detail in Section 6.2.2). Once the message is delivered, it is placed in the recipient's mailbox where it is stored until the recipient performs some action on it (e.g., read, delete) using the MUA. Figure 2.1 illustrates the flow of the message through the various mail components discussed previously. This is the general process of sending an email.

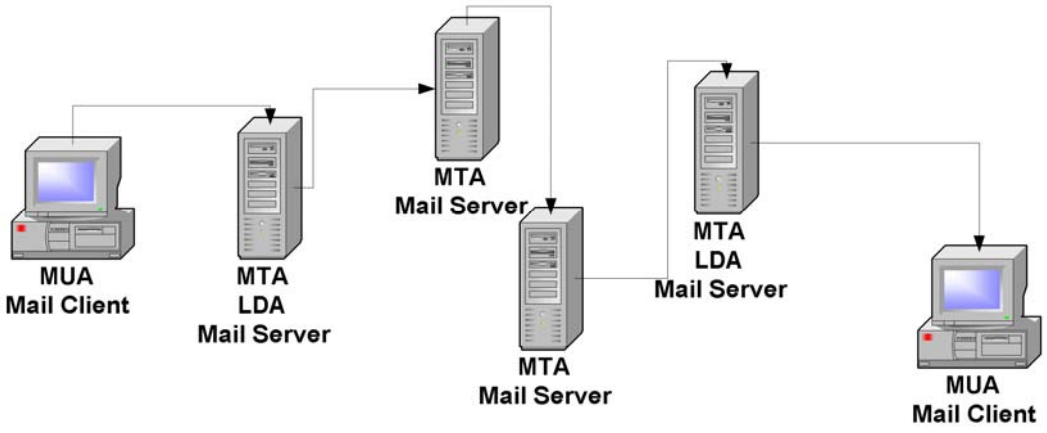

Figure 2.1: Example of Message Flow

2.2 Multipurpose Internet Mail Extensions

RFC 2822 provides a standard for transmitting messages containing textual content; however, it does not address messages that contain attachments, such as a mail message with a word processing document or photo included. Making use of the headers in an RFC 2822 message, the Multipurpose Internet Mail Extensions (MIME) provide almost endless possibilities to describe the structure of rich message content. MIME uses the convention of content-type/subtype pairs to specify the native representation or encoding of associated data. Examples of content types include the following:

- Audio – for transmitting audio or voice data.
- Application – used to transmit application data or binary data.
- Image – for transmitting still image (picture) data.
- Message – for encapsulating another mail message.
- Multipart – used to combine several message body parts, possibly of differing types of data, into a single message.

- Text – used to represent textual information in a number of character sets and formatted text description languages in a standardized manner.
- Video – for transmitting video or moving image data, possibly with audio as part of the composite video data format.

The current MIME standards include five parts: RFCs 2045, 2046, 2047, 4289 (which replaced 2048), and 2049 (see Appendix B). They address message body format, media types, non-American Standard Code for Information Interchange (non-ASCII) message header extensions, registration procedures, and conformance criteria, respectively. With this added functionality, email features such as message attachments and inline hypertext markup language (HTML) are possible. Although MIME extensions allow for binary message content, such content is incorporated into an RFC 2822 message using Base64 encoding, which provides a textual representation of binary data.[3]

2.3 Mail Transport Standards

To ensure reliability and interoperability among various mail applications, mail transport standards were established. In the simplest scenario, an email message is sent from one local user to another local user. For this case, an LDA is responsible for placing the message in the appropriate mailbox. When a message is sent to non-local recipients, an MTA is needed to send the message from the local mail server to the remote mail server. Depending on the type of systems involved, different MTAs may be used, which in turn may support different implementations of a particular message transfer protocol or more than one distinct transfer protocol.

The most common MTA transfer protocol is the Simple Mail Transfer Protocol (SMTP). SMTP is the de-facto Internet standard for sending email messages. Thus, any Internet messaging system must support SMTP to facilitate communication with other email messaging applications. Other messaging systems exist that use different MTA transfer protocols between similar or clustered messaging systems. For the most part, these MTAs are proprietary and work only with specific systems. Sections 2.3.1 and 2.3.2 provide background information on SMTP and SMTP extensions, while Section 2.3.3 discusses proprietary MTAs.

2.3.1 Simple Mail Transfer Protocol

Jon Postel of the University of Southern California developed SMTP in August 1982. As RFC 821, *Simple Mail Transfer Protocol,* states, "SMTP was developed to ensure a more reliable and efficient way to transport messages." At the most basic level, SMTP is a minimal language that defines a communications protocol for delivering email messages. Figure 2.2 lists the SMTP commands and syntax as defined in RFC 2821, *Simple Mail Transfer Protocol*, which replaced RFC 821.

[3] Base64 encoding was originally derived from RFC 1421 for Privacy Enhanced Mail (PEM).

HELO <domain>	(Hello) Connect to the server as specified in <domain>
MAIL FROM:<reverse-path> [Mail-parameters]	Tell the server the sender's identity as specified in <reverse-path>
RCPT TO:<forward-path> [Rcpt-parameters]	(Recipient) Tell the server the intended recipient's identity as specified in <forward-path>
DATA	Convey the message body to the server
RSET	(Reset) Reset the server connection
VRFY <string>	(Verify) Ask the receiver to confirm that a user has been identified
EXPN <string>	(Expand) Ask the receiver to confirm that a mailing list has been identified
HELP [<string>]	Obtain help information
NOOP [<string>]	(No operation) Indicate no operation, but signify the sender is still connected (i.e.,"alive")
QUIT	Close the server connection

Figure 2.2: SMTP Commands

When a user sends an email, the client contacts its SMTP server and conducts a "conversation" using the SMTP language. A MUA is typically part of the mail client application (e.g., Outlook, Eudora). If an MUA is unavailable, email messages can be sent using a Telnet client connected to the SMTP service. Figure 2.3 depicts a sample SMTP conversation using Telnet. The Telnet and SMTP commands entered by the user for this session are shown in bold. During a manual SMTP Telnet session, the HELP command can be used to determine which of the SMTP commands are enabled on the server.

telnet mail.nowhere.com 25
Connected to mail.nowhere.com.
Escape character is '^]'.
220 test.mail.com SMTP Service (Sample Mail Server String)
HELO
250 test.mail.com
MAIL FROM: jdoe@nowhere.com
250 Sender <jdoe@nowhere.com> Ok
RCPT TO: jsmith@somewhere.com
250 Recipient <jsmith@somwhere.com> Ok
DATA
354 Ok Send data ending with <CRLF>.<CRLF>
Hello World!
.
250 Message received: GM1BAR00.F4M
QUIT
221 mail.nowhere.com SMTP server closing connection.
Connection closed by foreign host.

Figure 2.3: Sample SMTP Conversation

2.3.2 Simple Mail Transfer Protocol Extensions

As the number of email users grew, additional functionality was sought in mail clients and SMTP servers. For SMTP servers to support this additional functionality, extensions were added to SMTP. In 1993, RFC 1425 introduced the concept of SMTP service extensions. Subsequently, RFC 1425 was superseded by RFC 1651 in 1994, RFC 1869 in 1995, and RFC 2821 in 2001. These RFCs added three pieces to the SMTP framework:

- New SMTP commands (RFC 1425)
- Registry for SMTP service extensions (RFC 1651)
- Additional parameters for SMTP MAIL FROM and RCPT TO commands (RFC 1869).

To be compatible with older SMTP servers, there needed to be a method to allow the mail client application to determine whether the server supported extensions. This was accomplished through the "enhanced hello" (EHLO) command. When connecting to a server, a mail client could issue the EHLO command. If the server supported SMTP extensions, it would give a successful response and list the extensions that were supported. If the server did not support SMTP extensions, it would issue a command failure response prompting the MUA to respond with the standard HELO command. Servers that support SMTP extensions, also known as Extended SMTP (ESMTP), typically respond with ESMTP in their banner.[4] Figure 2.4 is an excerpt from an ESMTP server transaction involving the EHLO command.

```
telnet mail.nowhere.com 25
Connected to mail.nowhere.com.
Escape character is '^]'.
220 test.mail.com ESMTP Service (Sample Mail Server String)
EHLO
250 test.mail.com says hello
250-HELP
250-EXPN
250 SIZE 20971520
…
```

Figure 2.4: Sample ESMTP Conversation

As depicted in Figure 2.4, the sample server supports only one extension – SIZE. Numerous extensions are supported by a variety of SMTP servers. Table 2.1 lists some of the more common SMTP extensions and their associated RFCs. In particular, RFC 2554 specifies a new command and protocol for identifying and authenticating a user. The default configuration of most mail servers typically does not have authenticated relay enabled.

[4] Many application services (e.g., email, Web, File Transfer Protocol) that operate on a server respond to a client request with a banner. This banner is a text message that contains information on the server such as application and operating system type and version. This information can be useful to attackers and should be changed as discussed later in the document. Most mail clients do not display this banner to the end user.

Table 2.1: SMTP Extensions

SMTP Extension	Associated RFC
SMTP Service Extension for Authentication	2554
SMTP Service Extension for Command Pipelining	2920
SMTP Service Extension for Delivery Status Notifications (DSNs)	3461
SMTP Service Extension for Message Size Declaration	1870
SMTP Service Extension for Message Tracking	3885
SMTP Service Extension for Remote Message Queue Starting	1985
SMTP Service Extension for Returning Enhanced Error Codes	2034
SMTP Service Extension for Secure SMTP over Transport Layer Security	3207
SMTP Service Extensions for Transmission of Large and Binary MIME Messages	3030

2.3.3 Proprietary Mail Transports

As mentioned previously, some messaging systems use MTAs that do not support either SMTP or ESMTP. These types of MTAs are designed to work within a closed messaging environment. Many large-scale government, academic, and private organizations have messaging systems that use these types of MTAs. However, these organizations still rely on SMTP or ESMTP-capable MTAs for communicating with external messaging systems. Some examples of messaging systems that use proprietary protocols are MTAs for Lotus Notes and Microsoft Exchange.[5] Discussion on the benefits and disadvantages of using MTAs that support only proprietary message transfer protocols is outside the scope of this document.

2.4 Client Access Standards

Once a message is delivered by the LDA, users need to access the mail server to retrieve the message. Mail clients (MUAs) are used to access the mail server and retrieve email messages. Several methods exist for users to access their mailboxes, the simplest being direct access.

The simplest scenario for a messaging system would be one in which all users have direct access to their mailbox (common on hosts employing the Unix operating system). For each account that exists on the system, there is a corresponding mailbox in that user's home directory. When messages are received, users can use command line-based mail programs, such as *mail* or *pine*, to directly access the mailbox. Although this method is straightforward, it requires all users accessing the mail server to receive messages to have a user account and a command-line interface on the host operating system.

Allowing users, particularly external users, to have access to a command-line interface is a significant security risk. To mitigate this risk, mailbox access protocols were devised. The two most widely supported mailbox access protocols are Post Office Protocol (POP) and Internet Message Access Protocol (IMAP). They are covered in Sections 2.4.1 and 2.4.2, respectively. As with message transfer protocols for MTAs, other proprietary mailbox access protocols exist that are regularly used by commercial software manufacturers; proprietary protocols are discussed in Section 2.4.3. It is important to understand that POP, IMAP, and indeed most proprietary protocols in their default configuration use cleartext

[5] These product families have SMTP MTAs as well as their proprietary MTAs.

passwords for authentication, which can be intercepted by other hosts attached to the network. Section 2.4.4 briefly discusses the protocols used for Web-based mail access.

2.4.1 Post Office Protocol

POP was first developed in 1984. At its core, POP was nothing more than a way to copy messages from the mail server mailbox to the mail client. It worked much like a traditional post office mailbox. The mail client opens a connection to the mail server mailbox, downloads the email messages, and then closes the connection. As described in RFC 918, only nine commands were originally available for POP (see "Basic Commands" in Figure 2.5).

Basic Commands from RFC 918	
USER <name>	Set username
PASS <password>	Set password
STAT	Check the status of the mailbox, typically retrieves number of messages
LIST [msg]	List messages in the mailbox; Optional argument for message [msg]
RETR <msg>	Retrieve message <msg>
DELE <msg>	Delete message <msg>
QUIT	Quit
NOOP	No operation
RSET	Reset
Optional Commands from RFC 1939	
TOP <msg> <n>	Retrieve the top <n> lines of message <msg>
UIDL [msg]	Retrieve unique id for [msg]
APOP <name> <digest>	A more robust form of authentication than USER/PASS
Extension Command from RFC 2449	
CAPA	Retrieve a list of capabilities supported by the POP3 server

Figure 2.5: POP3 Commands

Since 1984, POP has gone through several changes and is now in its third iteration as defined in RFC 1939. The basic command set is very similar to the command set of 1984; however, POP version 3 offers a few new optional commands, listed in Figure 2.5. From a security standpoint, the addition of the APOP was important, since it avoids transmitting a user's password in the clear. Instead, a challenge/response mechanism is used, by which the client responds with a cryptographic hash of the combined challenge sent from the server and the user's password, for verification by a POP mail server performing the same operation for the user in question.

RFC 2449, *POP3 Extension Mechanism*, defines an extension to POP3 that allows clients to discover additional information about POP3 servers, such as which extensions and optional commands they support. Figure 2.5 shows the command added to POP3 by the extension.

The POP mailbox access standard has some significant limitations. Typically, when users retrieve their email, copies of the messages that reside on the server are deleted. This means that the user has the sole responsibility of maintaining message archives. Although this may be acceptable for personal accounts, it is generally unacceptable for most commercial or governmental organizations that have to meet certain legal requirements. In addition, if a user employs several workstations for retrieving email, the messages are dispersed on multiple hosts. POP may be configured so that the original messages are not deleted from the server. However, the user will either have to download all of the messages previously viewed as

well as the new messages when accessing a mailbox from another host, or have to set up a retention period after which messages are automatically deleted from the server.

2.4.2 Internet Message Access Protocol

To address the above-mentioned issues with POP, IMAP was developed in 1988. The IMAP protocol was developed as a functional superset of the POP version 2 protocol. At the most basic level, IMAP was designed so user mailboxes could be centrally located and accessed from multiple mail clients or MUAs.

Initially, IMAP offered very little functionality beyond that of POP, but since 1988, it has evolved into a robust mailbox access protocol. The current edition of the IMAP standard is RFC 3501: *Internet Message Access Protocol – Version 4, Revision 1* (4rev1). Because IMAP 4rev1 supports many different features, it has a much wider command set than that of POP. Figure 2.6 provides a list of IMAP 4rev1 commands. Additionally, with the CAPABILITY command, the IMAP server can be queried to determine if other IMAP extensions are supported.

NOOP	Perform no operation
STARTTLS	Establish confidentiality and integrity protection
AUTHENTICATE <type>	Choose authentication method
LOGIN <user> <passwd>	Login with username and password
LOGOUT	Logout the current user
SELECT <mailbox>	Select the desired mailbox to access
EXAMINE <mailbox>	Same as SELECT except opens mailbox for read-only
CREATE <mailbox>	Create a mailbox with the name <mailbox>
DELETE <mailbox>	Delete selected mailbox
RENAME <mailbox> <newmailbox>	Rename mailbox
SUBSCRIBE <mailbox>	Subscribe to selected mailbox
UNSUBSCRIBE <mailbox>	Unsubscribe from selected mailbox
LIST <reference> [pattern]	List contents of current reference based on an optional pattern
LSUB <reference> [pattern]	List a set of mailboxes matching the pattern
STATUS <mailbox> <item>	Show the status of specific items in the selected mailbox
APPEND <mailbox> [flags] <msg>	Append a message to the selected mailbox
CHECK	Perform a checkpoint on the currently selected mailbox
CLOSE	Close the currently selected mailbox
EXPUNGE	Expunge deleted messages from the mailbox
SEARCH <criteria>	Search the mailbox based on certain criteria
FETCH <message> <item>	Fetch the specified item from the selected message
STORE <message> <item> <newvalue>	Update the selected item in a message
COPY <message> <mailbox>	Copy a message to the provided mailbox
UID <command> [args]	Perform an operation on a message based on its UID
CAPABILITY	Query the server for its capabilities

Figure 2.6: IMAP 4 Revision 1 Commands

Table 2.2 lists the associated RFCs for the noted IMAP extensions. IMAP has been extended with a challenge/response mechanism comparable to APOP, which is called the Challenge-Response Authentication Mechanism (CRAM). CRAM requires the client to make note of the challenge data sent by the server and respond with a string consisting of the user's name, a space, and a digest computed by applying a keyed hash algorithm[6] against the timestamp sent with the challenge, using a shared secret as the key.

[6] Most implementations use a popular one-way hash function called MD5. Developed by Ronald Rivest to create a message digest for digital signatures, MD5 is faster than SHA-1, but is considered less secure. MD5 is not approved for use in securing information for Federal agencies; see Section 3 for more information on this.

Table 2.2: IMAP Extension RFC Documents

IMAP Extension	Associated RFC
IMAP URL Scheme	2192
IMAP/POP AUTHorize Extension for Simple Challenge/Response	2195
IMAP4 ID extension	2971
IMAP4 IDLE command	2177
IMAP4 Login Referrals	2221
IMAP4 Mailbox Referrals	2193
IMAP4 Multi-Accessed Mailbox Practice	2180
IMAP4 Namespace	2342
IMAP4 non-synchronizing literals	2088
IMAP4 QUOTA extension	2087
IMAP4 UIDPLUS extension	4315

2.4.3 Proprietary Mailbox Access Mechanisms

Proprietary mailbox access protocols are designed to work within closed messaging environments. Microsoft Exchange and Lotus Notes are examples of messaging systems that use proprietary mailbox access protocols. These proprietary protocols offer additional functionality when used with their associated clients. Nearly all proprietary messaging systems support standard protocols, including SMTP, POP, and IMAP, in order to interoperate with other types of MTAs and MUAs. Organizations must decide for themselves whether it is appropriate to support proprietary protocols in their mail clients and servers. As mentioned earlier, regardless of whether they are standard or proprietary, most access protocols default to weak authentication mechanisms (unencrypted authentication information). Therefore, organizations need to configure the access protocols to support stronger forms of authentication.

2.4.4 Web-Based Mail Access

Web-based mail applications, also known as Webmail applications, are increasingly being used as a means of email service delivery, because Web browsers that enable access to the client are available on nearly every Internet-enabled device. A user simply runs a Web browser and connects to a Web site that hosts the Web-based mail application. The connection is made using either Hypertext Transfer Protocol (HTTP) or HTTP over Transport Layer Security (TLS), also known as HTTPS. HTTPS encrypts the communications, which protects both authentication information and email message content. HTTP alone does not offer any protection, so organizations should consider using HTTPS for Web-based mail application communications.

Web-based mail applications incorporate much of the mail-handling functionality of traditional mail clients and communicate with their associated mail servers using the same mailbox access protocols described earlier—SMTP, POP, and IMAP, as well as proprietary protocols. The mailbox access protocols are used between the Web servers and mail servers only; the protocols are not carried between the Web servers and Web browsers.

This page has been left blank intentionally.

3. Signing and Encrypting Email Messages

Organizations often want to protect the confidentiality and integrity of some of their email messages, such as preventing the exposure of personally identifiable information in an email attachment. Email messages can be protected by using cryptography in various ways, such as the following:

- Sign an email message to ensure its integrity and confirm the identity of its sender.
- Encrypt the body of an email message to ensure its confidentiality.
- Encrypt the communications between mail servers to protect the confidentiality of both the message body and message header.

The first two methods, message signing and message body encryption, are often used together. For example, if a message needs to be encrypted to protect its confidentiality, it is usually digitally signed as well, so that the recipient can ensure the integrity of the message and verify the identity of the signer. Messages that are digitally signed are usually not encrypted if the confidentiality of the contents does not need to be protected.

The third cryptography method listed above, encrypting the transmissions between mail servers, is typically applicable only when two organizations want to protect emails regularly sent between them. For example, the organizations could establish a virtual private network (VPN) to encrypt the communications between their mail servers over the Internet. Unlike methods that can only encrypt a message body, a VPN can encrypt entire messages, including email header information such as senders, recipients, and subjects. In some cases, organizations may need to protect header information. However, a VPN solution alone cannot provide a message signing mechanism, nor can it provide protection for email messages along the entire route from sender to recipient.[7]

Because most email messages are protected individually by digitally signing and optionally encrypting them, this section focuses on the use of these methods. The most widely used standards for signing messages and encrypting message bodies are Open Pretty Good Privacy (OpenPGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME).[8] Both are based in part on the concept of public key cryptography, which involves a user having a pair of related keys: a public key that anyone can hold, and a private key that is held exclusively by its owner. Because public key cryptography is so computationally intense, it is used sparingly in email security; symmetric key cryptography, which is much more efficient, is much more heavily used.

Symmetric key cryptography requires a single key to be shared between communicating parties, the sender and recipient of an email message. The process involves the sender generating a random key and encrypting the message with it using a symmetric key encryption algorithm. The sender then encrypts the symmetric key with a corresponding public key encryption algorithm using the recipient's public key, and sends both the encrypted message and encrypted symmetric key together to the recipient. This hybrid process uses public key encryption only to encrypt the symmetric key. Because only the intended message recipient holds the private key that is needed to recover the symmetric key, no other party can decrypt the message and read it. Digital signature techniques rely on the creation of a digest or

---

[7] For additional information on VPNs, see NIST SP 800-77, *Guide to IPsec VPNs*, which is available at http://csrc.nist.gov/publications/nistpubs/.

[8] Many other methods for protecting emails have been proposed since the invention of email. Two of these mechanisms were Privacy Enhanced Mail (PEM), first developed in 1987, and MIME Object Security Services (MOSS). Since neither method is broadly used today, they are not discussed in this document.

fingerprint of the information (i.e., the message being sent) using a cryptographic hash, which can be signed more efficiently than the entire message.[9]

Federal organizations are required to use cryptographic algorithms that have been approved by the Federal government.[10] Other organizations may wish to choose encryption schemes approved by the Federal government because these are well-tested and secure. Table 3.1 presents general recommendations for selecting cryptographic suites for protecting email messages.

Table 3.1: Recommended Cipher Suites

Recommended Use	Cipher Suites
Highest Security	Encryption: Advanced Encryption Standard (AES) [11] 128, 192, or 256-bit encryption Authentication & Digest: Digital Signature Standard (DSS) or RSA with a key size of 2048 bits or higher and SHA with a digest size of 256 bits (SHA-256) [12]
Security and Performance	Encryption: AES 128-bit encryption Authentication & Digest: DSS or RSA with a key size of 1024 bits or higher and SHA-1
Security and Compatibility	Encryption: Triple Data Encryption Standard (3DES) [13] 168/112-bit encryption (note: 3DES is considerably slower than AES) Authentication & Digest: DSS with a key size of 1024 bits or higher and SHA-1
Authentication and Tamper Detection	Authentication & Digest: DSS with a key size of 1024 bits or higher and SHA-1 or SHA-256

3.1 OpenPGP

OpenPGP is a protocol for encrypting and signing messages and for creating certificates using public key cryptography. It is based on an earlier protocol, PGP, which was created by Phil Zimmerman and implemented as a product first released in June 1991. The initial PGP protocol was proprietary and used some encryption algorithms with intellectual property restrictions. In 1996, version 5.x of PGP was defined in IETF RFC 1991, *PGP Message Exchange Formats*. Subsequently, OpenPGP was developed as a new standard protocol based on PGP version 5.x. OpenPGP is defined in RFC 2440, *OpenPGP Message Format*, and RFC 3156, *MIME Security with OpenPGP*.[14]

---

9 For more detailed information on public key cryptography, please refer to NIST Special Publication (SP) 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure* (http://csrc.nist.gov/publications/nistpubs/).

10 Federal agencies are required to use Federal Information Processing Standards (FIPS) approved cryptographic algorithms contained in validated cryptographic modules. The Cryptographic Module Validation Program (CMVP) is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada for the validation of cryptographic modules against certain FIPS publications. The CMVP Web site is located at http://csrc.nist.gov/cryptval/; it includes a complete list of FIPS-approved algorithms.

11 For more information about AES, see http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

12 For more information about the SHA and the associated Secure Hash Standard (SHS), see FIPS PUB 180-2, *Secure Hash Standard (SHS)*, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf. NIST has recommended that the use of SHA-1 be phased out by 2010 in favor of SHA-224 and other larger, stronger hash functions. See http://csrc.nist.gov/hash_standards_comments.pdf for additional information.

13 For more information about DES and 3DES, see http://csrc.ncsl.nist.gov/cryptval/.

14 The IETF working group for OpenPGP has a Web site at http://www.ietf.org/html.charters/openpgp-charter.html.

Many free and commercial products that use the OpenPGP standard are currently available. The software can be downloaded or purchased from a variety of Web sites.[15] Some OpenPGP-based products fully support the cryptographic algorithms recommended to the Federal government by NIST in FIPS PUB 140-2 and other publications, including 3DES and AES for data encryption, Digital Signature Algorithm (DSA)[16] and RSA for digital signatures, and SHA for hashing.[17] Some implementations of OpenPGP support other encryption schemes not addressed here.

Although certain aspects of OpenPGP do use public key cryptography, such as digitally signed message digests, the actual encryption of the message body is performed with a symmetric key algorithm, as outlined earlier. The following is a brief description of signing and encrypting a message with OpenPGP (some steps may occur in a different order):

- OpenPGP compresses the plaintext, which reduces transmission time and strengthens cryptographic security by obfuscating plaintext patterns commonly searched for during cryptanalysis.
- OpenPGP creates a random session key (in some implementations of OpenPGP, users are required to move their mouse at will within a window to generate random data).
- A digital signature is generated for the message using the sender's private key, and then added to the message.
- The message and signature are encrypted using the session key and a symmetric algorithm (e.g., 3DES, AES).
- The session key is encrypted using the recipient's public key and added to the beginning of the encrypted message.
- The encrypted message is sent to the recipient.

The recipient reverses the steps to recover the session key, decrypt the message, and verify the signature. Popular mail clients such as Mozilla Thunderbird, Apple Mail, Eudora, and Microsoft Outlook require the installation of plug-ins to enable the user to send and receive OpenPGP-encrypted messages. The OpenPGP distribution sites listed earlier in this section contain instructions on how to use OpenPGP with various mail client applications.

There are also security gateway servers available that can use OpenPGP to encrypt, decrypt, sign, and verify signatures on email messages on behalf of users. If two organizations exchanging emails both use compatible security gateway servers, then the use of OpenPGP is essentially transparent to users. If only one organization has such a gateway, it can still be used to protect messages, but it is not a transparent process at all to users at other organizations. If a gateway user sends an email to a recipient at another organization, that recipient will actually receive a notification email from the gateway that explains how to retrieve the protected email, typically through an SSL-encrypted HTTP session. Some gateways can also perform these functions for emails sent to lists of users. For example, a single user could send an encrypted and signed email to a mailing list address. The gateway would decrypt the email and re-

---

[15] Sites include the Free Software Foundation (http://www.gnupg.org/), Hushmail (http://www.hushmail.com/), International PGP Site (http://www.pgpi.org/), OpenPGP Site (http://www.openpgp.org/), and PGP (commercial version) (http://www.pgp.com/).

[16] For more information about the DSA and the associated Digital Signature Standard (DSS), see FIPS PUB 186-2, *Digital Signature Standard (DSS)*, http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf.

[17] FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*; FIPS PUB 180-2, *Secure Hash Standard (SHS)*, and FIPS PUB 186-2, *Digital Signature Standard (DSS)* are available at http://csrc.nist.gov/publications/fips/index.html.

encrypt it for all the individual recipients of the mailing list. Each recipient can then decrypt the email and verify the original signature.

3.2 S/MIME

S/MIME, which was originally proposed in 1995 by RSA Data Security, Inc., is based on their proprietary (although widely supported) Public Key Cryptography Standard (PKCS) #7 for data format of encrypted messages, and the X.509 version 3 standard for digital certificates.[18] S/MIME version 2 achieved wide adoption throughout the Internet mail industry. Although it is not a recognized IETF standard, it is specified by informational RFCs 2311, 2312, 2313, 2314, 2315, and 2268.

S/MIME version 3 was developed by the IETF S/MIME Working Group, which now coordinates all development of the S/MIME standard,[19] and adopted as an IETF standard in July 1999. S/MIME version 3 is specified by the following RFCs:

- Cryptographic Message Syntax (RFC 3852)
- S/MIME Version 3 Message Specification (RFC 3851)
- S/MIME Version 3 Certificate Handling (RFC 3850)
- Diffie-Hellman Key Agreement Method (RFC 2631)
- Enhanced Security Services for S/MIME (RFC 2634).

The most significant feature of S/MIME is its built-in and nearly "automatic" nature. Because of heavy industry involvement from manufacturers, S/MIME functionality exists with default installations of common mail clients such as Mozilla and Outlook Express.

The actual process by which S/MIME-enabled mail clients send messages is similar to that of OpenPGP.[20] S/MIME version 3.1 supports two symmetric key encryption algorithms recommended by FIPS PUB 140-2: AES, which is recommended but optional for compliant implementations to support, and 3DES, which is mandatory for implementations to support. Organizations using S/MIME to protect emails should use AES or 3DES (preferably AES, which is considered a stronger algorithm than 3DES).

As with OpenPGP, there are security gateway servers available that can use S/MIME to encrypt, decrypt, sign, and verify signatures on email messages on behalf of users. These gateways are very similar to those described in Section 3.1, and many of the gateways actually support both OpenPGP and S/MIME.

3.3 Key Management

Both OpenPGP and S/MIME use digital certificates to manage keys. A digital certificate identifies the entity (e.g., a user) that was issued the certificate, the public key of the entity's public key pair, and other information, such as the date of expiration, signed by some trusted party. However, differences exist in the key management models used by OpenPGP and S/MIME to establish trust using digital certificates.

---

[18] For more information about the RSA PKCS standards, consult the PKCS home page (http://www.rsasecurity.com/rsalabs/node.asp?id=2124).

[19] The homepage for the S/MIME Working Group can be found at http://www.ietf.org/html.charters/smime-charter.html.

[20] The following IBM Redbook provides a detailed example of how S/MIME works: http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg245341.pdf.

The default and traditional model that OpenPGP uses for key management is referred to as the "web of trust," which has no central key issuing or approving authority. The web of trust relies on the personal decisions of users for management and control. For example, if Alice trusts Bob and Carol trusts Alice, then Carol should trust Bob's emails. While this is suitable for individual users and very small organizations, the overhead of such a system is unworkable in most medium to large organizations. Some organizations deploy keyservers that users can access to get others' keys and store their own keys. Although this does promote scalability, the process is typically controlled mainly by individual users, and organizations are often not comfortable trusting keyservers to provide sufficient assurance of user identity.

Conversely, S/MIME works on a classical, more hierarchical arrangement of authorities that the organization chooses to trust. Typically, there is a master registration and approving authority, referred to as a root Certificate Authority (CA), that issues a public key certificate for itself and any subordinate CAs it sanctions. Subordinate CAs normally issue certificates to users and also to any other subordinate CAs that they in turn sanction, forming a hierarchy. Such a public key infrastructure can be used to establish a chain of trust between any two users holding valid certificates issued under it. By default, S/MIME-enabled mail clients depend on the trust of their immediate master CA when processing S/MIME transactions. This authority can be either a third-party CA[21] or a CA that is controlled by the organization issuing the certificates.

Having an organization exchange OpenPGP or S/MIME-protected emails with other organizations is usually extremely complicated, especially when attempting to maintain transparency for the users. The biggest challenges are key exchange and establishing trust relationships between the organizations. Organizations can connect their PKIs or use a mutually trusted third-party PKI, but in either case there are often technical and legal or regulatory challenges. Also, support for OpenPGP and S/MIME varies considerably depending on the mail client in use.

Third-party services are available that allow organizations to exchange encrypted email without having to establish trust relationships or worry about mail application compatibility. However, the use of such services necessitates placing sensitive messages on third-party servers, which itself can be a security concern. The use of mail encryption gateways between two organizations typically has lesser key management concerns because the keys are maintained on the gateways and a trust relationship already exists between the gateways.

Work is currently underway on a possible method of reducing key management concerns for email signing and encryption. Identity-based encryption (IBE) is a form of public key encryption that allows any string to be used as a public key. By using email addresses as public keys, IBE could simplify key management, making it much easier for senders to protect the emails that they send. However, there are serious barriers to adoption of IBE, including no open standards for IBE and no FIPS-approved IBE products. Informational Internet-Drafts have been started that propose how IBE could be performed using S/MIME.

3.4 Issues with Email Encryption

Although encrypting email provides additional security, it does come at a cost, so organizations should carefully weigh the issues associated with encrypting email messages:

---

[21] Examples of CAs are Entrust (http://www.entrust.com/), Thawte (http://www.thawte.com/), and Verisign (http://www.verisign.com/).

- Scanning for viruses and other malware and filtering email content at the firewall and mail server is made significantly more complicated by encryption. If the firewall or mail server does not have a method for decrypting the email, it cannot read and act upon the contents. Some malware scanners can decrypt emails if the scanner is a recipient of the emails or if the sender specifically encrypts the emails for the scanner, but such solutions are technically complex and often hard to enforce. Also, giving the malware scanner the ability to decrypt many or all emails could have serious consequences if the malware scanner host is itself infected or otherwise compromised. If having the malware scanner decrypt emails is not feasible, scanning might have to be performed on the hosts of the mail clients that perform decryption.
- Encryption and decryption require processor time. Organizations might need to upgrade or replace equipment that is not capable of supporting the load of encryption and decryption.
- Organization-wide use of encryption can require significant ongoing administrative overhead. Examples of this include key distribution, key recovery, and revocation of encryption keys.
- Email encryption can complicate the review of email messages by law enforcement and other investigative parties.
- Encrypted emails sent to or received from other organizations may be insufficiently protected if those organizations do not support the use of strong encryption algorithms and key sizes. Organizations should ensure that their users' mail applications notify them when they receive a weakly encrypted message or when they are attempting to send an encrypted message to a recipient that only supports weak encryption methods. Users can then contact the relevant party to notify them of the problem and request that they either use a stronger encryption algorithm or transfer the information that needs protected through a mechanism other than email.

4. Planning and Managing Mail Servers

The most critical aspect of deploying a secure mail server is careful planning before installation, configuration, and deployment. Careful planning will ensure that the mail server is as secure as possible and in compliance with all relative organizational policies. Many mail server security and performance problems can be traced back to a lack of planning or management controls. The importance of management controls is difficult to overstate. In many organizations, the information technology support structure is highly fragmented. This fragmentation leads to inconsistencies, and these inconsistencies can lead to security vulnerabilities.

4.1 Installation and Deployment Planning

Security of the mail server should be considered from the initial planning stage at the beginning of the systems development life cycle to maximize security and minimize costs. It is much more difficult and expensive to address security once implementation and deployment have occurred. Organizations are more likely to make decisions about configuring hosts appropriately and consistently when they begin by developing and using a detailed, well-designed deployment plan. Developing such a plan enables organizations to make informed tradeoff decisions between usability and performance, and risk. A deployment plan allows organizations to maintain secure configurations and aids in identifying security vulnerabilities, which often manifest themselves as deviations from the plan.

In the planning stages of a mail server, the following items should be considered [Alle00]:

- Identify the purpose(s) of the mail server.
  - What information categories will be stored on, processed on, or transmitted through the mail server?
  - What are the security requirements for this information?
  - What other service(s) will be provided by the mail server (in general, dedicating the host to being only a mail server is the most secure option)?
  - What are the security requirements for these additional services?
  - What are the requirements for continuity of mail services, such as those specified in continuity of operations plans and disaster recovery plans?
  - Where on the network will the mail server be located (see Section 7.1)?
- Identify the network services that will be provided on the mail server (in addition to the organization's standard services provided by every server for backup, remote administration, etc.), such as those supplied through standard email protocols (e.g., SMTP, POP, IMAP) and proprietary email protocols.
- Identify any network service software, both client and server, to be installed on the mail server and any other support servers.
- Identify the users or categories of users of the mail server and any support hosts, including servers providing Web-based mail access.
- Determine the privileges that each category of user will have on the mail server and support hosts.

- Determine how the mail server will be managed (e.g., locally, remotely from the internal network, remotely from external networks).
- Decide if and how users will be authenticated and how authentication data will be protected.
- Identify any security or privacy requirements for address-related information, such as username, user identity, and organizational association.
- Determine how appropriate access to information resources will be enforced.
- Determine which mail server applications meet the organization's requirements. Consider servers that may offer greater security, albeit with less functionality in some instances. Some issues to consider include the following:
  - Cost
  - Compatibility with existing infrastructure
  - Knowledge of existing employees
  - Existing manufacturer relationship
  - Past vulnerability history
  - Functionality
- Work closely with manufacturer(s) in the planning stage.

The choice of mail server application may determine the choice of operating system. However, to the degree possible, mail server administrators should choose an operating system that provides the following [Alle00]:

- Minimal exposure to vulnerabilities (which can be identified on all operating systems)
- Ability to restrict administrative or root level activities to authorized users only
- Ability to deny access to information on the server other than that intended to be available
- Ability to disable unnecessary network services that may be built into the operating system or server software
- Ability to log appropriate server activities to detect intrusions and attempted intrusions.

In addition, organizations should consider the availability of trained, experienced staff to administer the server and server products. Many organizations have learned the difficult lesson that a capable and experienced administrator for one type of operating environment is not automatically as effective for another.

Given the sensitive nature of the mail server, it is critical that it is located in an area that provides a secure physical environment. When planning the location of the mail server, the following items should be considered:

- Does the proposed location offer the appropriate physical security protection mechanisms? Examples include locks, card reader access, security guards, and physical intrusion detection systems (e.g., motion sensors, cameras).

- Does the proposed location offer the appropriate environmental controls so that the necessary humidity and temperature are maintained?
- Is there a backup power source?
- If the location is subject to known natural disasters, is it hardened against those disasters and/or is there a contingency site outside the potential disaster area?

4.2 Security Management Staff

Because mail server security is tightly intertwined with the organization's general information system security posture, a number of IT and system security staff may be interested in mail server planning, implementation, and administration. This section provides a list of those roles and identifies their responsibilities as related to mail server security. These roles may vary with the organization, however, and not all organizations will have the identical roles described here.

4.2.1 Senior IT Management/Chief Information Officer (CIO)

The Senior IT Management/CIO ensures that the organization's security posture is adequate. The Senior IT Management provides direction and advisory services for the protection of information systems for the entire organization. The Senior IT Management/CIO is responsible for the following activities that are associated with mail servers:

- Coordinating the development and maintenance of the organization's information security policies, standards, and procedures
- Coordinating the development and maintenance of the organization's change control and management procedures
- Ensuring the establishment of, and compliance with, consistent IT security policies for departments throughout the organization
- Coordinating with upper management, public affairs, and other relevant personnel to produce a formal policy and process for email usage guidelines (e.g., personal use, monitoring, encryption).

4.2.2 Information Systems Security Program Managers

The Information Systems Security Program Managers (ISSPM) oversee the implementation of and compliance with the standards, rules, and regulations specified in the organization's security policy. The ISSPMs are responsible for the following activities associated with mail servers:

- Ensuring that security procedures are developed and implemented
- Ensuring that security policies, standards, and requirements are followed
- Ensuring that all critical systems are identified and that contingency planning, disaster recovery plans, and continuity of operations plans exist for these critical systems
- Ensuring that critical systems are identified and scheduled for periodic security testing according to the security policy requirements of each respective system.

4.2.3 Information Systems Security Officers

Information Systems Security Officers (ISSO) are responsible for overseeing all aspects of information security within a specific organizational entity. They ensure that the organization's information security practices comply with organizational and departmental policies, standards, and procedures. ISSOs are responsible for the following activities associated with mail servers:

- Developing internal security standards and procedures for the mail server(s) and supporting network infrastructure
- Cooperating in the development and implementation of security tools, mechanisms, and mitigation techniques
- Maintaining standard configuration profiles of the mail servers and supporting network infrastructure controlled by the organization, including but not limited to operating systems, firewalls, routers, and mail server applications
- Maintaining operational integrity of systems by conducting security tests and ensuring that designated IT professionals are conducting scheduled testing on critical systems.

4.2.4 Mail Server and Network Administrators

Mail server administrators are system architects responsible for the overall design, implementation, and maintenance of a mail server. Network administrators are responsible for the overall design, implementation, and maintenance of a network. On a daily basis, mail server and network administrators contend with the security requirements of the specific system(s) for which they are responsible. Security issues and solutions can originate from either outside (e.g., security patches and fixes from the manufacturer or computer security incident response teams) or within the organization (e.g., the security office). The administrators are responsible for the following activities associated with mail servers:

- Installing and configuring hosts in compliance with the organizational security policies and standard system/network configurations
- Maintaining hosts in a secure manner, including frequent backups and timely application of patches
- Monitoring system integrity, protection levels, and security-related events
- Following up on detected security anomalies associated with their information system resources
- Conducting security tests as required.

4.3 Management Practices

Appropriate management practices are critical to operating and maintaining a secure mail server. Security practices entail the identification of an organization's information system assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability of information system resources.

To ensure the security of a mail server and the supporting network infrastructure, organizations should implement the following practices:

- **Organizational Information System Security Policy**—A security policy should specify the basic information system security tenets and rules and their intended internal purpose. The policy should also outline who in the organization is responsible for particular areas of information security (e.g.,

implementation, enforcement, audit, review). The policy must be enforced consistently throughout the organization to be effective. Generally, the CIO and upper management are responsible for drafting the organization's security policy.

- **Configuration/Change Control and Management**—The process of controlling modification to a system's design, hardware, firmware, and software provides sufficient assurance that the system is protected against the introduction of an improper modification before, during, and after system implementation. Configuration control leads to consistency with the organization's information system security policy. Configuration control is traditionally overseen by a configuration control board that is the final authority on all proposed changes to an information system.

- **Risk Assessment and Management**—Risk assessment is the process of analyzing and interpreting risk. It involves determining an assessment's scope and methodology, collecting and analyzing risk-related data, and interpreting the risk analysis results. Collecting and analyzing risk data requires identifying assets, threats, vulnerabilities, safeguards, consequences, and the probability of a successful attack. Risk management is the process of selecting and implementing controls to reduce risk to a level acceptable to the organization.

- **Standardized Configurations**—Organizations should develop standardized secure configurations for widely used operating systems and applications. This will provide guidance to mail server and network administrators on how to configure their systems securely and ensure consistency and compliance with the organizational security policy. Because it only takes one insecurely configured host to compromise a network, organizations with a significant number of hosts are especially encouraged to apply this recommendation. Section 5 contains additional information on standard configurations.

- **Security Awareness and Training**—A security training program is critical to the overall security posture of an organization. Making users and administrators aware of their security responsibilities and teaching the correct practices helps them change their behavior to conform to security best practices. Training also supports individual accountability, which is an important method for improving information system security.

- **Contingency, Continuity of Operations, and Disaster Recovery Planning**—Contingency plans, continuity of operations plans, and disaster recovery plans are established in advance to allow an organization or facility to maintain operations in the event of a disruption.[22]

- **Certification and Accreditation**—Certification in the context of information systems security means that a system has been analyzed as to how well it meets all of the security requirements of the organization. Accreditation occurs when the organization's management accepts that the system meets the organization's security requirements.[23]

4.4 System Security Plan

The objective of system security planning is to improve protection of information system resources.[24] Plans that adequately protect information assets require managers and information owners—directly affected by and interested in the information and/or processing capabilities—to be convinced that their

---

[22] For more information, see NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems* (http://csrc.nist.gov/publications/nistpubs/).

[23] For more information on certification and accreditation, see NIST SP 800-37, *Federal Guidelines for the Security Certification and Accreditation of Information Technology Systems* (http://csrc.nist.gov/publications/nistpubs/).

[24] For more information on system security plans, see NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems* (http://csrc.nist.gov/publications/nistpubs/).

information assets are adequately protected from loss, misuse, unauthorized access or modification, unavailability, and undetected activities.

The purpose of the system security plan is to provide an overview of the security and privacy requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system owner, and the senior agency information security officer (SAISO).

For Federal agencies, all information systems must be covered by a system security plan. Other organizations should strongly consider the completion of a system security plan for each of their systems as well. The information system owner[25] is generally the party responsible for ensuring that the security plan is developed and maintained and that the system is deployed and operated according to the agreed-upon security requirements.

In general, an effective system security plan should include the following:

- **System Identification.** The first sections of the system security plan provide basic identifying information about the system. They contain general information such as the key points of contact for the system, the purpose of the system, the sensitivity level of the system, and the environment in which the system is deployed.
- **Controls.** This section of the plan describes the control measures (in place or planned) that are intended to meet the protection requirements of the information system. Controls fall into three general categories:
  - Management controls, which focus on the management of the computer security system and the management of risk for a system.[26]
  - Operational controls, which are primarily implemented and executed by people (as opposed to systems). They often require technical or specialized expertise, and often rely upon management activities as well as technical controls.
  - Technical controls, which are security mechanisms that the computer system employs. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the organization. [Swan06]

---

[25] The information system owner is responsible for defining the system's operating parameters, authorized functions, and security requirements. The information owner for information stored within, processed by, or transmitted by a system may or may not be the same as the information system owner. In addition, a single system may utilize information from multiple information owners.

[26] For more detail on management, operational, and technical controls, see NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, and NIST SP 800-100, *Information Security Handbook: A Guide for Managers* (http://csrc.nist.gov/publications/nistpubs/).

4.5 Human Resources Requirements

The greatest challenge and expense in developing and securely maintaining a mail server is providing the necessary human resources to adequately perform the required functions. Many organizations fail to fully realize the amount of expense and skills required to field a secure mail server. This failure often results in overworked employees and insecure systems. From the initial planning stages, organizations need to determine the necessary human resource requirements. Appropriate and sufficient human resources are the single most important aspect of mail server security. Organizations should also consider the fact that, in general, technical solutions are not a substitute for skilled and experienced personnel.

When considering the human resource implications of developing and deploying a mail server, organizations should address the following in the deployment plan:

- **Required Personnel** – What types of personnel are going to be required? This would include such positions as system and mail server administrators, network administrators, and ISSOs.
- **Required Skills** – What are the required skills to adequately plan, develop, and maintain the mail server in a secure manner? Examples include operating system administration, network administration, active content expertise, and programming.
- **Available Personnel** – What are the available human resources within the organization? In addition, what are their current skill sets and are they sufficient for supporting the mail server? Often an organization discovers that its existing human resources are not sufficient and needs to consider the following options:
  - Train Current Staff – If there are personnel available but they do not have the requisite skills, the organization may choose to train the existing staff in the skills required. While this is an excellent option, the organization should ensure that employees meet all prerequisites for training.
  - Hire Additional Staff – If there is not enough staff available or they do not have the requisite skills, it may be necessary to hire additional personnel.

Once the organization has staffed the project and the mail server is active, it will be necessary to ensure the number and skills of the personnel are still adequate. The threat and vulnerability levels of hosts including mail servers are constantly changing, as is the technology. This means that what is adequate today may not be tomorrow.

4.6 General Information System Security Principles

When addressing mail server security issues, it is an excellent idea to keep some general information security principles in mind [Curt01 and Salt75]:

- **Simplicity**—Security mechanisms (and the information systems in general) should be as simple as possible. Complexity is at the root of many security issues.
- **Fail-Safe**—If a failure occurs, the system should fail in a secure manner by which security controls and settings remain in effect and are enforced. It is usually better to lose functionality rather than security.
- **Complete Mediation**—Rather than providing direct access to information, mediators that enforce access policy should be employed. Common examples include file system permissions, proxies, firewalls, and mail gateways.

- **Open Design**—System security should not depend on the secrecy of the implementation or its components. "Security through obscurity" is not reliable.
- **Separation of Privilege**—Functions, to the degree possible, should be separate and provide as much granularity as possible. The concept can apply to both systems and operators/users. In the case of systems, such functions such as read, edit, write, and execute should be separate. In the case of system operators and users, roles should be as separate as possible. For example, if resources allow, the role of system administrator should be separate from that of the security administrator.
- **Least Privilege**—This principle dictates that each task, process, or user is granted the minimum rights required to perform its job. By applying this principle consistently, should a task, process, or user be compromised, the scope of damage is constrained to the limited resources available to the compromised entity.
- **Psychological Acceptability**—Users should understand the necessity of security. This can be provided through training and education. In addition, the security mechanisms in place should present users with sensible options that give them the usability they require on a daily basis. If users find the security mechanisms too cumbersome, they may devise ways to work around or compromise them. The objective is not to weaken security so it is understandable and acceptable, but to train, educate, and design security mechanisms and policies that are usable and effective.
- **Least Common Mechanism**—When providing a feature to the system, it is best to have a process or service gain some function without granting the same function to other parts of the system. The ability for the mail server process to access a backend database, for instance, should not also enable other applications on the system to access the backend database.
- **Defense in Depth**—Organizations should understand that a single security mechanism would generally prove insufficient. Security mechanisms (defenses) need to be layered so that compromise of a single security mechanism is insufficient to compromise a host or network. There is no "silver bullet" for information system security.
- **Work Factor**—Organizations should understand what it would take to break the system or network's security features. The amount of work necessary for an attacker to break the system or network should exceed the value that the attacker would gain from a successful compromise.
- **Compromise Recording**—Records and logs should be maintained so that if a compromise does occur, evidence of the attack is available to the organization. This information can assist in securing the network and host after the compromise and assist in identifying the methods and exploits used by the attacker. This information can be used to better secure the host or network in the future. In addition, this can assist organizations in identifying and prosecuting attackers.

4.7 Checklist for Planning and Managing Mail Servers

Completed	Action
	Plan the installation and deployment of mail server
☐	Identify functions of the mail server
☐	Identify categories of information that will be stored on, processed on, and transmitted through the mail server
☐	Identify security requirements of information
☐	Identify requirements for continuity of mail services
☐	Identify a dedicated host to run the mail server
☐	Identify network services that will be provided or supported by the mail server
☐	Identify users and categories of users of the mail server and determine privilege for each category of user
☐	Determine how the mail server will be managed (e.g., locally, remotely)
☐	Identify user authentication methods for the mail server
☐	Identify security or privacy requirements for email address-related information
	Choose appropriate operating system for mail server
☐	Minimal exposure to vulnerabilities
☐	Ability to restrict administrative or root level activities to authorized users only
☐	Ability to deny access to information on the server other than that intended to be available
☐	Ability to disable unnecessary network services that may be built into the operating system or server software
☐	Ability to log appropriate server activities to detect intrusions and attempted intrusions
☐	Availability of trained, experienced staff to administer the server and server products
	Plan the location of the mail server
☐	Appropriate physical security protection mechanisms
☐	Appropriate environmental controls to maintain the necessary temperature and humidity
☐	Backup power source
☐	Preparation for known natural disasters

This page has been left blank intentionally.

5. Securing the Mail Server Operating System

Protecting a mail server from compromise involves hardening the underlying operating system, the mail server application, and the network to prevent malicious entities from directly attacking the mail server. The first step in securing a mail server, hardening the underlying operating system, is discussed at length in this section. (Securing the mail server application and the network are addressed in Sections 6 and 7, respectively).

All commonly available mail servers operate on a general-purpose operating system. Many security issues can be avoided if the operating systems underlying the mail servers are configured appropriately. Default hardware and software configurations are typically set by manufacturers to emphasize features, functions, and ease of use at the expense of security. Because manufacturers are unaware of each organization's security needs, each mail server administrator must configure new servers to reflect their organization's security requirements and reconfigure them as those requirements change. The practices recommended here are designed to help mail server administrators configure and deploy mail servers that satisfy their organization's security requirements.[27] Mail server administrators managing existing mail servers should confirm that their systems address the issues discussed.

The techniques for hardening different operating systems vary greatly; therefore, this section includes the generic procedures common in securing most operating systems. Security configuration guides and checklists for many operating systems are publicly available; these documents typically contain recommendations for settings that improve the default level of security, and they may also contain step-by-step instructions for securing systems.[28] In addition, many organizations maintain their own guidelines specific to their requirements. Some automated tools also exist for hardening operating systems and their use is strongly recommended.

Five basic steps are necessary to maintain basic operating system security:

1. Planning the installation and deployment of the host operating system and other components for the mail server
2. Patching and updating the host operating system as required
3. Hardening and configuring the host operating system to address security adequately
4. Installing and configuring additional security controls, if needed
5. Testing the host operating system to ensure that the previous four steps adequately address all security issues.

The first step is discussed in Section 4.1. The other steps are covered in Sections 5.1 and 5.2.

---

[27] If Web-based mail access will be provided, administrators should ensure that the associated Web servers are secured properly, including securing their operating systems and Web server software. See NIST SP 800-44, *Guidelines on Securing Public Web Servers*, for additional information (http://csrc.nist.gov/publications/nistpubs/).

[28] Checklists and implementation guides for various operating systems and applications are available from NIST at http://checklists.nist.gov/. Also, see NIST SP 800-70, *Security Configuration Checklists Program for IT Products*, available at the same Web site, for general information about NIST's checklists program.

5.1 Updating and Configuring the Operating System

This section provides an overview of the second, third, and fourth steps in the list above. The combined result of these steps should be to have reasonable protection for the mail server's operating system.

5.1.1 Patch and Upgrade Operating System

Once an operating system is installed, applying needed patches or upgrades to correct for known vulnerabilities is essential. Any operating system has known vulnerabilities that should be corrected before using it to host a mail server. To adequately detect and correct these vulnerabilities, mail server administrators should do the following:

- Create and implement a patching process[29]
- Identify vulnerabilities and applicable patches[30]
- Mitigate vulnerabilities temporarily if needed and if feasible (until patches are available, tested, and installed)
- Install permanent fixes (often called patches, hotfixes, service packs, or updates).

Administrators should ensure that mail servers, particularly new ones, are adequately protected during the patching process. For example, a mail server that is not fully patched or not configured securely could be compromised by threats if it is publicly accessible while it is being patched. When preparing new mail servers for deployment, administrators should do either of the following:

- Keep the servers disconnected from networks or connect them only to an isolated "build" network until all patches have been transferred to the servers through out-of-band means (e.g., CDs) and installed, and the other configuration steps listed in Section 5.1 have been performed.
- Place the servers on a virtual local area network (VLAN) or other network segment that severely restricts what actions the hosts on it can perform and what communications can reach the hosts—only allowing those events that are necessary for patching and configuring the hosts. Do not transfer the hosts to regular network segments until all the configuration steps listed in Section 5.1 have been performed.

Administrators should generally not apply patches to mail servers without first testing them on another identically configured server, because patches can inadvertently cause operational problems. Although administrators can configure mail servers to download patches automatically, the servers should not be configured to install them automatically so that they can first be tested.

5.1.2 Remove or Disable Unnecessary Services and Applications

Ideally, a mail server should be on a dedicated, single-purpose host. When configuring the operating system, disable everything except that which is expressly permitted – that is, disable all services and applications, enable only those required by the mail server, and then remove the unneeded services and applications. If possible, install the minimal operating system configuration that is required for the mail

---

[29] For more information, see NIST SP 800-40 Version 2.0, *Creating a Patch and Vulnerability Management Program*, which is available at http://csrc.nist.gov/publications/nistpubs/. A single patch management process can be put into place for both operating systems and applications (including mail server and mail client software).

[30] To check for vulnerabilities in operating systems, services, and other applications, see the NIST National Vulnerability Database (NVD) at http://nvd.nist.gov/.

server application. Choose the "minimal installation" option, if available, to minimize the effort required in removing unnecessary services. In addition, many uninstall scripts or programs are far from perfect in completely removing all components of a service; therefore, it is always better not to install unnecessary services. Some common types of services and applications that should usually be disabled if not required include the following:

- File and printer sharing services (e.g., Windows Network Basic Input/Output System [NetBIOS] file and printer sharing, Network File System [NFS], File Transfer Protocol [FTP])
- Default Web servers
- Wireless networking services
- Remote control and remote access programs, particularly those that do not strongly encrypt their communications (e.g., Telnet)[31]
- Directory services (e.g., Lightweight Directory Access Protocol [LDAP], Kerberos, Network Information System [NIS])
- Language compilers and libraries
- System development tools
- System and network management tools and utilities, including Simple Network Management Protocol (SNMP).

Removing unnecessary services and applications is preferable to simply disabling them through configuration settings, because attacks that attempt to alter settings and activate a disabled service cannot succeed when the functional components are completely removed. Disabled services could also be enabled inadvertently through human error.

Eliminating or disabling unnecessary services enhances the security of a mail server in several ways [Alle00]:

- Other services cannot be compromised and used to attack the host or impair the services of the mail server. Each service added to a host increases the risk of compromise for that host because each service is another possible avenue of access for an attacker. Less is more secure in this case.
- Other services might have flaws or might be incompatible with the mail server itself. Disabling or removing them prevents them from affecting the mail server, including its availability.
- The host can be configured to better suit the requirements of the particular service. Different services might require different hardware and software configurations, which could lead to unnecessary vulnerabilities or negatively affect performance.
- By reducing services, the number of logs and log entries is reduced; therefore, detecting unexpected behavior becomes easier (see Section 9).

Organizations should determine the services to be enabled on a mail server. Services in addition to the mail server service that might be installed include directory protocols to access the organization's user directory and remote administration services. These services may be required in certain instances, but

[31] If a remote control or remote access program is absolutely required and it does not strongly encrypt its communications, it should be tunneled over a protocol that provides encryption, such as secure shell (SSH) or IP Security (IPsec).

they may increase the risks to the server. Whether the risks outweigh the benefits is a decision for each organization to make.

If Web-based mail access is to be provided, the Web server running the mail application should be on a separate host from the mail server. Having the Web and mail servers on separate hosts limits the impact if one of them is compromised when compared with having both servers on the same host. The benefits of the latter arrangement are efficient and protected communications, because the Web and mail servers communicate directly within a host instead of over a network.

5.1.3 Configure Operating System User Authentication

For mail servers, the authorized users who can configure the operating system are limited to a small number of designated mail server administrators. The users who can access the mail server, however, may range from unrestricted to restricted subsets of the organization's employees. To enforce policy restrictions, if required, the mail server administrator must configure the operating system to authenticate a prospective user by requiring proof that the user is authorized for such access.

Enabling authentication by the host computer involves configuring parts of the operating system, firmware, and applications, such as the software that implements a network service. In special cases, for high-value/high-risk sites, organizations may also use authentication hardware, such as tokens or one-time password devices. Use of authentication mechanisms where authentication information is reusable (e.g., passwords) and transmitted in the clear over a network is strongly discouraged, because the information can be intercepted and used by an attacker to masquerade as an authorized user.

To ensure the appropriate user authentication is in place, take the following steps [Alle00]:

- **Remove or disable unneeded default accounts and groups.** The default configuration of the operating system often includes guest accounts (with and without passwords), administrator or root level accounts, and accounts associated with local and network services. The names and passwords for those accounts are well known. Remove or disable unnecessary accounts to eliminate their use by attackers, including guest accounts on computers containing sensitive information. If there is a requirement to retain a guest account or group, severely restrict its access and change the default password in accordance with the organizational password policy. For default accounts that need to be retained, change the names (where possible and particularly for administrator or root level accounts) and passwords to be consistent with the organizational password policy. Default account names and passwords are commonly known in the attacker community.

- **Disable non-interactive accounts.** Disable accounts (and the associated passwords) that need to exist but do not require an interactive login. For Unix systems, disable the login shell or provide a login shell with NULL functionality (e.g., /bin/false).

- **Create the user groups.** Assign users to the appropriate groups. Then assign rights to the groups, as documented in the deployment plan. This approach is preferable to assigning rights to individual users because the latter becomes unwieldy with large numbers of users.

- **Create the user accounts.** The deployment plan identifies who will be authorized to use each computer and its services. Create only the necessary accounts. Permit the use of shared accounts only when no viable alternatives exist.

- **Check the organization's password policy.** Set account passwords appropriately. This policy should address the following areas:

- **Length** – a minimum length for passwords. Specify a minimum length of at least eight characters.
- **Complexity** – the mix of characters required. Require passwords to contain both uppercase and lowercase letters and at least one non-alphanumeric character, and to not be a "dictionary" word.[32]
- **Aging** – how long a password may remain unchanged. Require users to change their passwords periodically. Administrator or root level passwords should be changed every 30 to 120 days. User level passwords should also be changed periodically, with the period determined by the enforced length and complexity of the password combined with the sensitivity of the information protected. When considering the appropriate aging duration, the exposure level of user passwords should also be taken into account.
- **Reuse** – whether a password may be reused. Some users try to defeat a password aging requirement by changing the password to one they have used previously. If possible, ensure that users cannot change their password by merely appending characters to the beginning or end of their original password (e.g., original password was "mysecret" and is changed to "1mysecret" or "mysecret1").
- **Authority** – who is allowed to change or reset passwords and what sort of proof is required before initiating any changes.
- **Password Security** – how passwords should be secured, such as not storing passwords unencrypted on the mail server, and requiring administrators to use different passwords for their mail administration accounts than their other administration accounts.

- **Configure computers to prevent password guessing.** It is relatively easy for an unauthorized user to try to gain access to a computer by using automated software tools that attempt all passwords. If the operating system provides the capability, configure it to increase the period between login attempts with each unsuccessful attempt. If that is not possible, the second alternative is to deny login after a limited number of failed attempts (e.g., three). Typically, the account is "locked out" for a period of time (such as 30 minutes) or until a user with appropriate authority reactivates it.

  The choice to deny login is another situation that requires the mail server administrator to make a decision that balances security and convenience. Implementing this recommendation can help prevent some kinds of attacks, but it can also allow an attacker to make failed login attempts to prevent user access, a denial of service (DoS) condition.

  Failed network login attempts should not prevent an authorized user or administrator from logging in at the console. Note that all failed login attempts whether via the network or console should be logged. If remote administration is not to be implemented (see Section 9.5), disable the ability for the administrator or root level accounts to log in from the network.

- **Install and configure other security mechanisms to strengthen authentication.** If the information on the mail server requires it, consider using other authentication mechanisms such as biometrics, smart cards, client/server certificates, or one-time password systems. They can be more expensive and difficult to implement, but they may be justified in some circumstances. When such

[32] This would include any personal names, place names, terms, or words in any language that could be found in a dictionary or word list.

authentication mechanisms and devices are used, the organization's policy should be changed accordingly.

As mentioned earlier, attackers using network sniffers can easily capture passwords passed across a network in clear text. However, passwords are economical and appropriate if properly protected while in transit. Implement authentication and encryption technologies, such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Secure Shell (SSH), or Virtual Private Networks (VPNs) (for remote users), to protect passwords during transmission. Requiring server side authentication to be used with encryption technologies reduces the likelihood of successful man-in-the-middle attacks.

5.1.4 Configure Resource Controls Appropriately

All commonly used modern server operating systems provide the capability to specify access privileges individually for files, directories, devices, and other computational resources. By carefully setting access controls and denying personnel unauthorized access, the mail server administrator can reduce security breaches. For example, denying read access to files and directories helps to protect confidentiality of information, and denying unnecessary write (modify) access can help maintain the integrity of information. Limiting the execution privilege of most system-related tools to authorized system administrators can prevent users from making configuration changes that could reduce security. It also can restrict the attacker's ability to use those tools to attack the system or other systems on the network.

5.1.5 Install and Configure Additional Security Controls

Operating systems often do not include all of the security controls necessary to secure the operating system, services, and applications adequately. In such cases, administrators need to select, install, and configure additional software to provide the missing controls. Commonly needed controls include the following:

- Anti-malware software, such as anti-virus software, anti-spyware software, and rootkit detectors, to protect the local operating system from malware and to detect and eradicate any infections that occur.[33] Examples of when anti-malware software would be helpful include a mail administrator bringing infected media to the mail server and a network service worm contacting the server and infecting it. This software is independent of the anti-malware software used to scan the email passing through the server. For many mail systems, anti-virus software is the only form of anti-malware software needed to protect the OS.
- Host-based intrusion detection and prevention software, to detect attacks performed against the mail servers. Section 7.2.2 contains additional information on host-based intrusion detection and prevention software.
- Host-based firewalls, to protect the server from unauthorized access.[34]
- Patch management software, to ensure that vulnerabilities are addressed promptly. Patch management software can be used just to apply patches, or also to identify new vulnerabilities in the mail server's operating systems, services, and applications.

---

[33] Additional information on anti-malware software is available from NIST SP 800-83, *Guide to Malware Incident Prevention and Handling* (http://csrc.nist.gov/publications/nistpubs/).

[34] For more information on firewalls, see NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy* (http://csrc.nist.gov/publications/nistpubs/).

Some mail server administrators also install one or more forms of host-based intrusion detection software on their servers. For example, file integrity checking software can identify changes to critical system files.

When planning security controls, mail server administrators should consider the resources that the security controls will consume. A server's performance could degrade if it does not have enough memory and processing capacity for the controls.

5.2 Security Testing the Operating System

Periodic security testing of the operating system is a vital way to identify vulnerabilities and to ensure that the existing security precautions are effective. Methods for testing operating systems include vulnerability scanning and penetration testing. Vulnerability scanning usually entails using an automated vulnerability scanner to scan a host or groups of hosts on a network for application, network, and operating system vulnerabilities. Penetration testing is a testing process designed to compromise a network using the tools and methodologies of an attacker. It involves iteratively identifying and exploiting the weakest areas of the network to gain access to the remainder of the network, eventually compromising the overall security of the network. Vulnerability scanning should be conducted periodically, such as weekly or monthly, and penetration testing should be conducted at least annually. Because both of these testing techniques also are applicable to testing the mail server application, they are discussed in detail in Section 9.4.[35]

5.3 Checklist for Securing the Mail Server Operating System

Completed	Action
	Patch and upgrade operating system
☐	Create and implement a patching process
☐	Identify, test, and install all necessary patches and upgrades to the operating system
	Remove or disable unnecessary services and applications
☐	Remove or disable unnecessary services and applications
☐	Use separate hosts for Web servers, directory servers, and other services
	Configure operating system user authentication
☐	Remove or disable unneeded default accounts and groups
☐	Disable non-interactive accounts
☐	Create the user groups for the particular computer
☐	Create the user accounts for the particular computer
☐	Check the organization's password policy, and set account passwords appropriately (e.g., length, complexity)
☐	Configure computers to prevent password guessing
☐	Install and configure other security mechanisms to strengthen authentication
	Configure resource controls appropriately
☐	Set access controls for files, directories, devices, and other resources

[35] For information on these and other testing techniques, see NIST SP 800-42, *Guideline on Network Security Testing*, (http://csrc.nist.gov/publications/nistpubs/).

Completed	Action
☐	Limit privileges for most system-related tools to authorized system administrators
	Install and configure additional security controls
☐	Select, install, and configure additional software to provide needed controls not included in the operating system
	Test the security of the operating system
☐	Test operating system after initial install to determine vulnerabilities
☐	Test operating system periodically to determine new vulnerabilities

6. Securing Mail Servers and Content

Hardening mail server applications is an important step in protecting mail servers from compromise. This section provides recommendations for securely installing mail servers and configuring operating system and mail server access controls. Another important part of mail security is protecting the email content that traverses the server, which includes content filtering, malware scanning, and spam prevention. Securing access to mailboxes by encrypting communications, including Web-based mail access, is also addressed in this section. Email content security can also involve email encryption to preserve confidentiality and digital signatures to support integrity and non-repudiation; these are discussed in Section 3.

6.1 Hardening the Mail Server Application

After ensuring that the mail server's operating system is secured properly, the next step is to install the mail server application and secure it from likely threats. The subsections that follow provide an overview of these two actions.

6.1.1 Securely Installing the Mail Server

In many respects, the secure installation and configuration of the mail server application mirrors the operating system process discussed in Section 5. The overarching principle, as before, is to install only the services required for the mail server and to eliminate any known vulnerabilities through patches or upgrades. Any unnecessary applications, services, or scripts that are installed should be removed immediately once the installation process is complete. During the installation of the mail server, the following steps should be performed:

- Install the mail server software on a dedicated host
- Apply any patches or upgrades to correct for known vulnerabilities
- Create a dedicated physical disk or logical partition (separate from operating system and mail server application) for mailboxes, or host the mailboxes on a separate server
- Remove or disable all services installed by the mail server application but not required (e.g., Web-based mail, FTP, remote administration)
- Remove or disable all unneeded default login accounts created by the mail server installation
- Remove all manufacturer documentation from the server
- Remove any example or test files from the server
- Apply appropriate security template or hardening script to the server
- Reconfigure SMTP, POP, and IMAP service banners (and others as required) NOT to report mail server and operating system type and version (this may not be possible with all mail servers)
- Disable dangerous or unnecessary mail commands (e.g., VRFY and EXPN).

6.1.2 Configuring Operating System and Mail Server Access Controls

Most mail server host operating systems provide the capability to specify access privileges individually for files, devices, and other computational resources on that host. Any information that the mail server can access using these controls can potentially be distributed to all users accessing the mail server. The

mail server software is likely to include mechanisms to provide additional file, device, and resource access controls specific to its operation. It is important to set identical permissions for both the operating system and mail server application; otherwise, too much or too little access may be granted to users. Mail server administrators should consider how best to configure access controls to protect information stored on their public mail server from two perspectives:

- Limit the access of the mail server application to a subset of computational resources
- Limit the access of users through additional access controls enforced by the mail server, where more detailed levels of access control are required.

The proper setting of access controls can help prevent the disclosure of sensitive or restricted information that is not intended for public dissemination. In addition, access controls can be used to limit resource use in the event of a DoS attack against the mail server.

Typical files to which access should be controlled are as follows:

- Application software and configuration files
- Files directly related to security mechanisms:
  - Password hash files and other files used in authentication
  - Files containing authorization information used in controlling access
  - Cryptographic key material used in confidentiality, integrity, and non-repudiation services
- Server log and system audit files
- System software and configuration files.

Ensure that the mail server application executes only under a unique individual user and group identity with very restrictive access controls. Thus, new user and group identities to be used exclusively by the mail server software need to be established. The new user and new group should be independent and unique from all other users and groups. This is a prerequisite for implementing the access controls described in the following steps. Although the server may initially have to run with root (Unix) or administrator/system (Windows) privileges to bind to the necessary TCP ports, do not allow the server to continue to run at this level of access.

In addition, use the mail server operating system to limit files accessed by the mail service processes. These processes should have read-only access to those files necessary to perform the service and should have no access to other files, such as server log files. Use mail server host operating system access controls to enforce the following:

- Temporary files created by the mail server application are restricted to a specified and appropriately protected subdirectory (if possible).
- Access to any temporary files created by the mail server application is limited to the mail server processes that created these files (if possible).

It is also necessary to ensure that the mail server cannot save files outside the specified file structure dedicated to the mail server. This may be a configuration choice in the server software, or it may be a choice in how the server process is controlled by the operating system. Ensure that such directories and

files (outside the specified directory tree) cannot be accessed, even if users know the locations of those files.

On Linux and Unix hosts, consider using a "chroot jail" for the mail server application. Using chroot changes the mail server's "view" of the host file system such that the apparent root directory is not the real file system root directory but rather one of its subparts. Thus, if the mail server is successfully compromised, the attacker only gains access to the limited subpart of the file system accessible via chroot. This is a very powerful security measure.

To mitigate the effects of certain types of DoS attacks, configure the mail server to limit the amount of operating system resources it can consume. Some examples include:

- Installing users' mailboxes on a different server (preferred), hard drive, or logical partition than the operating system and mail server application
- Configuring the mail server application so that it cannot consume all available space on its hard drives or partitions
- Limiting the size of attachments that are allowed
- Ensuring log files are stored in a location that is sized appropriately.

To some degree, these actions protect against attacks that attempt to fill the file system on the mail server host operating system with extraneous and incorrect information that may cause the system to crash. This also protects against attacks that attempt to fill primary random access memory with unnecessary processes to slow down or crash the system, thus limiting mail server availability. Logging information generated by the mail server host operating system may help in recognizing such attacks. As discussed in Section 9.1, administrators should store mail server logs on centralized logging servers whenever possible, and also store logs locally if feasible. If an attack causes the mail server to be compromised, the attacker could modify or erase locally stored logs to conceal information on the attack. Having a copy of the logs on a centralized logging server gives administrators more information to use when investigating such a compromise.

6.2 Protecting Email from Malware

Email has increasingly been used as a means for sending binary files in the form of attachments. Initially, this did not pose much of a security risk because attachments were mostly small word processing documents or photos. As more organizations began using email for day-to-day collaboration, the size and types of email attachments increased. Today, many email messages are sent with attachments such as program executables, pictures, music, and sounds. Many forms of malware, including viruses, worms, Trojan horses, and spyware—malware intended to violate a user's privacy—are often transmitted in attachments. Increasingly, attackers are using email to deliver zero-day attacks at targeted organizations before these vulnerabilities are known publicly. These attacks are often targeted at office productivity software and give the attacker control over users' workstations. This control can be exploited to escalate privileges, gain access to sensitive information, monitor users' actions (e.g., keystrokes), and perform other malicious actions.

Determining whether to allow certain types of attachments can be a difficult decision for an organization. Not allowing any attachments would simplify a system and make it more secure; however, it would dramatically reduce its usefulness, and users might employ encoding tricks to work around the restriction to "get the job done". Ultimately, organizations choose to allow at least some email attachments.

Organizations should determine which types of attachments to allow. The simplest approach is to allow all types of attachments. If this is the case, then some sort of malware scanner (e.g., anti-virus software, anti-spyware software) should be installed in the mail transit path to filter out known malware, and perhaps even some behavior blocking utility installed at the client to prevent any unwanted operations by executable attachments from occurring. A better approach is to filter potentially dangerous attachment types (e.g., .vbs, .ws, .wsc file extensions) at the mail server or mail gateway, while conducting malware scans on allowed file types. Although filtering on such extensions is a good first step, its effectiveness is limited because attackers can alter the extensions. Instead of simply checking the extension, filtering should check the file header, footer, or other identifying aspects of the file if possible to identify the attachment. Organizations might also wish to consider setting different rules for internally originated versus externally originated email or trusted versus untrusted organizations (e.g., trust .gov/.mil domains), although this latter option is subject to email address spoofing.

Attachment filtering is not completely effective unless all attachments are blocked, and that is not feasible. Some of the most useful attachment types, such as those from office productivity suites, are also some of the riskiest. Also, sophisticated attackers can obfuscate the true nature of their malicious attachments in various ways. For example, attackers sometimes send emails that have hyperlinks to a malicious file on a remote Web site; if a user clicks on the hyperlink and it uses HTTPS instead of HTTP, the malicious file will be downloaded while protected by HTTPS, concealing it from detection by network-based security controls. Organizations could filter active hyperlinks in email messages to prevent this, but this would reduce the usability of email messages for users. Also, an organization might find it desirable for users to place hyperlinks to files in their email messages instead of attaching the files to their messages, since this reduces the load on the mail servers.

Organizations should also consider restricting the maximum acceptable size for email attachments. This benefits mail servers in several ways, including decreasing mail queue latency, storage requirements, and server processor requirements. The combination of these benefits decreases the likelihood of a successful denial of service attack caused by a deluge of oversized messages. [Mell05] However, setting a low maximum size for attachments could inadvertently cause legitimate content to be blocked, reducing the usability and value of the mail system.

Email encryption tends to make filtering more complicated or ineffective. Once a message is encrypted, filtering on the mail server and/or perimeter devices is ineffective unless they can decrypt the message, scan it, and re-encrypt it. This is problematic because of the huge performance requirement. Privacy and other concerns with this sort of solution also exist. Generally speaking, if encryption is used extensively, then filtering has to occur at the end point (mail client user workstation), which is susceptible to being bypassed.

Another vector for email-borne malware that is often overlooked is personal mail accounts accessed via Web browsers. Organizations need to determine if having access to personal mail accounts from organizational computers is appropriate, and if so, take measures to ensure users do not put organization assets at risk when accessing their personal accounts.

In addition to email attachments, malware can be transmitted via email by other means. For example, many mail clients support HTML-based messages. These messages often contain active content in the form of a client-side scripting language or control objects that can affect the client. The most popular types of active content are ActiveX, Java, JavaScript, and Visual Basic Script (VBScript). Organizations should determine whether or not to allow or block active content or forms of active content within email

messages.[36] HTML-based messages also frequently contain other undesirable content, such as spam messages and phishing attempts.[37] Phishing refers to use of deceptive computer-based means to trick individuals into disclosing sensitive personal information. For example, an attacker could send victims an email message that looks as if it were sent from a well-known organization, such as an online business, credit card company, or financial institution. The email is intended to deceive users into responding to the email and disclosing personal data.

If a mail server does not have malware scanning software installed (e.g., anti-virus software, anti-spyware software), or the software is ineffective, the potential security threat posed by malware increases for end users. Some popular mail clients have default configurations that are used by malware to infect client hosts and transmit malware to other users. Section 8 contains additional information on configuring mail clients to improve their security. In addition to mail client configuration, it is important that the mail client hosts use anti-virus software and possibly other security technologies as well to protect them from email-borne threats.

Section 6.2.1 discusses the need for malware scanning for both individual mail clients and the mail infrastructure. Sections 6.2.2 discusses content filtering technologies that can also be helpful at stopping email-borne threats. In addition to deploying and configuring technologies, an organization should also conduct training and awareness activities for users, particularly telecommuters using computers outside the organization's control, so that users can better recognize malicious email messages and attachments and handle them appropriately. This is discussed in Section 6.2.3.

6.2.1 Malware Scanning

To protect against viruses, worms, and other forms of malware, it is necessary to implement scanning at one or more points within the email delivery process. Malware scanning can be implemented on the firewall, mail relay, or mail gateway appliance as the email data enters the organization's network, on the mail server itself, and/or on the end users' hosts. Each option has its own strengths and weaknesses, which are discussed below. Generally, organizations should implement at least two levels of malware scanning—one at the end users' host level and one at the mail server or the firewall/mail relay/mail gateway level—and should consider implementing malware scanning at all three levels.

When providing multiple layers of malware protection, organizations should consider choosing products from different manufacturers. Diversity increases the chances of blocking the latest threats, because the response time of individual manufacturers to new threats varies. This means that when the newest threats appear, one product can often detect them earlier than another over some period of time (typically hours, perhaps a few days). Since each manufacturer uses different detection methods, some products are also better able to detect certain types of new threats than other products.

6.2.1.1 Scanning at the Firewall, Mail Relay, or Mail Gateway Appliance

The first option is scanning for malware at the firewall (application proxy), mail relay (see Figure 6.1), or mail gateway appliance, which can intercept messages before they reach the organization's mail server. The device listens on TCP port 25 for SMTP connections, scans each message, then forwards the

---

[36] For more information on active content, see NIST SP 800-28, *Guidelines on Active Content and Mobile Code*, (http://csrc.nist.gov/publications/nistpubs/).

[37] Limiting the use of HTML within email, such as requiring users to send and view emails in plaintext only, has security benefits but can seriously impact functionality for users, such as causing graphics, hyperlinks, and other HTML-based content to be disabled or suppressed altogether. Some organizations choose to block all HTML-based email because they have decided the security benefits outweigh the loss of functionality.

messages not containing malware to the mail server, which is configured to listen on an unprivileged, unused port, rather than the usual port 25. A disadvantage to this approach is that constant scanning of the SMTP stream can reduce firewall/ mail relay/mail gateway performance. Whether this performance hit is significant depends on mail load, including both the typical number of emails per day and the peak rates of emails, and quality of service requirements. One remedy to improve performance is to offload malware scanning to a dedicated server.

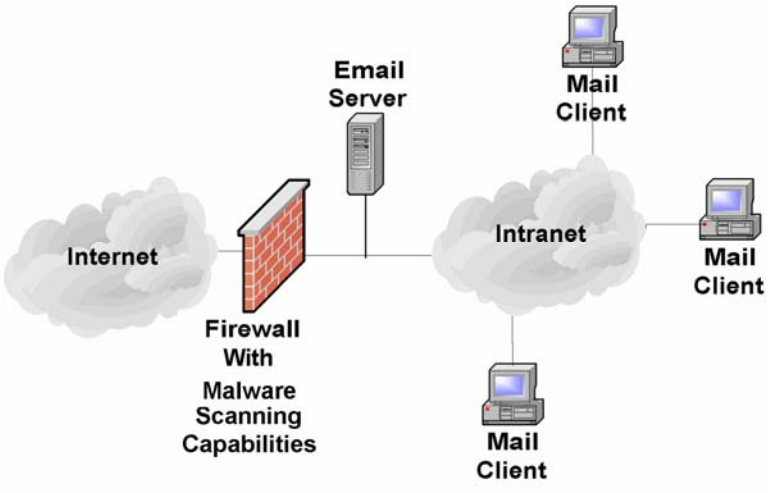

Figure 6.1: Malware Scanning Implemented on Firewall

The benefits of scanning email at the firewall, mail relay, or mail gateway appliance are as follows:

- Can scan email in both directions (inbound and outbound from the organization's network)
- Can stop the majority of messages containing malware at the perimeter before they enter the network and are passed to the mail server
- Can implement scanning for inbound email with minor changes to the existing mail server configuration
- Can reduce the amount of email reaching the mail servers, allowing them to operate more efficiently with lower operational costs
- Can reduce the amount of scanning to be performed by the mail servers, thus reducing their load
- Can centrally manage scanning to ensure compliance with the organization's security policy and regular application of updated malicious code signatures
- For some mail firewall appliances, can provide secure authenticated access to Web-based mail applications.

Scanning for malware at the firewall, mail relay, or mail gateway appliance has a number of weaknesses:

- Can require significant modification of the existing mail server configuration when scanning mail in the outbound direction
- Cannot scan encrypted emails

- Offers no protection to internal users once malware is on the organization's internal network, unless the network is configured so that SMTP traffic gets routed through a dedicated scanner before reaching the mail server
- May require powerful (expensive) servers or appliances to handle the load of a large organization.

6.2.1.2 Scanning on the Mail Server Itself

The second option for placement of a mail malware scanner is on the mail server itself (see Figure 6.2). Many third-party applications are available to scan the contents of the message stores for most popular mail servers. These applications inspect the email sent between internal users, which normally do not pass through the organization's firewall/mail relay/mail gateway. Performing scanning on the mail server also provides an additional layer of protection against malware, and also helps to stop internal malware outbreaks. Some mail servers offer application programming interfaces (API) that support the integration of malware scanning, content filtering, attachment blocking, and other security services within the MTA.

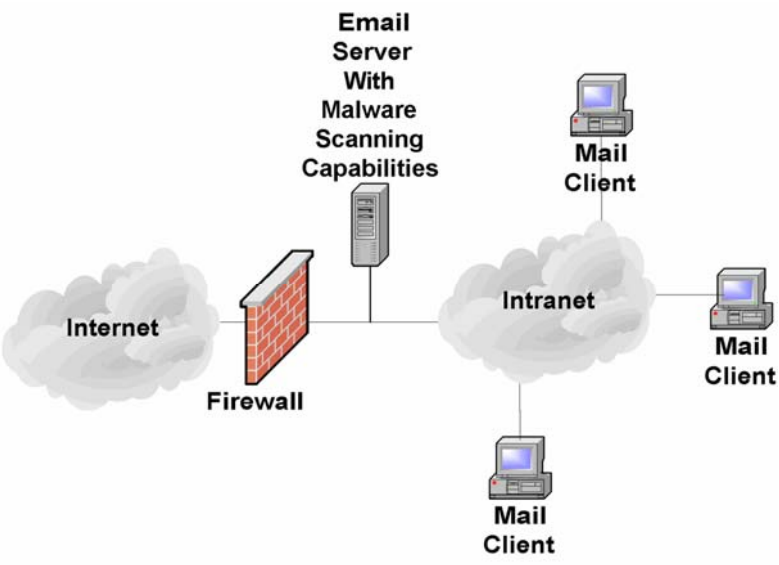

Figure 6.2: Malware Scanning Implemented on Mail Server

The major disadvantage of implementing malware scanning on the mail server is the negative effect on the performance of the mail server caused by the requirement to scan all messages. Also disadvantageous is that malware scanning on the mail server often requires significant modifications to the existing mail server configuration. However, this option provides a number of advantages:

- Can scan email in both directions (inbound and outbound)
- Can be centrally managed to ensure compliance with the organization's security policy and that updates are applied regularly
- Offers protection to internal users once malware is on the organization's internal network.

Scanning for malware at the mail server has a number of weaknesses:

- May require significant modification of the existing mail server configuration (less true for most newer mail servers)

- Cannot scan encrypted emails
- May require more powerful (expensive) servers to handle the load of a large organization.
- Can detect only those threats that have been identified; offers little protection against zero-day exploits.

When considering mail server-based malware scanners, look for the following qualities:

- Detects and cleans all types of malware typically carried by email (e.g., viruses, worms, Trojan horses, malicious mobile code, spyware)
- Provides heuristic scanning (provides some protection from new and unknown malware)
- Provides content filtering (see Section 6.2.2)
- Incorporates mechanisms to help prevent email from circumventing the system
- Provides ease of management
- Provides automated downloading and installation of updates
- Provides frequent updates (critical)
- Can identify and apply rules to different types of content
- Provides a robust and configurable alert mechanism
- Provides detailed logging capabilities (see Section 9.1).

6.2.1.3 Scanning on Client Hosts

Malware scanners can also be located on client hosts (see Figure 6.3). This type of malware scanner is installed on user workstations and mobile devices, such as personal digital assistants (PDA). Incoming emails are scanned as they are opened by the user, and outbound emails are checked as the user attempts to send them. The primary advantage of this type of configuration is that scanning is distributed across many hosts and therefore has minimal effect on the performance of each individual host. Also, if a client machine becomes infected with malware, this layer of protection might stop the malware from spreading to the mail server and other mail clients.

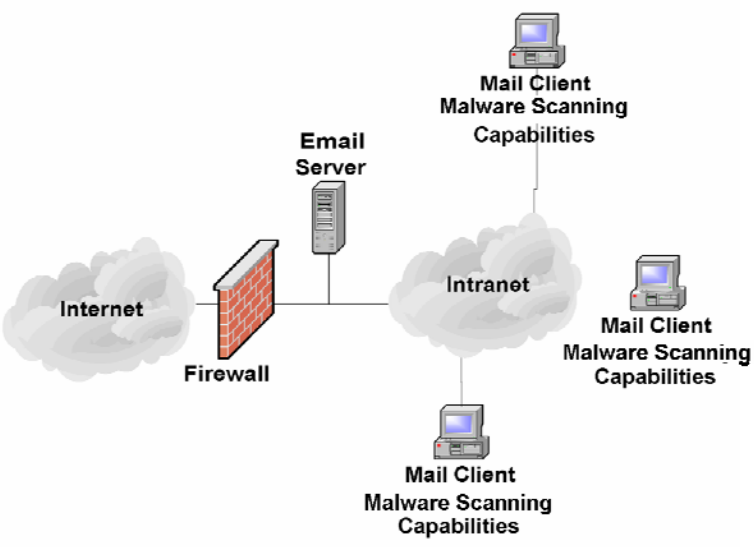

Figure 6.3: Malware Scanning Implemented on User Workstations

The greatest challenge of implementing malware scanning on user workstations is the difficulty in managing and regularly updating the distributed malware scanners. However, enterprise-level solutions for malware scanning provide a means of central administration of malware scanners on individual hosts. Another weakness is that to the degree that users have control of the malware scanner, end users may disable some or all of its functionality (whether accidentally or intentionally). Enterprise solutions offer the capability to lock down some or all of the clients' scanners' functionality to ensure they are configured correctly.

The benefits of client-side malware scanning are as follows:

- Does not require any modification to the mail server
- Can scan encrypted emails when they are decrypted by the user
- Distributes malware scanning and thus minimizes the impact of scanning on any one host
- Offers protection to internal users, even when malware is received from an internal user.

The disadvantages of client-side malware scanning are as follows:

- Can be difficult to centrally manage, especially for mobile client hosts (e.g., laptops)
- Can take time before users update malware scanners, resulting in the organization being more susceptible to an outbreak
- Can be intentionally or accidentally disabled or weakened by users.
- Can detect only those threats that have been identified; offers little protection against zero-day exploits.

6.2.2 Content Filtering

Content filtering works in a similar manner to malware scanning at the firewall or mail server except that it is looking for emails containing undesirable content other than malware, such as spam or emails

containing inappropriate language. When implementing file-type restrictions and malware scanning, only a certain level of security is provided. The contents of an email message or its attachments could prove much more damaging to an organization than a virus or rogue executable. For this case, some sort of content filtering mechanism should be employed.

6.2.2.1 Implementing Content Filters

For maximum effectiveness, content filtering should be performed on all incoming and outgoing messages and conducted in the same locations as malware scanning—on the firewall/mail relay/mail gateway, mail servers, and end users' hosts. In fact, many products are available for popular messaging systems that incorporate content filtering, malware scanning, and file-type restriction (see Appendix D for a listing of common products). Incorporation of these features into one product can reduce the administration of security controls.

In general, rules are defined to forward, quarantine, park, clean, block, or delete any data passing through the server depending upon the results of the scan. Typical items that would be caught by the filter and possible actions taken on them could be as follows:

- Email that contains suspicious active content (e.g., ActiveX, JavaScript) is stripped of the active code and forwarded to the recipient.
- Spam email and phishing attempts may be deleted or tagged as suspicious.
- Extra-large files might be held for delivery during off-peak hours.

Another key feature of content filtering packages is the scanning of outbound data. A lexical analysis can be performed that scans email messages for words and phrases that might be viewed as inappropriate for use in organizational email. The lexical analysis can also save possible litigation against an organization by preventing inappropriate content, including hoaxes and spam (see Section 6.3), from leaving the organization. In addition, a lexical analysis might include searches for key words and phrases indicating that sensitive data is leaving the enterprise.

Organizations should also take steps to prevent email address spoofing, such as ensuring that external users cannot send emails to internal users that have one of the organization's email addresses as the spoofed sender. For example, a hypothetical company WidgetsRUs should block any incoming email with a "from" address in the domain widgetsrus.com at its mail gateway. Attackers often spoof email addresses to make their malicious emails appear to be from internal users, because it can trick users into trusting the emails. Checking digital signatures on emails is a way that users can detect some spoofing attempts.[38]

Before implementing any filtering solution, it is imperative to determine how the existing network and applications actually work. This entails running network analyzers (sniffers); analyzing router, firewall, and server log files; and interviewing all appropriate system and network administrators. It is also imperative to analyze the existing organization information system security policy, or draft one if one does not exist. Clearly defined security policies are critical to translating the organization's security goals into filter rules. Great care must be taken in crafting the rules because an incorrectly configured filter may fail to filter inappropriate content or may accidentally filter appropriate content. These steps will

[38] There are some emerging experimental standards for email sender verification, including Sender ID (currently defined in RFC 4406) and Sender Policy Framework (currently defined in RFC 4408). More information on these approaches is available at http://www.ietf.org/rfc/rfc4406.txt and http://www.ietf.org/rfc/rfc4408.txt, respectively.

make it easier to choose the appropriate filtering software and determine the types of rules that need to be configured.

Another effective way to decrease the number of unwanted messages reaching mail servers is using Lightweight Directory Access Protocol (LDAP) lookup on a mail gateway or firewall as a filtering mechanism. LDAP lookup allows the gateway or firewall to query the organization's user directory directly for user information. When an email is received by the gateway or firewall, it contacts the user directory to see if the email is addressed to a user that actually exists. If the user is not in the directory, the email is rejected and does not reach the mail server. Much of the spam sent to a domain is generated using a database of common usernames. Most of these addresses do not exist for a particular domain, but it is an easy method for spammers to get their messages to many users quickly. Using LDAP lookup prevents these messages from slowing the mail server.

Many Internet service providers (ISP) and third-party companies offer malware scanning and content filtering services, including spam filtering. These services can be helpful for organizations that wish to add an extra layer of defense but do not want to implement or maintain the extra layer of protection themselves. The services delete or tag messages before they reach an organization's mail server, therefore increasing its efficiency. Because these services may monitor emails for many organizations, they can often identify new unwanted messages very quickly. Disadvantages of using such a service include the following:

- **Privacy.** All of the organization's incoming email is routed through the service provider's servers and scanned by them.
- **False Positives.** The service provider's filtering solution might automatically delete emails tagged as spam or might not provide a way for administrators to check the validity of email tagging.
- **Availability.** If the service becomes unavailable, the organization should be able to change the routing of email to prevent delays in mail delivery.

6.2.2.2 Content Filtering Issues

Although email content filtering is critical to most organizations' security posture, a number of legal implications should be addressed before deployment. Content filtering needs to be backed up by a clearly defined written security policy. The email policy should include an explicit statement that email will be monitored for compliance, a description of any administrative or disciplinary actions that could result if the policy is violated, and a requirement for employees to acknowledge reading and understanding the policy. Although the policy should outline the organization's thinking, expectations, and restrictions regarding security, due regard should also be given to employee and individual rights. For instance, under some circumstances employees may have a right to privacy when it comes to their own correspondence; however, when representing their organization, the organization may be held legally responsible for what they say or do. Without an established policy, such issues often lead to misunderstanding and problems that can be difficult to resolve.

Similarly, in some situations, email messages may be deemed to carry the same legal weight as written documents, especially when digitally signed. This can mean having to store messages to comply with record-keeping requirements, including employees' personal messages. As such, all employees should be made aware of the security policy. To the extent possible, the security policy should be broadly distributed to employees [McKi01]. Moreover, it may be advisable to require employees to acknowledge the policy as part of their contract of employment or as a condition of working on a contract, and to also require employees to re-acknowledge the policy on a regular basis. Many email filter applications can

add a legal disclaimer to all incoming and outgoing messages, ensuring recipients understand the legal weight (or lack thereof) of the emails received from or through the organization.

Appropriate legal, privacy, personnel, and human resources authorities should be consulted when forming the policy. Inevitably, this means having the policy reviewed by experts to ensure that it is legally correct and does not infringe upon the rights of employees. Additionally, it is important to investigate all areas of an organization to determine how workers go about their work and what level of security is most appropriate. Completely restricting access to Internet resources might solve most security issues at a stroke, but this is usually an unacceptable tradeoff. This is where email filtering tools can help, enabling security policies to be more easily converted from theory into practice.

As previously mentioned, personal email accounts are problematic, especially those accessed via a Web browser that tend to bypass the email content filtering controls. In particular, if a user is using an SSL-encrypted Web page for personal email access and the organization does not decrypt and analyze SSL-encrypted HTTPS traffic, the content may be allowed out or in even though it would not be if it went through normal channels. Many organizations also allow encrypted protocols outbound (e.g., from their internal network to the Internet) such as SSH or IPsec that can also be used to tunnel traffic in or out of the organization without the restrictions of filtering.

If an organization allows mail protocols, such as SMTP, outbound to the Internet for all internal users, content filtering may be bypassed by users setting up their own mail servers. Organizations should be aware that certain products and applications use SMTP email for communications. It is not uncommon in large organizations for a significant percentage of the outbound email traffic to be generated by servers other than the centralized enterprise mail servers. Often these emails are generated from electronic commerce applications communicating with customers or business partners. One way to address the problem is to set up a mail gateway or application proxy at the perimeter that does content filtering on all email, even those messages generated by or destined to servers other than the centralized enterprise mail servers. Section 7 provides additional information on network architectures and mail gateway placements.

6.2.3 User Awareness

In addition to using anti-virus software and/or other malware scanning tools, as well as content filtering software, organizations should educate users about the dangers posed by email-borne malware and effective ways of avoiding threats, including the following actions:

- Never open attachments from unknown senders.
- Never open attachments with suspicious or potentially harmful names or file extensions (e.g., attachment.txt.vbs, attachment.exe) from known or unknown senders.
- Be suspicious of emails from known senders in which the subject line or content appears to be inappropriate for the existing relationship (e.g., an email with the subject “I love you” from a professional colleague) or generic subjects (e.g., “Look at this, it’s interesting”).
- Scan all attachments with malware scanning software before opening, preferably by configuring the scanning software to automatically perform this task.
- Update the signature database of the malware scanning software at least on a daily basis or when there is a malware outbreak.
- Warn users about malware outbreaks and how to identify emails that might contain malware.

Users should also be aware of the dangers of phishing attacks and how to avoid them. The Federal Trade Commission (FTC) posted a consumer alert outlining steps that users should take: [FTC06]

- Do not reply to email messages or popup ads asking for personal or financial information.
- Do not trust phone numbers in emails or popup ads. Voice over IP technology can be used to register a phone with any area code.
- Do not email personal or financial information.
- Review credit card and bank account statements regularly.
- Be cautious about accessing untrusted Web sites, because some Web browser vulnerabilities can be exploited simply by visiting a site. Users should also be cautious about opening any attachment or downloading any file from untrusted emails or Web sites.
- Forward phishing-related emails to spam@uce.gov and to the organization that is impersonated in the email.
- Request a copy of your credit report from each of the three credit reporting agencies yearly: Equifax, Transunion, and Experian. If an identity thief opens up accounts in your name, they will likely show up on a credit report.[39]

6.3 Blocking Spam-Sending Servers

Regardless of the communication medium, there are always entities that attempt to exploit any means of communication to publicize their ideas or products. Email is no exception. The most common terms for these messages are unsolicited commercial email (UCE), which is better known as spam. Most email users receive spam on a daily basis. Because email is largely unregulated, system administrators should police email traffic that traverses the servers they operate to reduce the amount of spam that reaches users. An added benefit of implementing server-based spam control is that it will reduce mailbox sizes, which in turn reduces server storage requirements.[40]

To control spam messages, administrators must address the following three concerns:

- Ensure that spam cannot be sent from the mail servers they control (see Section 6.4).
- Implement spam filtering for inbound messages (see Section 6.2).
- Block messages from known spam-sending servers—the topic of this section.

Because the Internet has no centralized policing authority, non-profit organizations and commercial companies have created lists of mail servers that have been identified as being used to send unsolicited email messages. These lists are often referred to as open relay blacklists (ORB) or DNS blacklists (DNSBL). Many popular mail server applications can be configured to query multiple ORBs and reject messages originating from the listed mail servers. These lists are updated on a daily basis; therefore, using them can drastically reduce spam message delivery. Additionally, most mail servers can be configured to reject messages from an explicitly defined set of domains.

---

[39] Under the Fair and Accurate Credit Transactions Act of 2003, consumers can request a free credit report from each of the three consumer credit reporting companies once every twelve months. See http://www.ftc.gov/os/statutes/fcrajump.htm for more information.

[40] For more information on spam, see RFC 2505, *Anti-Spam Recommendations for SMTP MTAs* (http://ietf.org/rfc/rfc2505.txt).

ORB spam control is not foolproof. Open relays are connected and disconnected regularly. Mail server administrators who wish to participate in the policing effort may submit UCE complaints to Web sites provided in Appendix E.

6.4 Authenticated Mail Relay

As mentioned previously, configuring mail relay authentication decreases the likelihood of someone using a particular mail server to send spam. An added benefit of implementing authenticated relay is increased security and usability.

Two methods are available for controlling mail relay. The first is to control the subnet or domain from which messages are being sent. This method is effective if the perimeter of the messaging system resides within known address ranges. However, if remote users have hosts with different address ranges, this method is not useful. To accommodate remote users, a more robust configuration is needed.

The second method is to require users to authenticate themselves before sending any messages. This is commonly referred to as authenticated relay, or SMTP AUTH, which is the SMTP extension that supports user authentication. Unfortunately, the default configuration of most mail servers does not implement authenticated relay; therefore, mail server administrators must configure the server appropriately. Requiring authenticated relay is one of the least used but most powerful security features of mail servers. (Refer to manufacturer documentation for configuring SMTP AUTH.)

Mail server administrators must use caution if choosing to have an authenticated relay. An improperly configured mail server could be exploited and used to send or relay spam. If the mail server is found to be an open relay, it might be put on a blacklist (as described in Section 6.3). Any organizations subscribing to and using these blacklists will not be able to receive any email from a blacklisted server, whether the messages are spam or valid emails.

If a mail server administrator learns that one of his or her mail servers is on a blacklist, the administrator will have to fix the open relay problem and perform testing to ensure the server is no longer relaying. The administrator then needs to determine which blacklists the server is on and check with each blacklist maintainer to get instructions on how to remove the server from the lists. Until the server has been removed from all blacklists and the updated blacklists have been propagated to their subscribers, outbound email from the organization may not reach all of its recipients. See Appendix D for a listing of Web sites that provide open relay testing tools as well as the maintainers of commonly used blacklists.

6.5 Secure Access

In Section 2, different mail transport and mailbox access protocols were discussed. Like many Internet protocols, most of these protocols did not initially incorporate any form of encryption or cryptographic authentication. These deficits posed three problems for email users. First, for users sending messages, the contents could be intercepted and read at any host on the path between the sender and recipient or even forged or modified. An apt paradigm from “regular” mail would be a postcard. Any person who handles the postcard could read the message on the back. Second, the recipients could not verify that messages were not modified by others during transit or actually originated by the sender. Third, rather than supplying non-reusable authentication information, a user accessing a mailbox would send a password over the network in the clear, which could be easily observed and reused by an attacker. Unfortunately, in most default configurations, mail clients are set up to send the user’s password in the clear, allowing it to be intercepted by other computers on the local network segment of the client or any host responsible for forwarding the password to the mail server.

The first two problems were addressed in Section 3, which discussed ways to protect messages. The third problem can be resolved by applying the same method normally used to secure World Wide Web (WWW) traffic – the Transport Layer Security (TLS) protocol.

TLS is similar to the Secure Sockets Layer (SSL) protocol, upon which it is based, and can be used in combination with POP, IMAP, and SMTP to encrypt communication between mail clients and servers. RFC 2595 defines how to use TLS to combat communications eavesdropping, to implement secure mailbox access and to further strengthen SMTP MTAs that incorporate SMTP AUTH. Figure 6.4 shows a sample configuration that enables TLS support for newer versions of sendmail.

```
define(`CERT_DIR', `MAIL_SETTINGS_DIR``'certs')dnl
define(`confCACERT_PATH', `CERT_DIR')dnl
define(`confCACERT', `CERT_DIR/CAcert.pem')dnl
define(`confSERVER_CERT', `CERT_DIR/MYcert.pem')dnl
define(`confSERVER_KEY', `CERT_DIR/MYkey.pem')dnl
define(`confCLIENT_CERT', `CERT_DIR/cert.pem')dnl
define(`confCLIENT_KEY', `CERT_DIR/MYkey.pem')dnl
```

Figure 6.4: Sendmail TLS Configuration Example from sendmail.mc

6.6 Enabling Web Access

Increasingly, organizations are providing Web browser-based access to their messaging systems. Enabling this type of access could introduce security issues at both the client (see Section 8.4) and server. Although Web site security is outside the scope of this document, there are several key concepts that should be followed:

- Avoid placing the Web server on the same machine as the mail server.
- The authentication mechanism of the Web front-end should employ encryption.
- The Web server should use SSL/TLS to encrypt all communications with clients.
- As with any public server, the Web server should be hardened before connecting it to the network.[41]

For some organizations, the processing requirements of dedicating a Web server to SSL/TLS communication may not be possible to accommodate. In cases such as this, the initial authentication should be encrypted.

Some organizations choose to use hardware appliances for their Web access solution. These appliances not only provide secure Web-based access to mail servers, but they also provide firewall, content filtering, and malware protection capabilities. The appliances typically are easier and faster to install and maintain than creating Web servers, and they often use hardened operating systems with all non-essential components disabled or removed, which limits the possible vulnerabilities the appliances might have. Some appliances offer additional capabilities, such as offering administrators granular control over user groups and access, performing SSL encryption for sessions, and terminating user sessions automatically

[41] For more information on securing Web servers, please refer to NIST SP 800-44, *Securing Public Web Servers* (http://csrc.nist.gov/publications/nistpubs/).

after a period of inactivity. Appliances are available that support the most commonly used Web-based mail systems.

Client security issues exist that also need to be considered before an organization approves the deployment of Web access to email. These issues are discussed in Section 8.4.

6.7 Checklist for Securing Mail Servers and Content

Completed	Action
	Harden the mail server application
☐	Install the mail server software on a dedicated host (if Web-based mail access is desired, install the mail server software on a different host from the Web server)
☐	Apply any patches or upgrades to correct for known vulnerabilities
☐	Create a dedicated physical disk or logical partition (separate from operating system and mail server application) for mailboxes, or host the mailboxes on a separate server
☐	Remove or disable all services installed by the mail server application but not required (e.g., Web-based mail, FTP, remote administration)
☐	Remove or disable all unneeded default login accounts created by the mail server installation
☐	Remove all manufacturer documentation from server
☐	Remove any example or test files from server
☐	Apply appropriate security template or hardening script to the server
☐	Reconfigure SMTP, POP and IMAP service banners (and others as required) NOT to report mail server and operating system type and version
☐	Disable dangerous or unnecessary mail commands (e.g., VRFY and EXPN)
	Configure operating system and mail server access controls
☐	Limit the access of the mail server application to a subset of computational resources
☐	Limit the access of users through additional access controls enforced by the mail server, where more detailed levels of access control are required
☐	Configure the mail server application to execute only under a unique individual user and group identity with restrictive access controls
☐	Ensure the mail server is not running with root or system/administrator privileges
☐	Configure the host operating system so that the mail server can write log files but not read them
☐	Configure the host operating system so that temporary files created by the mail server application are restricted to a specified and appropriately protected subdirectory
☐	Configure the host operating system so that access to any temporary files created by the mail server application is limited to the mail server processes that created these files
☐	Ensure that the mail server cannot save files outside of the specified files structure dedicated to the mail server
☐	Configure the mail server to run in a chroot jail on Linux and Unix hosts
☐	Install users' mailboxes on a different server (preferred), hard drive, or logical partition than the operating system and mail server application

Completed	Action
☐	Configure the mail server application so it cannot consume all available space on its hard drives or partitions
☐	Limit the size of attachments that are allowed
☐	Ensure log files are stored in a location that is sized appropriately
	Protect email from malware
☐	Determine which types of attachments to allow
☐	Consider restricting the maximum acceptable size for attachments
☐	Determine if having access to personal email accounts from organizational computers is appropriate
☐	Determine which types of active content should be permitted within email messages
☐	Implement centralized malware scanning (on the firewall, mail relay, mail gateway, and/or mail server)
☐	Install malware scanners on all client hosts
☐	Implement centralized content filtering
☐	Configure content filtering to block or tag suspicious messages (e.g., phishing, spam)
☐	Configure content filtering to strip suspicious active content from messages
☐	Configure lexical analysis if required
☐	Take steps to prevent address spoofing, such as blocking emails from external locations using internal “From” addresses
☐	Create a security policy that addresses content filtering
☐	Have the security policy reviewed by appropriate legal, privacy, and human resources authorities
☐	Add a legal disclaimer to emails, if required
☐	Educate users on the dangers of malware and how to minimize those dangers
☐	Notify users when an outbreak occurs
	Block spam-sending servers
☐	Configure mail gateways or firewalls to use LDAP lookup to confirm the existence of email recipients
☐	Configure mail server to block email from open relay blacklists or DNS blacklists, if required
☐	Configure mail server to block email from specific domains, if required
	Use authenticated mail relay
☐	Configure authenticated mail relay on the server
	Secure access to the mail server
☐	Configure mail server to use encrypted authentication
	Enable Web access to email
☐	Configure mail server to support Web access only via SSL/TLS and only if such access is deemed necessary

This page has been left blank intentionally.

7. Implementing a Secure Network Infrastructure

The network infrastructure that supports the mail server plays a critical role in the security of the mail server. In most configurations, the network infrastructure is the first line of defense between the Internet and a mail server. Network design alone, however, cannot protect a mail server. The frequency, sophistication, and variety of attacks perpetrated today lend support to the idea that email security must be implemented through layered and diverse protection mechanisms. This section discusses those network components that can support and protect mail servers to further enhance their overall security. While security issues are paramount, network infrastructure considerations are influenced by many factors other than security, including cost, performance, and reliability.

7.1 Network Composition and Structure

Firewalls and routers are devices or systems that control the flow of network traffic between networks. They can protect mail servers from vulnerabilities inherent in the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and help reduce the security issues associated with insecure applications and operating systems. However, an organization has many choices when determining a network environment for the mail server, and security may not be the principal factor in deciding among those options. Network composition and structure are the first and in many respects the most critical decisions that affect mail server security, since they determine what network infrastructure elements protect the mail server. For example, if the mail server is located before the organization's main firewall, then the firewall cannot be used to control traffic to and from the mail server. Network composition and structure also determine what other portions of the network are vulnerable if the mail server is compromised. For example, an externally accessible mail server located on the internal production network subjects the internal network to attack if the mail server is compromised.

7.1.1 Inadvisable Network Layout

Some organizations choose to locate their public mail servers on their internal production networks. That is, their mail servers reside on the same network as the internal users and servers. The principal weakness of this layout is that it exposes internal network components to additional risks. Mail servers are often targets of attackers. If attackers manage to compromise a mail server, they will have access to the internal network and be able to more easily compromise internal hosts. Therefore, this layout is not recommended.

Another network layout that is not generally recommended is placing the mail server before an organization's firewall or router that provides IP filtering. In this structure, the network provides little, if any, protection for the mail server. Because the mail server itself has to maintain security, it provides a single point of failure. To be even somewhat secure in this location, the mail server operating system and application have to be well-hardened, with all unnecessary and insecure services disabled and all necessary security patches applied. To maintain the "security" of the setup, the mail server administrator must stay up-to-date on vulnerabilities and related patches. Another limitation of this structure is that providing any sort of secure remote administration capability is difficult.

7.1.2 Demilitarized Zone

A demilitarized zone (DMZ) describes a host or network segment inserted as a "neutral zone" between an organization's private network and the Internet. It prevents outside users of the mail server from gaining direct access to an organization's internal network (intranet). A DMZ mitigates the risks of locating a mail server on an internal network or exposing it directly to the Internet. It is a compromise solution that offers the most benefits with the least amount of risk for most organizations. The DMZ allows access to

the resources located within it to both internal and external users. There are a wide variety of DMZ configurations, each with its own strengths and weaknesses.

Creating a DMZ involves placing a firewall between an organization's border router and its internal network, and creating a new network segment that can only be reached through the DMZ device. The mail server or mail gateway is placed on the new segment, along with other network infrastructure components and servers that need to be externally accessible. For example, if Web-based mail access is offered, the associated servers are typically placed on the DMZ. In some configurations, the border router itself may act as a basic firewall. Figure 7.1 illustrates an example of this simple DMZ using a router with access control lists (ACL) to restrict certain types of network traffic to and from the DMZ.

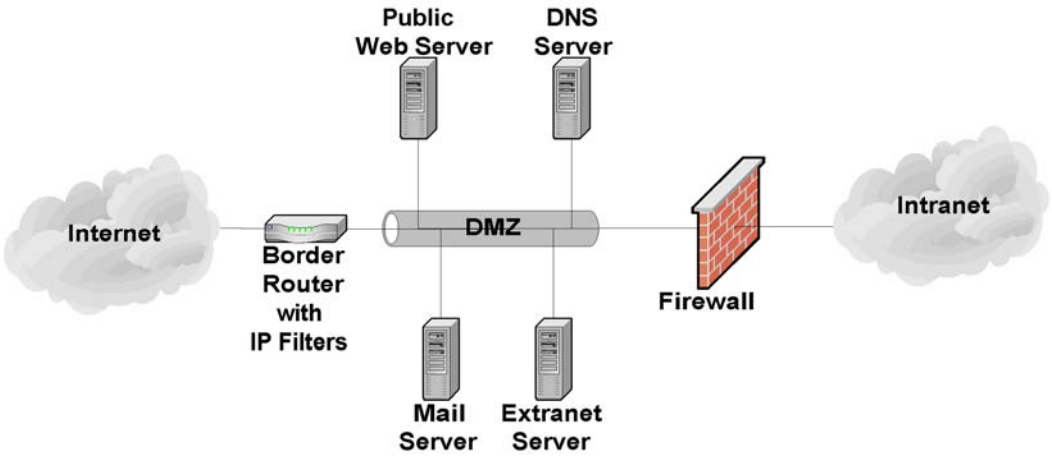

Figure 7.1: Simple Single-Firewall DMZ

A single-firewall DMZ is a low-cost approach, since the organization needs only to add a single firewall and use its existing border router to provide protection to the DMZ. It is usually appropriate only for small organizations that face a minimal threat. The basic weakness in the approach is that while the router is able to protect against most network attacks, it is not "aware" of the mail server application layer protocols (e.g., SMTP, POP, IMAP) and thus cannot protect against application layer attacks aimed at the mail server. In addition, a router cannot provide any virus scanning of incoming email. A superior approach is to add a second firewall between the Internet and the DMZ, as shown in Figure 7.2.

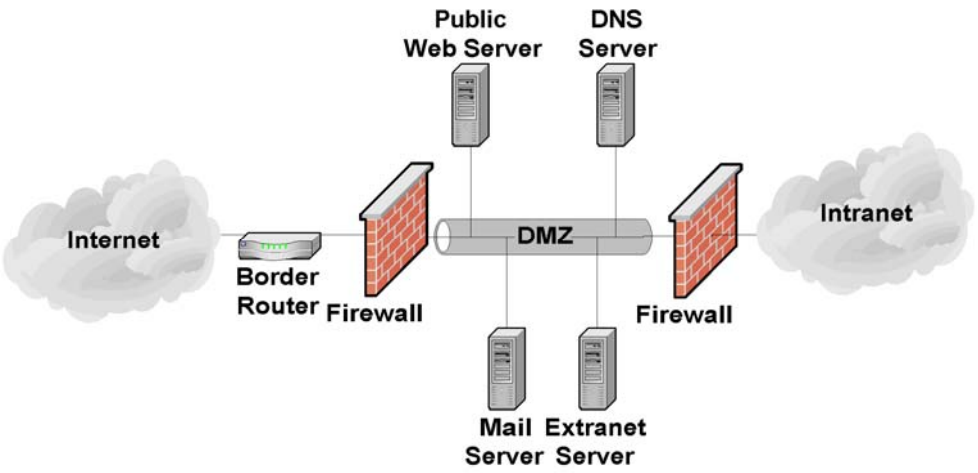

Figure 7.2: Two-Firewall DMZ

A two-firewall DMZ configuration improves protection over a router-firewall DMZ, since the dedicated firewalls can have more complex and powerful security rule sets. In addition, because a dedicated firewall is often able to analyze incoming and outgoing mail traffic, it can detect and defend against application layer attacks aimed at the mail server. Depending on the rule sets of the firewalls and the level of traffic the DMZ receives, this type of DMZ may result in some performance degradation.

For organizations that desire the security of the two-firewall DMZ, but do not have the resources to purchase two firewalls, another option exists called the "service leg" DMZ. In this configuration, a firewall is constructed with three (or more) network interfaces. One network interface attaches to the border router, another interface attaches to the internal network, and a third interface connects to the DMZ (see Figure 7.3).

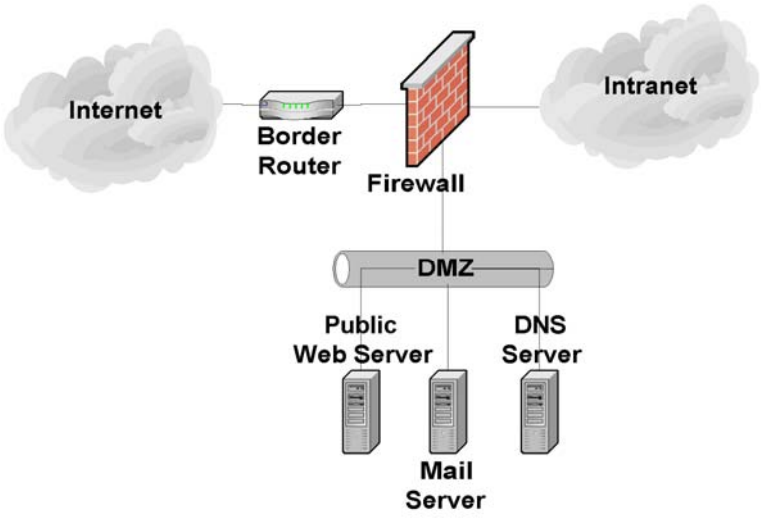

Figure 7.3: Three-Interface Firewall DMZ

This configuration subjects the firewall to an increased risk of service degradation during a DoS attack aimed at the DMZ. In the standard single-firewall DMZ network configuration discussed above, a DoS attack against the mail server generally affects only the mail server. In a service-leg DMZ network

configuration, the firewall bears the brunt of any DoS attack because it must examine any network traffic before the traffic reaches the mail server (or any other DMZ or internal network resource) [Wack02a]. However, it is increasingly likely that a DoS attack will take the form of a distributed denial of service (DDoS) attack and consume all of the incoming network bandwidth and related devices (e.g., Internet border routers) before ever reaching a DMZ firewall.

The advantages of a DMZ from a security standpoint are as follows:

- The mail server may be better protected, and network traffic to and from the mail server can be monitored.
- Compromise of the mail server does not directly threaten the internal production network.
- Greater control can be provided over the security of the mail server since traffic to and from the mail server can be controlled.
- The DMZ network configuration can be optimized to support and protect the mail servers.

The disadvantages of a DMZ from a security standpoint are as follows:

- DoS attacks aimed at the mail server may have an effect on the internal network.
- Depending on the firewall configuration controlling traffic between the DMZ and internal network, it may be possible for the mail server to be used to attack or compromise hosts on the internal network. In other words, protection offered by the DMZ depends in large part on the firewall configuration.

7.1.3 Mail Gateways

Using a mail gateway in the DMZ adds further protection for a mail server. The additional layer makes the mail server significantly more difficult to attack. When a mail server is located in the DMZ, it still must communicate with untrusted third parties, which provides an avenue for attackers. A mail gateway acts as a proxy between the real mail server and the Internet. All messages and communications must go through the proxy before they are forwarded to the mail server. Breaking the direct line of communication between the Internet and the mail server makes it much more difficult to attack the mail server. Since the mail gateway generally requires only limited functionality, it is much easier to harden and secure than a fully functional mail server. Figure 7.4 provides an example of using a mail gateway to fortify a mail server on the internal network.

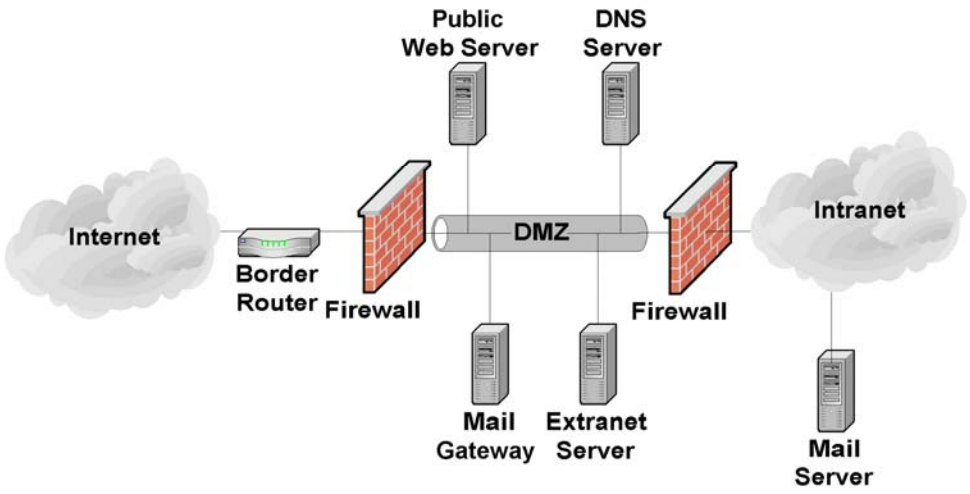

Figure 7.4: Mail Gateway

7.1.4 Management Network

Mail servers, gateways, and other important components can be connected to each other and managed through an organization's standard networks or through a separate network known as a *management network*. If a management network is used, each host being managed through the network has an additional network interface known as a *management interface* that connects to the management network. Also, each host being managed is unable to pass any traffic between its management interface and any of its other network interfaces. Consoles and other hosts that are used to manage the mail components are attached to the management network only. This architecture effectively isolates the management network from the production networks. The benefits of doing this are to protect the components from some attacks and to ensure that the components can be managed under adverse conditions (e.g., widespread email-borne malware infection). Disadvantages of using a management network include the additional costs in networking equipment and other hardware (e.g., PCs for the consoles) and the inconvenience for mail component administrators of using separate computers for management and monitoring.

7.2 Network Element Configuration

Once the mail server has been positioned in the network, the network infrastructure elements should be configured to support and protect it. The elements of a network infrastructure that affect mail server security are firewalls, routers, intrusion detection and intrusion prevention systems, and switches. Each has an important role to play and is critical to the overall strategy of protecting the mail server through layered protection. Unfortunately, when it comes to securing a mail server, there is no single "silver bullet" solution. A firewall or intrusion prevention system alone cannot adequately protect a mail server from all threats or attacks.

7.2.1 Router/Firewall Configuration

Several types of firewalls exist. The most basic ones are routers that can provide access control on IP packets. In the middle are stateful firewalls that can provide access control based on TCP and User

Datagram Protocol (UDP) as well as IP. The most powerful firewalls are application layer or proxy firewalls that are able to understand and filter email content and commands.[42]

A common misperception about firewalls and routers (acting as firewalls) is that they eliminate all risk and can protect against the misconfiguration of the mail server or poor network design. Unfortunately, this is not the case. Firewalls and routers themselves are vulnerable to misconfiguration and software vulnerabilities. In addition, most firewalls have limited or no "insight" into the application layer where many current attacks occur. Thus mail servers in particular are vulnerable to many attacks, even when located behind a secure, well-configured firewall.

A firewall or router (acting as a firewall) that is protecting a mail server should be configured to block all access to the mail server from the Internet except the necessary ports, such as TCP port 25 (SMTP). A firewall is the first line of defense for a mail server; however, to be truly secure, organizations need to implement layered protection for their mail servers (and networks). Most importantly, organizations should strive to maintain all systems in a secure posture and not depend solely on routers, firewalls, or any other single component to stop attackers.

A modern enterprise router is able to function as a network and transport layer filter (e.g., a basic firewall). A router functioning as a network/transport layer firewall can provide filtering based on several pieces of information [Wack02a], including the following:

- Source IP address
- Destination IP address
- Traffic type
- TCP/UDP port number and state.

The strengths of routers are in the following areas:

- Cost (most organizations already have a border router that can be configured to provide network/transport layer firewall capabilities).

The weaknesses of routers are in the following areas:

- Susceptibility to application layer attacks (e.g., cannot examine email content or commands)
- Susceptibility to attacks via allowed ports (routers are generally weaker than firewalls in this area because the routers do not perform analysis at the application layer, but the firewalls do, allowing the firewalls to recognize some attacks sent via allowed ports)
- Difficulty of configuration and administration
- Limitations in logging capabilities
- Processing capabilities may be more limited and overtaxed by complex rule sets (i.e., access controls lists)
- Insufficient rule set expressiveness and filtering capabilities.

---

[42] For more information about firewalls, see NIST SP 800-41, *Guide to Firewall Selection and Policy Recommendations,* (http://csrc.nist.gov/publications/nistpubs/).

The only "pure" network layer firewalls available today are small office/home office (SOHO) firewall appliances and personal firewalls [Wack02a] that may only perform basic packet-level filtering.

Stateful inspection firewalls are transport layer devices that incorporate "awareness" of the state of a TCP connection. Stateful inspection firewalls maintain internal information such as the state of the connections passing through and the contents of some of the data streams. This allows better and more accurate rule sets and filtering to be specified. Stateful inspection firewalls add the capability to enforce rules based on connection state to the capabilities of a filtering router.

Application layer firewalls (sometimes called application-proxy gateway firewalls) are advanced firewalls that combine network and transport layer access control with application layer functionality. Application layer firewalls permit no traffic directly between the Internet and the internal network, or between two networks. They can usually perform extensive logging and access control.

Application layer firewalls are considered the most secure type of firewall and have numerous advantages over packet filtering routers and stateful inspection firewalls, including the following areas:

- Logging capabilities
- Filtering capabilities (can filter specific types of email content and specific SMTP, POP, and IMAP commands)
- Ease of configuration
- User authentication capabilities.

The primary disadvantages that application layer firewalls have when compared to packet filtering routers and stateful inspection firewalls are as follows:

- Speed of throughput.
- Cost (if high end hardware is required to operate effectively)
- Support for less popular and new protocols.

Although not strictly a limitation, application layer firewalls are sometimes implemented on hosts running general-purpose operating systems (e.g., Windows, Linux, Unix). This arrangement introduces an added layer of complexity because that general-purpose operating system must also be secured in addition to the firewall software itself. Application layer firewalls are increasingly being deployed as appliance-based devices, which may use specialized operating systems. Routers and stateful inspection firewalls also typically run on specialized operating systems.

To successfully protect a mail server using a firewall, ensure that the firewall is patched to the latest or most secure level (application and underlying operating system) and is both capable of and configured to support the following items:

- Control all traffic between the Internet and the mail server
- Block all inbound traffic to the mail server except that traffic which is required, such as TCP port 25 (SMTP).
- Block (in conjunction with the intrusion detection or prevention system [see Section 7.2.2]) IP addresses or subnets that the IDS or IPS reports are attacking the organizational network

- Block known "blacklisted" networks or subnets as identified by a trusted external security response center
- Notify the network or mail server administrator of suspicious activity through an appropriate means (e.g., page, email, network trap)
- Provide content filtering
- Provide malware scanning
- Protect against DoS attacks
- Log critical events, including the following details:
  - Time/date
  - Interface IP address
  - Manufacturer-specific event name
  - Standard attack event identifier (if one exists)
  - Source and destination IP addresses
  - Source and destination port numbers
  - Network protocol.

Most firewall devices available in hardware and software perform some type of logging of the traffic they receive. For most firewalls, the default logging configuration is suitable, provided logging is enabled. Administrators should consult their manufacturer documentation if they believe they require additional information to be logged. Certain brands of hardware-based firewalls include an ability to track and log information for each rule. This ability enables accountability to a very specific extent.

Many firewalls support the ability to selectively decide what information to log. If a firewall receives a series of similar packets from the same location, it may decide not to log any additional packets after the first one. Although this is a valuable feature, consider the consequences: each packet that is dropped and not logged is potential evidence of malicious intent. The principle of logging, a fundamental aspect of accountability, is discussed in detail in Section 9.1.

As with operating systems and other security-enforcing elements, a firewall requires updates. Although more prevalent in software implementations of firewall technology, hardware and router firewalls are capable of updating their firmware. Specific instructions on how to update a firewall are found within the manufacturer documentation. Administrators should check for firewall updates frequently.

7.2.2 Intrusion Detection and Prevention Systems

An intrusion detection system (IDS) is an application that monitors the events occurring in a system or network and analyzes them for signs of potential incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.[43] An intrusion prevention system (IPS) has all the capabilities of an IDS and can also attempt to stop potential

[43] For more information on IDPSs, see NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)* (http://csrc.nist.gov/publications/nistpubs/).

incidents. Because IDS and IPS systems offer many of the same capabilities, they are often collectively called intrusion detection and prevention systems (IDPS). When an IDPS detects a potential incident, it notifies administrators through IDPS console messages, emails, pages, or other mechanisms.

The two types of IDPSs most relevant for email security are host-based and network-based.[44] A host-based IDPS monitors the characteristics of a single host and the events occurring within that host to identify and stop suspicious activity. Host-based IDPS software must be installed on each individual computer that is to be monitored or protected. Host-based IDPSs are very closely integrated with the operating system of the host computer they protect. Thus, a host-based IDPS must be designed specifically for each operating system (and often each version of that operating system). Host-based IDPSs monitor various aspects of hosts, such as network traffic, system logs, running processes, file access and modification, and system and application configuration changes.

Host-based IDPSs are especially useful when most of the network traffic to and from the mail server is encrypted (e.g., SSL/TLS or S/MIME is in use) because the functionality and capability of network-based IDPSs (see below) are severely limited when network traffic is encrypted. Also, because they are located on the server, host-based IDPSs can detect some attacks and penetration attempts not recognized by network-based IDPSs. Unfortunately, host-based IDPSs can have a negative impact on host performance. In general, enabling more extensive detection capabilities and monitoring more events cause a greater negative impact on the performance of the host. Host-based IDPSs may not detect some network-based attacks such as certain DoS attacks. If a host-based IDPS is on a mail server that is compromised, it is very likely that the attacker will also compromise the IDPS itself and vice versa.

A network-based IDPS monitors network traffic for particular network segments or network devices and analyzes the network and application protocol activity to identify and stop suspicious activity. Most network-based IDPSs use predefined "attack signatures" to detect and identify attacks. Attack signatures are patterns that correspond to known types of intrusions. Network-based IDPSs also use other detection methods to identify anomalous activity, protocol violations, and other unusual activity.

Unlike a host-based IDPS, a network-based IDPS can monitor network activity for many hosts simultaneously. Network-based IDPSs can usually detect more network-based attacks and can more easily provide a comprehensive picture of the current attacks against a network. Since network-based IDPSs are installed on dedicated hosts, they do not have a negative effect on the performance of the mail server host and are not immediately compromised by a successful attack on the mail server.

Network-based IDPSs do have some limitations. The timing of an attack can have a significant effect on the ability of a network-based IDPS to detect an attack. For example, if an attacker spreads out the timing of his attack over a period of hours or days, the attack may not be detected by the IDPS. Network configuration, such as the use of asymmetric routing, can have a negative effect on the ability of a network-based IDPS to detect attacks. Network-based IDPSs are also more susceptible to being disabled by DoS attacks (even those not directly targeted at the IDPS). Also, depending on how the network-based IDPS is integrated into the network, it is possible to negatively impact the availability of the network in the event of an IDPS hardware failure.

Most host-based and network-based IDPSs require frequent updates to their attack signature databases so that they can recognize new attacks. An IDPS that is not updated frequently will fail to recognize the latest (and often most popular) attacks. Both types of IDPSs may be limited in their ability to detect zero-

[44] Other major IDPS categories include wireless IDPS, which examines wireless networking protocols only, and network behavior analysis software, which monitors network traffic flows for flow anomalies. Neither of these types of IDPS technologies analyzes email activity.

day attacks because it is unlikely that an appropriate signature is available. A host-based IDPS may have a better chance of detecting a zero-day attack since it is better able to detect the actions taken by an attacker after a successful exploit (e.g., new unauthorized privileged accounts, installation of malicious software).

File integrity checkers are a simple form of host-based IDPS. A file integrity checker computes and stores a hash for every guarded file and establishes a database of file hashes. It provides a tool for system administrators to recognize changes to files, particularly unauthorized changes. File integrity checkers are available both as standalone products and bundled with other host-based IDPS techniques. Some host-based IDPSs can monitor file access attempts and stop suspicious attempts to read, modify, delete, and execute files. A host-based IDPS with this capability could be configured to protect important mail server files.

To successfully protect a mail server using an IDPS, ensure that the IDPS is capable of and configured to:

- Monitor network traffic to and from the mail server
- Monitor changes to critical files on the mail server (file integrity checking capability)[45]
- Monitor the system resources available on the mail server host (host-based)
- Block (in conjunction with the firewall) IP addresses or subnets that are attacking the organizational network
- Notify the necessary parties (e.g., IDPS administrator, mail server administrator, incident response team) of suspected attacks through appropriate means according to the organizational incident response policy and procedures
- Detect as wide a variety of scanning and attacks as possible with an acceptable level of false positives
- Log events, including the following details:
  - Time/date
  - Sensor IP address
  - Manufacturer-specific attack name
  - Standard attack name (if one exists)
  - Source and destination IP addresses
  - Source and destination port numbers
  - Network protocol.
- For network events, packet header information should be captured to assist with the analysis and forensics process
- Update with new attack signatures frequently (e.g., on a daily to weekly basis, typically after testing the updates).

[45] Certain critical files, such as files storing user passwords and log files, will change regularly and thus should not be protected by a file integrity checker. This will vary depending on the mail server and operating system employed.

In addition, it is critical that network-based IDPSs and their underlying operating systems are hardened, as network-based IDPSs are often a target of attackers. In particular, the network-based IDPSs should not respond to any type of system interrogation through their monitoring interfaces. If remote management is desired, it should be conducted through an out-of-band means (e.g., separate isolated network). Although typically difficult to administer and interpret, IDPSs are a critical early warning system that can provide the mail server administrator with the necessary information to defend the mail server from attack. [Scar07]

7.2.3 Network Switches

Network switches are devices that provide connectivity between two or more hosts located on the same network segments. They are similar to hubs in that they allow communications between hosts, but unlike hubs the switches have more "intelligence" and send communications to only those hosts to which the communications are addressed. The benefit of this from a security standpoint is that when switches are employed on a network, it is much more difficult to eavesdrop on communications between other hosts on the network segment. This is extremely important when a mail server is on a network segment that is used by other hosts. For example, if a hub is used and a host on the DMZ is compromised, an attacker may be able to eavesdrop on the communications of other hosts on the DMZ, possibly leading to the compromise of those hosts or the information they communicate across the network. A primary example of this is public Web servers, which are often on the same subnet as mail servers and, if compromised, would be able to sniff unencrypted email traffic and passwords within the DMZ.

Many switches include specific security settings that further enhance the security of the network by making it difficult for a malicious entity to "defeat" the switch. Some examples include the ability to minimize the risk of Address Resolution Protocol (ARP) spoofing and ARP poisoning attacks.[46] If a switch has these security capabilities, they should be enabled (see appropriate manufacturer documentation).

Switches can have a negative impact on network-based IDPSs (see Section 7.2.2). Most network switches allow network administrators to configure a specific port on the switch, known as a span port, so that it replicates all the switch's traffic to the port used by the IDPS. This allows a network-based IDPS to see all traffic on a particular network segment. However, under high loads, the switch might have to stop sending traffic to the span port, causing the IDPS to be unable to monitor network activity. Also, other devices also use span ports, and there are typically very few span ports on a switch, so it might not be possible to connect an IDPS to a particular switch because its span ports are all being used.

[46] ARP poisoning occurs when an attacker successfully updates the ARP cache on a target host with a forged ARP entry. This is generally used to redirect network traffic for malicious purposes.

7.3 Checklist for Implementing a Secure Network Infrastructure

Completed	Action
	Network location
☐	Mail server is located on the internal network and protected by a mail gateway and/or firewall, or Mail server is located in a DMZ
	Firewall configuration
☐	Mail server is protected by a firewall
☐	Mail server, if it faces a higher threat or if it is more vulnerable, is protected by an application layer firewall
☐	Firewall controls all traffic between the Internet and the mail server
☐	Firewall blocks all inbound traffic to the mail server except the necessary ports, such as TCP ports 25 (SMTP), 110 (POP3), 143 (IMAP), 398 (LDAP), 636 (secure LDAP), 993 (secure IMAP), and 995 (secure POP)
☐	Firewall blocks (in conjunction with the intrusion detection or prevention system) IP addresses or subnets that the IDS or IPS reports are attacking the organizational network
☐	Firewall blocks known “blacklisted” networks or subnets, as identified by a trusted external security response center
☐	Firewall notifies the network administrator or mail server administrator of suspicious activity through an appropriate means
☐	Firewall provides content filtering and malware scanning
☐	Firewall is configured to protect against DoS attacks
☐	Firewall logs critical events
☐	Firewall and firewall operating system patched to latest or most secure level
	Intrusion detection and prevention systems
☐	IDPS configured to monitor traffic network traffic to and from the mail server
☐	IDPS configured to monitor changes to critical files on mail server (host-based IDPS or file integrity checker)
☐	IDPS configured to monitor the system resources available on the mail server host (host-based IDPS)
☐	IDPS blocks (in conjunction with the firewall) IP addresses or subnets that are attacking the organizational network
☐	IDPS notifies the necessary parties of suspected attacks through appropriate means according to the organization’s incident response policy and procedures
☐	IDPS configured to maximize detection with an acceptable level of false positives
☐	IDPS configured to log events and to capture packet header information for network events
☐	IDPS updated with new attack signatures frequently (e.g., on a daily to weekly basis, typically after testing the updates)
	Network switches
☐	Network switches are used to protect against network eavesdropping
☐	Network switches are configured in high-security mode to defeat ARP spoofing and ARP poisoning attacks
☐	Network switches are configured to send all traffic on network segment to network-based IDPS

8. Securing Mail Clients

Hundreds to thousands of mail clients access every operational mail server. Regardless of the security in place on mail servers, it is important to secure the client side. In many respects, the client side represents a greater risk to security than the mail server. Numerous issues need to be carefully considered and addressed to provide an appropriate level of security for mail clients. This section provides general recommendations that apply to most mail client applications. Specific recommendations for securing particular applications are not included in this document.

8.1 Installing and Configuring Client Applications

8.1.1 Patching and Updating Mail Clients

The most important step in securing a mail client is to ensure that all users are using the latest and/or most secure version of the mail client with all necessary patches applied.[47] Most major mail clients have had significant vulnerabilities. To identify the vulnerabilities of a particular mail client, see the NIST National Vulnerability Database (NVD) (http://nvd.nist.gov/). The best resource for patches is the appropriate manufacturer's Web site. Appendix E contains a list of mail client manufacturer Web sites.

Updating some mail clients is made slightly more complicated because they operate in conjunction with Web browsers. For example, the close integration and bundling of Microsoft Outlook, a mail client, and Internet Explorer, a Web browser, has allowed the configuration settings and vulnerabilities of the latter to affect the former. In such situations, keeping both the mail client and Web browser updated to secure versions and patch levels is particularly important. Failure to run a secure version of a mail client reduces the effectiveness of the rest of the security measures discussed below.

8.1.2 Configuring Mail Client Security Features

Mail client applications may not be configured securely in their default configurations. Mail clients should be configured to:

- Disable automatic message preview.
- Disable automatic opening of messages.
- Disable automatic loading of pictures in messages.
- Disable downloading and processing of active content. Examples include ActiveX controls, Java applets, and JavaScript. This may cause problems for mail applications that are bundled with Web browsers, because disabling this functionality could affect the Web browser, where such functionality may be required. In those cases, some selective and careful disabling/enabling of active content may be needed. In the case of Microsoft Outlook and Internet Explorer, separate Security Zones could be defined for each, which would allow Internet Explorer to have less restrictive security settings than Outlook.
- Enable anti-spam and anti-phishing features, if available. These features often have rather permissive settings by default, so it may be beneficial from a security perspective to set them to a higher level. Also, users should be educated on reviewing tagged or filtered messages to identify ones that have

[47] When and how to apply patches includes many complex issues that are beyond the scope of this document. For a more detailed discussion of security patches, see NIST SP 800-40 Version 2.0, *Creating a Patch and Vulnerability Management Program* (http://csrc.nist.gov/publications/nistpubs/).

been incorrectly labeled. Some mail clients allow users to configure filtering features such as creating lists of safe senders and senders to block.

There are additional issues specific to portable mail clients, such as those on cell phones and PDAs. The use of portable mail clients has increased significantly in recent years. Users should be made aware that the information that is stored on them is at risk, and that they need to take the necessary precautions in case their devices are lost or stolen. Beyond the obvious physical security measures, users should also reconfigure their devices, which are typically configured insecurely by default. Security features to consider include the following:

- Requiring a password or a PIN to gain access to the device.
- Encrypting locally stored data, including messages and downloaded file attachments.
- Encrypting and/or signing messages, such as supporting S/MIME or OpenPGP and managing digital certificates.
- Encrypting communications between the mail client and the mail server, such as using SSL-based encryption to protect POP, IMAP, and SMTP communications.
- Remotely rendering the device useless or deleting its information if it is compromised.
- Changing the Bluetooth discovery PIN number on Bluetooth devices to prevent unauthorized access.

Organizations should also ensure that their security policy supports the protection of portable mail clients, such as requiring that the devices have anti-virus software enabled on them if available and that wireless functionality be turned off when not being used. Organizations that do not want certain types of devices used to access email should specify the restriction in their security policy.

Many organizations configure mobile devices with VPN access to corporate networks or applications that can connect remotely to servers. As a good security measure, limit access to these applications or remove them if they are not being used. Also, do not store logins, passwords, or personal information on the devices. If the device is stolen, an attacker could potentially use network login information with the VPN to access internal network resources.

8.1.3 Configuring Authentication and Access

Early mail client applications did not require user authentication because mailbox access was restricted by the local file system and the user owned the mailbox file. As MUAs evolved and provided the functionality to access mailboxes remotely via POP and IMAP (see Section 2), user authentication became a requirement. Typically, this was accomplished with users inputting a username and a password when accessing their mailbox. To be more "user-friendly," mail clients incorporated configuration files that contained (e.g., "remembered") usernames and passwords with which to access the mail server. Although this provides ease of use for users, it introduces security weaknesses insofar as a remote or local attacker having logical or physical access to the mail client host may gain access to the authentication information and, in turn, the mailbox contents. In addition, if automatic completion of user input is enabled, a local attacker may be able to use the feature to discover passwords systematically.

Disabling password recall functionality is an effective way to increase mail client security. If the functionality cannot be disabled, then keeping these configuration files secure is important. Most operating systems provide file permission and access control features that offer some means of protection. With hosts that do provide these controls, ensure that the mail client configuration files are restricted for accessibility by only the file owner. Additionally, ensure that the file is located in a directory controlled

by the owner. In cases where a host's file permissions and access controls are unavailable, the best resolution is to remove the user passwords from the configuration files.

Another area to address is the actual communication between the mail client and mail server. As mentioned in Section 2, all network communication with the default configurations of SMTP, POP, and IMAP occurs unencrypted. This makes usernames, passwords, and message content subject to interception and alteration by malicious entities. To increase client to server security, this communication can be encrypted using SSL/TLS. Most commonly used mail clients support SSL/TLS; it should be used if it is available. TLS version 1 is preferred for use; at a minimum, SSL version 3 should be used.[48]

The selection of email addresses and user account names also affects authentication. Using account names in email addresses should be avoided, so that an attacker cannot easily determine a person's account name from the person's email address. Organizations that allow users to select their own email account names should put controls in place to ensure that account names and email addresses are distinct and unrelated. Organizations might also want to place additional restrictions on email addresses, such as having different naming conventions for certain types of users (e.g., contractors, foreign nationals) to allow the user type to be easily recognized. Examples of such naming conventions are *firstname.lastname.countrycode@domain.gov* for a foreign national's address, and *firstname.lastname.ctr@domain.gov* for a contractor's address.

8.1.4 Securing the Client Host's Operating System

Many host operating systems provide a number of configuration settings and other measures for increasing the security of the mail client either directly or indirectly. The host operating system is a key component of the overall security of a client host. The following should be done to secure the host operating system:

- Keep it updated to the most secure patch level.
- Configure it to allow only the appropriate user(s) to access locally stored messages and mail client configuration files.
- Configure (Windows hosts only) the Windows Script Host (WSH) [Pits01]:
  - Remove WSH or allow only the administrator to access
  - Change the default action of the following file extensions from execute to edit:[49]
    - JS (JavaScript)
    - JSE (JavaScript Encoded File)
    - VBE (VBScript Encoded File)
    - VBS (Visual Basic Script)
    - WS (Windows Script File)

---

[48] For more information on TLS and SSL, see NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations* (http://csrc.nist.gov/publications/nistpubs/).

[49] Some email clients may execute files with these extensions, even though the operating system is configured not to execute them.

  - WSC (Windows Script Component)
  - WSF (Windows Script File)
  - WSH (Windows Script Host Settings File)

- On Windows hosts, configure them to display full file extensions (this ensures that an email attachment such as iloveyou.txt.vbs is displayed instead of iloveyou.txt).
- Install an anti-virus application and configure it to automatically scan all incoming messages and any attachments as they are opened.[50] Also, install and use an anti-spyware application if the anti-virus software does not offer robust anti-spyware capabilities. Section 6.2.1 contains a detailed explanation of malware scanning at the client, server, and network layers.
- Install a personal firewall to protect the computer from unauthorized communications, unless the computer is already sufficiently protected by existing network security devices (e.g., network firewalls).
- Ensure that the operating system enforces the concept of least privilege, because malicious code runs in the security context on which it was launched (i.e., the user's access level). For example, users should only read and compose email using accounts without administrator-level privileges.
- Ensure that critical components of the operating system are protected from malicious code.[51]
- Use a file encrypting application to protect the email stored locally on the user's hard drive (this is especially important for laptop computers and other mobile devices, which are more likely to be stolen).
- Configure the operating system to automatically lock the current OS session after a fixed period of inactivity.

8.2 Secure Message Composition

Encryption should be used to securely send email messages containing sensitive information. Two primary methods for encrypting email are S/MIME and OpenPGP, which were discussed in detail in Section 3. Both offer similar levels of protection, but their inherent architectures are different. Most mail clients support S/MIME natively, whereas OpenPGP usually comes in the form of a plug-in. Ultimately, the choice comes down to which solution meets the requirements of the organization.[52] As a general rule, unencrypted email should be treated as a postcard – anyone can read and modify.

Securing messages using S/MIME or OpenPGP involves obtaining digital certificates for both the sender and recipient. A digital certificate has several components, including the name and email address of the person to whom the certificate was issued, a public key and its expiration date, information about the CA that issued the certificate (including its digital signature), and the serial number of the certificate. When the sender has both the sender and receiver's digital certificates, the sender can digitally sign and encrypt email messages to the recipient. Digitally signing a message is important in three ways:

- Authenticity allows the recipient to be confident that the message is from the sender.

---

[50] More information on anti-virus software is available from NIST SP 800-83, *Guide to Malware Incident Prevention and Handling* (http://csrc.nist.gov/publications/nistpubs/).

[51] For more information, see NIST SP 800-28, *Guidelines on Active Content and Mobile Code*, and NIST SP 800-83, *Guide to Malware Incident Prevention and Handling* (http://csrc.nist.gov/publications/nistpubs/).

[52] This includes cryptography requirements, as discussed in Section 3.

- Non-repudiation ensures that the sender cannot deny creating the message.
- Integrity ensures that the message has not accidentally or maliciously been altered during transmission from sender to recipient.

Digital certificates can be obtained from either an internal certificate authority (CA) or a public, third-party CA.[53] Table 3.3 contains a list of third-party CAs.

For a mail client that is configured to send and receive encrypted messages, received messages should be stored in their encrypted format only if they need to continue to be protected; otherwise, it is preferable to allow users to choose which messages should be stored encrypted, if any.[54] The mail client may also be configured to send and receive unencrypted, but authenticated, messages, where integrity is the primary concern. Under normal circumstances, the mail client should be set to require a password once per email session. Requiring a password each time a message is opened for reading can take considerable time and can discourage people from using encryption to protect emails; accordingly, this level of security is typically used only for the highest-security needs.

8.3 Plug-ins

A number of different plug-ins are available for mail clients. These plug-ins offer additional functionality beyond that of the basic mail client configuration. Mail encryption, anti-virus, pop-up blocker, and malware prevention plug-ins are a small subset of the types of plug-ins available. Some provide advanced filtering capabilities, whereas others provide audible notification of new messages. Regardless of the type of plug-in, care needs to be taken when installing them. Generally, only install plug-ins from trusted sources. Be wary of any plug-in that has not been distributed from the manufacturer in a digitally signed archive. Some plug-ins offering additional functionality may contain spyware that can track the Web sites a user visits or adware that delivers pop-up advertisements. They can come in the form of a toolbar that is automatically installed in your Internet browser. Using manufacturers' Web sites to acquire plug-ins reduces the likelihood of installing a malicious plug-in.

8.4 Accessing Web-Based Mail Systems

From a user standpoint, accessing a mail server via a Web browser can be efficient and convenient. Unfortunately, a number of security concerns should be carefully considered before implementing Web-based access to mail servers. Many of the concerns are the same as those for standard mail clients. For example, the default configuration for Web-based access normally sends passwords and data in the clear, such as those for POP and IMAP. For greater security, organizations should configure the mail server to accept Web connections only via 128-bit SSL/TLS connections.[55] This setting causes both user authentication and email content to be encrypted during transmission from the user's Web browser to the Web server. However, it does not protect the content as it is transmitted from the mail server to the recipient(s); some form of email encryption, such as S/MIME or OpenPGP, would need to be used if message confidentiality is required. Unfortunately, most Web-based mail systems do not directly support

---

[53] For more information about CAs, see NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure* (http://csrc.nist.gov/publications/nistpubs/).

[54] In most cases, users can save email attachments unencrypted, print the unencrypted email message text, and perform other actions that leave the email message content unprotected. If such actions are permitted, then requiring the emails to be stored encrypted may create a false sense of protection. Also, it might be difficult or impossible to read the encrypted emails after the current credentials have expired.

[55] For more information on SSL/TLS and its use with Web servers, see NIST SP 800-44, *Guidelines on Securing Public Web Servers*, and NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security Implementations*, (http://csrc.nist.gov/publications/nistpubs/).

them. One solution is to encrypt the data separately and then paste it into the browser for transmission (this is easily done with OpenPGP).

Enabling Web-based access often requires a weakening in the overall security posture of the mail server. Organizations must be aware of the risks and carefully consider whether to implement Web-based access to their mail server (see Section 6.6).

A serious risk with Web-based mail systems is access from public computers (e.g., college computing lab, Internet café, public library). In these situations, the browser may be configured to store and recall usernames and passwords automatically. If it is configured this way, an unauthorized person may use these credentials to obtain access to the organization's mail server. Another danger is that a public computer may have a keystroke logger that registers and saves all keystrokes entered by the mail user, including username and password. Again, this data could be used to access and compromise the organization's mail server. Web browsers also temporarily cache a user's credentials for a fixed period after the user logs in. If the user fails to empty the browser cache and close the browser after completing access to the mail server, it is possible for an unauthorized person to employ the cached credentials to access the organization's mail server. The use of SSL/TLS does not generally protect against these dangers. Web browsers also cache downloaded files and create temporary files that may contain email messages, email attachments, and other information from Web-based mail access. If the Web browser does not clean the cache and temporary files after the session ends, other users of the computer could potentially access these files.

The security of Web-based mail is based in large part on the expertise of users. For example, some Web-based mail applications ask users if they are using public or private computers; users should select the public option to further protect their email information. Thus, users should be made aware of what they should do before being granted access to Web-based mail. Organizations should also consider creating a "Rules of Behavior" agreement that each user signs, in which he or she acknowledges responsibility and accountability for the appropriate use of Web-based mail.

8.5 Checklist for Securing Mail Clients

Completed	Action
	Patch and update mail clients
☐	Update mail client to newest or most secure version
☐	Apply any necessary patches to mail client (in conformance with organizational polices and configuration management)
☐	Apply any necessary patches to Web browser (for mail clients that are integrated with browser)
	Configure mail client security features
☐	Disable automatic message preview
☐	Disable automatic opening of messages
☐	Disable automatic loading of pictures in messages
☐	Disable downloading and processing of active content (if appropriate)
☐	Enable anti-spam and anti-phishing features
☐	Reconfigure portable mail clients, such as those on cell phones and PDAs, to improve their security
☐	Ensure that security policy supports the protection of portable mail clients, such as requiring anti-virus software to be installed and enabled

Completed	Action
☐	Limit access to VPN clients and other remote access applications on mobile devices, or remove the clients/applications if they are not needed
	Configure authentication and access
☐	Enable secure authentication and access
☐	Disable ability of mail client to store username and passwords
☐	Configure client to use encryption (TLS) for SMTP, POP, and IMAP communications
☐	Set restrictions on the selection of email addresses, such as ensuring they are unrelated to user account names
	Secure the mail client host operating system
☐	Keep the OS updated to the most secure patch level
☐	Configure the OS to allow only the appropriate user(s) to access locally stored messages and mail client configuration files
☐	Secure or remove Windows Script Host (Windows hosts only)
☐	Change the default action on files associated with the Windows Script Host from execute to edit (Windows hosts only)
☐	Ensure that the OS is configured to show full file extensions (Windows hosts only)
☐	Install an anti-virus application and configure it to scan incoming messages and attachments; also install an anti-spyware application if the anti-virus software does not offer robust anti-spyware capabilities
☐	Install a personal firewall if needed to protect the computer from unauthorized communications
☐	Ensure the OS enforces the concept of least privilege, because malicious code runs in the security context on which it was launched (i.e., the user's access level)
☐	Ensure that critical components of the operating system are protected from malicious code
☐	Use a file encrypting application to protect the email stored locally on the user's hard drive (especially important for mobile devices)
☐	Configure the OS to automatically lock the current session after a fixed period of inactivity
	Secure message composition
☐	Provide security for email message content (e.g., S/MIME, OpenPGP)
	Use of plug-ins
☐	Enable and install only absolutely necessary plug-ins from trusted sources
	Access to Web-based mail systems
☐	Configure Web-based mail access to only use 128-bit SSL/TLS connections
☐	Make users aware of what they should do before granting them access to Web-based mail

This page has been left blank intentionally.

9. Administering the Mail Server

After initially deploying a mail server, administrators need to maintain its security continuously. This section provides general recommendations for securely administering mail servers. Vital activities include handling and analyzing log files; performing regular mail server backups; recovering from mail server compromises; testing the mail server's security regularly; and performing remote administration securely.

9.1 Logging

Logging is a cornerstone of a sound security posture. Capturing the correct data in the logs and then monitoring those logs closely is vital.[56] Network and system logs are important, especially system logs in the case of S/MIME or OpenPGP (see Section 3) enabled mail servers, where network monitoring is less effective. Mail server software can provide additional log data relevant to mail-specific events.

Reviewing logs is mundane and reactive, and many mail server administrators devote their time to performing duties that they may consider more important or urgent. However, log files are often the only record of suspicious behavior. Enabling the mechanisms to log information allows the logs to be used to detect failed and successful intrusion attempts and to initiate alert notifications when further investigation is needed. Procedures and tools need to be in place to process and analyze the log files and to review alert notifications.

Mail server logs provide:

- Alerts to suspicious activities that require further investigation
- Tracking of an attacker's activities
- Assistance in the recovery of the system
- Assistance in post-event investigation
- Required information for legal proceedings.

The selection and implementation of specific mail server software determine which set of detailed instructions presented below the mail administrator should follow to establish logging configurations. Some of the guidance contained in the steps below may not be fully applicable to all manufacturers' mail server software products.

9.1.1 Recommended Generic Logging Configuration

Although the logging capabilities of a mail server vary for each product, the following generic configuration is recommended. Set logging on the mail server to the standard level used within the organization. Once the overall logging detail level is set, ensure the following events are logged (if supported by the mail server software):

- Local host related logging
  - IP stack setup errors

[56] For more information on logging, see NIST SP 800-92, *Guide to Computer Security Log Management*, which is available at http://csrc.nist.gov/publications/nistpubs/.

  - Resolver configuration problems (e.g., DNS, NIS)
  - Mail server configuration errors (e.g., mismatch with DNS: local configuration error, out of date alias database)
  - Lack of system resources (disk space, memory, CPU)
  - Alias database rebuilds
- Connection-related logging
  - Failed logins, and also successful logins if adequate space is available
  - Security problems (e.g., spamming)
  - Lost communications (network problems)
  - Protocol failures
  - Connection timeouts
  - Connection rejections
  - Use of VRFY and EXPN commands
- Message-related logging
  - Send on behalf of
  - Send as
  - Malformed addresses
  - Message collection statistics
  - Creation of error messages
  - Delivery failures (permanent errors)
  - Messages being deferred (transient errors).

Ensuring that sufficient log capacity is available is a concern, since logs often take considerably more space than administrators initially estimate, especially when logging is set to a highly detailed level. Administrators should closely monitor the size of the log files when they implement different logging settings to ensure that the log files do not fill up the allocated storage. Due to the size of the log files, removing and archiving the logs more frequently or reducing the logging level of detail may be necessary.

Some mail server programs provide a capability to enforce or disable the checking of specified access controls during program startup. This level of control may be helpful, for example, to avoid inadvertent alteration of log files because of errors in file access administration. Mail server administrators should determine the circumstances under which they may wish to enable such checks (assuming the mail server software supports this feature).

9.1.2 Log File Review and Retention

Reviewing log files is a tedious and time-consuming task which informs administrators of events that have already occurred. Accordingly, they are often useful for corroborating other evidence, such as a CPU utilization spike or anomalous network traffic reported by an IPS. When a log is used to corroborate other evidence, a focused review is in order. For example, if an IPS reported an inbound connection to the mail server at 8:17 a.m. that attempted to use the VRFY command, then a review of the logs generated just before 8:17 a.m. is appropriate. Mail server logs should also be reviewed for indications of attacks or spamming. The frequency of the reviews depends on the following factors:

- Amount of traffic the server receives
- General threat level (certain sites receive many more attacks than other sites and thus should review their logs more frequently)
- Specific threats (at certain times specific threats arise that may require more frequent log file analysis)
- Vulnerability of the mail server
- Value of data and services provided by the mail server.

Reviews should take place regularly (e.g., daily) and when a suspicious activity has been noted or a threat warning has been issued. Obviously, the task could quickly become burdensome to a mail administrator. To reduce this burden, automated log analysis tools have been developed (see Section 9.1.3).

In addition, a long-term and more in-depth analysis of the logs is needed. Because a typical mail server attack can involve hundreds of unique requests, an attacker may attempt to disguise a mail attack by increasing the interval between requests. In this case, reviewing a single day's or week's logs may not show recognizable trends. However, when trends are analyzed over a week, month, or quarter, multiple attacks from the same host or subnet can be more easily recognized.

Log files should be protected to ensure that if an attacker does compromise a mail server, the log files cannot be altered to cover the attack. Although encryption can be useful in protecting log files, the best solution is to store log files on a host separate from the mail server. This is often called a centralized logging server. Centralized logging is often performed using syslog, which is a standard logging protocol.[57] Alternately, some organizations use security information and event management (SIEM) software that uses centralized servers to perform log analysis, database servers to store logs, and agents installed on each host to parse particular types of logs, such as mail server logs, and transfer their data to the centralized servers.[58]

Log files should be backed up and archived regularly. Archiving log files for a period of time is important for several reasons, including supporting certain legal actions and troubleshooting problems with the mail server. The retention period for archived log files depends on a number of factors, including:

- Legal requirements
- Organizational requirements

---

[57] Syslog is defined in IETF RFC 3164, *The BSD Syslog Protocol*, which is available at http://www.ietf.org/rfc/rfc3164.txt.

[58] More information on syslog and SIEM implementations is provided in NIST SP 800-92, *Guide to Computer Security Log Management*, which is available at http://csrc.nist.gov/publications/nistpubs/

- Size of logs (which is directly related to the traffic of the site and the number of details logged)
- Value of mail server data and services
- Threat level.

9.1.3 Automated Log File Analysis Tools

Most mail servers receive significant amounts of traffic, and the log files quickly become voluminous. Automated log analysis tools should be installed to ease the burden on the mail server administrator. These tools analyze the entries in the mail server log files and identify suspicious and unusual activity. As mentioned in Section 9.1.2, some organizations use SIEM software for centralized logging, which can also perform automated log file analysis.

Many commercial and public domain tools are available to support regular analysis. The automated log analyzer should forward any suspicious events to the responsible mail administrator or security incident response team as soon as possible for follow-up investigation. Some organizations may wish to use two or more log analyzers to reduce the risk of missing an attack or other significant events in the log files. [Kent06]

9.2 Backing Up Mail Servers

One of the most important functions of a mail server administrator is to maintain the integrity of the data on the mail server. This is important because mail servers are often one of the most exposed and vital servers on an organization's network. The mail administrator needs to perform backups of the mail server on a regular basis for several reasons. For example, a mail server could fail as a result of a malicious or unintentional act or a hardware or software failure. In addition, Federal agencies and many other organizations are governed by regulations on the backup and archiving of mail server data. Mail server data should also be backed up on a regular basis for legal and financial reasons.

All organizations need to create a mail server backup policy. Three main factors influence the contents of this policy:

- Legal requirements
  - Applicable laws and regulations (Federal, state, and international)
  - Litigation requirements
- Mission requirements
  - Contractual
  - Accepted practices
  - Criticality of data to organization
- Organizational guidelines and policies.

Although each organization's mail server backup policy will be different to reflect its particular environment, it should address the following issues:

- The purpose of the mail server backup policy

- The parties affected by the mail server backup policy
- The mail servers covered by the backup policy
- The definitions of key terms, especially legal and technical
- The detailed requirements from the legal, business, and organization's perspective
- The required frequency of backups
- The procedures for ensuring that data is properly retained and protected
- The procedures for ensuring that data is properly destroyed or archived when no longer required
- The procedures for preserving information for Freedom of Information Act (FOIA) requests, legal investigations, and other such requests
- The responsibilities of those involved in data retention, protection, and destruction activities
- The retention period for each type of information logged[59]
- The specific duties of the central/organizational data backup team, if one exists.

Three primary types of backups exist: full, incremental, and differential. Full backups include the operating system, applications, and data stored on the mail server (i.e., an image of every piece of data stored on the mail server hard drives). The advantage of a full backup is that it is easy to restore the entire mail server back to the state (e.g., configuration, patch level, data) it was in when the backup was performed. The disadvantage of full backups is that they take considerable time and resources to perform. Incremental backups reduce the impact by backing up only data that has changed since the previous backup (either full or incremental).

Differential backups reduce the number of backup sets that must be accessed to restore a configuration by backing up all changed data since the last full backup. However, as time lapses from the last full backup, each differential backup becomes increasingly larger, taking more processing time and storage than an incremental backup would. Generally, full backups are performed less frequently (weekly to monthly or when a significant change occurs), and incremental or differential backups are performed more frequently (daily to weekly). Several factors determine the frequency of backups:

- Volatility of information on and configuring of the mail server
- Amount of data to be backed up
- Backup device and media available
- Time available for dumping backup data
- Criticality of data

---

[59] Organizations should carefully consider the retention period for email messages, transaction logs, and other mail server-related records. Many organizations are subject to multiple sets of legal and regulatory requirements that can affect their retention of email records. The National Archives and Records Administration (NARA) has a Web site for Federal records management, which is located at http://www.archives.gov/records-mgmt/. Additional information on NARA regulations related to mail retention is available at http://edocket.access.gpo.gov/2006/pdf/06-1545.pdf. Federal agencies often retain email messages for an extended period of time, such as a year or more, whereas other organizations more commonly retain messages for only 30 to 90 days.

- Threat level faced by the mail server
- Effort required to data reconstruction without data backup
- Other data backup or redundancy features of the mail server (e.g., Redundant Array of Inexpensive Disks [RAID]).

When archiving or backing up email data, organizations should generally conform to the following guidelines:

- Employ write-once, read-many media (to prevent the alteration or accidental erasure of archived information)
- Contain a verification capability to ensure that data is being correctly backed up or archived
- Include the capability to serialize and time-date the information stored
- Provide for easy retrieval of indexes and records preserved on the backup media
- Maintain at least two copies in two geographically distinct locations
- Accurately organize and index all information maintained on both original and duplicate storage media.

9.3 Recovering from a Security Compromise

Most organizations eventually face a successful compromise of one or more hosts on their network. The first step in recovering from a compromise is to create and document the required policies and procedures for responding to successful intrusions *before* an intrusion.[60] The response procedures should outline the actions that are required to respond to a successful compromise of the mail server and the appropriate sequence of these actions (sequence can be critically important). Most organizations already have a dedicated incident response team in place which should be contacted immediately when there is suspicion or confirmation of a compromise. In addition, the organization may wish to ensure that some of its staff are knowledgeable in the fields of computer and network forensics.[61]

A mail server administrator should follow the organization's policies and procedures for incident handling, and the incident response team should be contacted for guidance before taking any action after a suspected or confirmed security compromise. Examples of steps commonly performed after discovering a successful compromise are as follows:

- Report the incident to the organization's computer incident response capability
- Isolate the compromised systems or take other steps to contain the attack so that additional information can be collected[62]
- Consult, as appropriate, with management, legal counsel, and law enforcement expeditiously

---

[60] For more information on this area, see NIST SP 800-61, *Computer Security Incident Handling Guide*, and NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems* (http://csrc.nist.gov/publications/nistpubs/).

[61] More information on computer and network forensics is available from NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response* (http://csrc.nist.gov/publications/nistpubs/).

[62] Isolating the system must be accomplished with great care if the organization wishes to collect evidence. Many attackers configure compromised systems to erase evidence if a compromised system is disconnected from the network or rebooted. One method to isolate a system would be to reconfigure the nearest upstream switch or router.

- Investigate similar[63] hosts to determine if the attacker also has compromised other systems
- Analyze the intrusion, including:
  - Capture the current state of the server starting with the most ephemeral data first (e.g., current network connections, memory dump, files time stamps, logged in users, etc.)
  - Modifications made to the system's software and configuration
  - Modifications made to the data
  - Tools or data left behind by attacker
  - System logs, intrusion detection, and firewall log files
- Restore the system
  - One of the following two options:
    - Install clean version of operating system
    - Restore from backups (this option can be more risky, as the backups may have been made after the compromise, and restoring from a compromised backup may still allow the attacker access to the system)
  - Disable unnecessary services
  - Apply all patches
  - Change all passwords (even on uncompromised hosts as required)
  - Reconfigure network security elements (firewall, router, IPS) to provide additional protection and notification
- Test system to ensure security
- Reconnect system to network
- Monitor system and network for signs that the attacker is attempting to access the system or network again
- Document lessons learned.

System administrators should decide whether to reinstall the operating system of a compromised system or restore it from a backup based on organization policy and procedures. Factors that are often considered include the following:

- Level of access that the attacker gained (e.g., root, user, guest, system)
- Type of attacker (internal or external)

[63] Similar hosts would include hosts that are in the same IP address range, have the same or similar passwords, share a trust relationship, and/or have the same operating system and/or applications.

- Purpose of the compromise (e.g., email spoofing, illegal software repository, platform for other attacks)
- Method used for the system compromise
- Actions of the attacker during and after the compromise (e.g., log files, intrusion detection reports)
- Duration of the compromise
- Extent of the compromise on the network (e.g., the number of hosts compromised)
- Results of consultation with management and legal counsel.

The lower the level of access gained by the attacker and the more the mail server administrator understands about the attacker's actions, the less risk there is in restoring from a backup and patching the vulnerability. For incidents in which there is less known about the attacker's actions and/or in which the attacker gains high-level access, it is recommended that the operating system and applications be reinstalled from the manufacturer's original distribution media and that the mail server data be restored from a known good backup.

If legal action is pursued, system administrators need to be aware of the guidelines for handling a host after a compromise. Consult legal counsel and relevant law enforcement authorities as appropriate.

9.4 Security Testing Mail Servers

Periodic security testing of public mail servers is critical.[64] Without periodic testing, there is no assurance that current protective measures are working or that the security patch just applied by the mail server administrator is functioning as advertised. Although a variety of security testing techniques exists, vulnerability scanning is the most common. Vulnerability scanning assists a mail server administrator in identifying vulnerabilities and verifying whether the existing security measures are effective. Penetration testing is also used, but less frequently and usually only as part of an overall penetration test of the organization's network.[65]

9.4.1 Vulnerability Scanning

Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfiguration of hosts. Many vulnerability scanners also provide information about mitigating discovered vulnerabilities.

Vulnerability scanners attempt to identify vulnerabilities in the hosts scanned. Vulnerability scanners can help identify out-of-date software versions, missing patches or system upgrades, and validate compliance with or deviations from the organization's security policy. To accomplish this effort, vulnerability scanners identify operating systems and major software applications running on hosts and match them with known vulnerabilities. Vulnerability scanners employ large databases of vulnerabilities to identify vulnerabilities associated with commonly used operating systems and applications.

---

[64] If Web-based mail access is being provided, periodic security testing of the Web servers providing that access is also critical. See NIST SP 800-44, *Guidelines on Securing Public Web Servers*, for information on performing security testing for Web servers. It is available at http://csrc.nist.gov/publications/nistpubs/.

[65] For information about vulnerability scanning, penetration testing, and other testing techniques, see NIST SP 800-42, *Guideline on Network Security Testing* (http://csrc.nist.gov/publications/nistpubs/).

However, vulnerability scanners have some significant weaknesses. Generally, they identify only surface vulnerabilities and are unable to address the overall risk level of a scanned mail server. Although the scan process itself is highly automated, vulnerability scanners can have a high false positive error rate (reporting vulnerabilities when none exist). This means an individual with expertise in mail server security and administration must interpret the results. Furthermore, vulnerability scanners cannot generally identify vulnerabilities in custom code or applications.

Vulnerability scanners rely on periodic updating of the vulnerability database to recognize the latest vulnerabilities. Before running any scanner, mail server administrators should install the latest updates to its vulnerability database. Some vulnerability scanner databases are updated more regularly than others (the frequency of updates should be a major consideration when choosing a vulnerability scanner).

Vulnerability scanners are often better at detecting well-known vulnerabilities rather than more esoteric ones because it is impossible for any one scanning product to incorporate all known vulnerabilities in a timely manner. In addition, manufacturers want to keep the speed of their scanners high (more vulnerabilities detected requires more tests, which slows the overall scanning process). Therefore, vulnerability scanners may be of little use to mail server administrators operating less popular mail servers, operating systems, or custom-coded applications.

Vulnerability scanners provide the following capabilities:

- Identifying active hosts on the network
- Identifying active services (ports) on hosts and which of these are vulnerable
- Identifying applications and banner grabbing
- Identifying operating systems
- Identifying vulnerabilities associated with discovered operating systems and applications
- Testing compliance with host application usage/security policies.

Organizations should conduct vulnerability scanning to validate that operating systems and mail server applications are up to date on security patches and software versions. Vulnerability scanning is a labor-intensive activity that requires a high degree of human involvement to interpret the results. It may also be disruptive to operations by taking up network bandwidth, slowing network response times and potentially impacting the availability of the scanned server or its applications. However, vulnerability scanning is extremely important for ensuring that vulnerabilities are mitigated as soon as possible, before they are discovered and exploited by adversaries. Vulnerability scanning should be conducted on a weekly to monthly basis. Many organizations also run a vulnerability scan whenever a new vulnerability database is released for the organization's scanner application. Vulnerability scanning results should be documented and discovered deficiencies corrected.

Organizations should also consider running more than one vulnerability scanner. As previously discussed, no scanner is able to detect all known vulnerabilities; however, using two scanners generally increases the number of vulnerabilities detected. A common practice is to use one commercial and one freeware scanner. Network- and host-based vulnerability scanners are available for free or for a fee.

9.4.2 Penetration Testing

"Penetration testing is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation" [NISS99]. The purpose

of penetration testing is to exercise system protections (particularly human response to attack indications) by using common tools and techniques developed by attackers. This testing is highly recommended for complex or critical systems.

Penetration testing can be an invaluable technique for any organization's information security program. However, it is a very labor-intensive activity and requires great expertise to minimize the risk to targeted systems. At a minimum, it may slow the organization's network response time because of network mapping and vulnerability scanning. Furthermore, the possibility exists that systems may be damaged or rendered inoperable in the course of penetration testing. Although this risk is mitigated by the use of experienced penetration testers, it can never be fully eliminated.

Penetration testing does offer the following benefits [Wack02b]:

- Tests the network using the same methodologies and tools employed by attackers
- Verifies whether vulnerabilities exist
- Goes beyond surface vulnerabilities and demonstrates how these vulnerabilities can be exploited iteratively to gain greater access
- Demonstrates that vulnerabilities are not purely theoretical
- Provides the "realism" necessary to address security issues
- Allows for testing of procedures and the susceptibility of the human element to social engineering.

9.5 Remotely Administering a Mail Server

It is strongly recommended that remote administration of a mail server be allowed only after careful consideration of the risks.[66] The most secure configuration is to disallow any remote administration. However, that may not be viable for all organizations. The risk of enabling remote administration varies considerably depending on the location of the mail server on the network (see Section 7.1). For a mail server that is located behind a firewall, remote administration can be implemented relatively securely from the internal network, but not without added risk. Remote administration should generally not be allowed from a host located outside the organization's network unless performed from an organization-controlled computer through the organization's remote access solution, such as a virtual private network.

If an organization determines that it is necessary to remotely administer a mail server, following these steps should ensure that it is implemented in as secure a manner as possible:

- Use a strong authentication mechanism (e.g., public/private key pair, two factor authentication).
- Restrict which hosts can be used to remotely administer the mail server:
  - Restrict by authorized users
  - Restrict by IP address (not hostname); for example, access could be restricted to some or all hosts on the internal network, or hosts using the organization's enterprise remote access solution

[66] Similar caution is needed for Web servers used for Web-based mail access. See NIST SP 800-44, *Guidelines on Securing Public Web Servers*, for additional information (http://csrc.nist.gov/publications/nistpubs/).

- Use secure protocols that can provide encryption for both passwords and data, such as secure shell [SSH] or Secure HTTP [HTTPS], and not less secure protocols (e.g., Telnet, FTP, NFS, HTTP) unless absolutely required and tunneled over an encrypted protocol such SSH, SSL or IPsec.
- Enforce the concept of least privilege on remote administration (e.g., attempt to minimize the access rights for the remote administration accounts).
- Do not allow remote administration from the Internet through the firewall unless accomplished via strong mechanisms such as VPNs.
- Change any default accounts or passwords from the remote administration utility or application.
- Do not mount any file shares on the internal network from the mail server or vice versa.

9.6 Checklist for Administering the Mail Server

Completed	Action
	Logging
☐	Log IP stack setup errors
☐	Log resolver configuration problems (e.g., DNS, NIS)
☐	Log mail server configuration errors (e.g., mismatch with DNS, local configuration error, out-of-date alias database)
☐	Log lack of system resources (e.g., disk space, memory, CPU)
☐	Log alias database rebuilds
☐	Log logins (failed, and also successful if adequate space is available)
☐	Log security problems (e.g., spamming)
☐	Log lost communications (network problems)
☐	Log protocol failures
☐	Log connection timeouts
☐	Log connection rejections
☐	Log use of VRFY and EXPN commands
☐	Log send on behalf of
☐	Log send as
☐	Log malformed addresses
☐	Log message collection statistics
☐	Log creation of error messages
☐	Log delivery failures (permanent errors)
☐	Log messages being deferred (transient errors)
☐	Store logs on a separate logging server
☐	Backup and archive logs according to organizational requirements
☐	Review logs daily
☐	Review logs weekly (for more long-term trends)
☐	Use automated log file analysis tool(s)
	Mail server backups
☐	Create a mail server backup policy
☐	Back up mail server differentially or incrementally on a daily to weekly basis
☐	Back up mail server fully on a weekly to monthly basis

Completed	Action
☐	Periodically archive backups
	Recovering from a compromise
☐	Report incident to organization's computer incident response capability
☐	Isolate compromised system(s) or take other steps to contain attack so additional evidence can be collected
☐	Consult, as appropriate, with management, legal counsel, and law enforcement expeditiously
☐	Investigate similar hosts to determine if the attacker has also compromised other systems
☐	Analyze the intrusion
☐	Restore the system
☐	Test system to ensure security
☐	Reconnect system to network
☐	Monitor system and network for signs that the attacker is attempting to access the system or network again
☐	Document lessons learned
	Security testing
☐	Periodically conduct vulnerability scans on mail server and supporting network
☐	Update vulnerability scanner before testing
☐	Correct any deficiencies identified by the vulnerability scanner
☐	Conduct penetration testing on the mail server and the supporting network infrastructure
☐	Correct deficiencies identified by penetration testing
	Remote administration
☐	Use a strong authentication mechanism (e.g., public/private key pair, two factor authentication)
☐	Restrict which hosts can be used to remotely administer the mail server by IP address or by authorized users
☐	Use secure protocols (e.g., SSH, HTTPS) that can provide encryption for both passwords and data
☐	Enforce the concept of least privilege on remote administration (e.g., attempt to minimize the access rights for the remote administration accounts)
☐	Change any default accounts or passwords for the remote administration utility or application
☐	Do not allow remote administration from the Internet unless mechanisms such as VPN are used
☐	Do not mount any file shares on the internal network from the mail server and vice versa

Appendix A—Glossary

Address Resolution Protocol (ARP) – A protocol used to obtain a node's physical address. A client station broadcasts an ARP request onto the network with the Internet Protocol (IP) address of the target node it wishes to communicate with, and the node with that address responds by sending back its physical address so that packets can be transmitted to it.

Body – The section of an email message that contains the actual content of the message.

Demilitarized Zone (DMZ) – A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet.

Header – The section of an email message that contains vital information about the message, including origination date, sender, recipient(s), delivery path, subject, and format information. The header is generally left in clear text even when the body of the email message is encrypted.

Internet Message Access Protocol (IMAP) – A mailbox access protocol defined by IETF RFC 3501. IMAP is one of the most commonly used mailbox access protocols. IMAP offers a much wider command set than POP.

Local Delivery Agent (LDA) – A program running on a mail server that delivers messages between a sender and recipient if their mailboxes are both on the same mail server. An LDA may also process the message based on a predefined message filter before delivery.

Mail Server – A host that provides "electronic post office" facilities. It stores incoming mail for distribution to users and forwards outgoing mail. The term may refer to just the application that performs this service, which can reside on a machine with other services, but for this document the term refers to the entire host including the mail server application, the host operating system and the supporting hardware.

Mail Server Administrator – The mail server equivalent of a system administrator. Mail server administrators are system architects responsible for the overall design and implementation of mail servers.

Mail Transfer Agent (MTA) – A program running on a mail server that receives messages from mail user agents or other MTAs and either forwards them to another MTA or, if the recipient is on the MTA, delivers the message to the local delivery agent (LDA) for delivery to the recipient. Common MTAs include Microsoft Exchange and sendmail.

Mail User Agent (MUA) – A mail client application used by an end user to access a mail server to read, compose, and send email messages. Common MUAs include Microsoft Outlook and Mozilla Thunderbird.

Malware – A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

Multipurpose Internet Mail Extensions (MIME) – A protocol that makes use of the headers in an IETF RFC 2822 message to describe the structure of rich message content.

Network Administrator – A person who manages a network within an organization. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily

activity, enforcing licensing agreements, developing a storage management program, and providing for routine backups.

Open Pretty Good Privacy (OpenPGP) – A protocol defined in IETF RFCs 2440 and 3156 for encrypting messages and creating certificates using public key cryptography. Most mail clients do not support OpenPGP by default; instead, third-party plug-ins can be used in conjunction with the mail clients. OpenPGP uses a "web of trust" model for key management, which relies on users for management and control, making it unsuitable for medium to large implementations.

Operating System – The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on, and its principal component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the mail server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations.

Patch – A "repair job" for a piece of programming; also known as a "fix". A patch is the immediate solution to an identified problem that is provided to users; it can sometimes be downloaded from the software maker's Web site. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In many operating systems, a special program is provided to manage and track the installation of patches.

Phishing – Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Post Office Protocol (POP) – A mailbox access protocol defined by IETF RFC 1939. POP is one of the most commonly used mailbox access protocols.

Secure Multipurpose Internet Mail Extensions (S/MIME) – A protocol defined in IETF RFCs 3850 through 3852 and 2634 for encrypting messages and creating certificates using public key cryptography. S/MIME is supported by default installations of many popular mail clients. S/MIME uses a classic, hierarchical design based on certificate authorities for its key management, making it suitable for medium to large implementations.

Simple Mail Transfer Protocol (SMTP) – An MTA protocol defined by IETF RFC 2821. SMTP is the most commonly used MTA protocol.

Spam – Unsolicited bulk commercial email messages.

Spyware – Malware intended to violate a user's privacy.

System Administrator – A person who manages a computer system, including its operating system and applications. Responsibilities are similar to that of a network administrator.

Vulnerability – A security exposure in an operating system or other system software or application software component. A variety of organizations maintain publicly accessible databases of vulnerabilities based on the version numbers of software. Each vulnerability can potentially compromise the system or network if exploited.

Web Server – A computer that provides World Wide Web (WWW) services on the Internet. It includes the hardware, operating system, Web server software, and Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an "intranet server".

This page has been left blank intentionally.

Appendix B—Email-Related RFCs

This appendix contains lists of IETF RFCs that are related to email and email security. The first list contains an extensive list of RFCs, sorted by RFC number. The subsequent lists contain subsets of the first list, focused on particular protocols such as IMAP4, POP, SMTP, and MIME.

Email-Related RFCs by RFC Number

RFC No.	RFC Cat.[67]	RFC Title	URL	Replaced/ Updated
1731	ST	IMAP4 Authentication Mechanisms	http://www.ietf.org/rfc/rfc1731.txt	
1732	IT	IMAP4 Compatibility with IMAP2 and IMAP2BIS	http://www.ietf.org/rfc/rfc1732.txt	
1733	IT	Distributed Electronic Mail Models in IMAP4	http://www.ietf.org/rfc/rfc1733.txt	
1870	STD 10	SMTP Service Extension for Message Size Declaration	http://www.ietf.org/rfc/rfc1870.txt	RFC 1653
1939	STD 53	Post Office Protocol - Version 3	http://www.ietf.org/rfc/rfc1939.txt	RFC 1725
1957	IT	Some Observations on Implementations of the Post Office Protocol (POP3)	http://www.ietf.org/rfc/rfc1957.txt	RFC 1939 (updates)
1985	ST	SMTP Service Extension for Remote Message Queue Starting	http://www.ietf.org/rfc/rfc1985.txt	
1991	IT	PGP Message Exchange Formats	http://www.ietf.org/rfc/rfc1991.txt	
2015	ST	MIME Security with Pretty Good Privacy (PGP)	http://www.ietf.org/rfc/rfc2015.txt	
2034	ST	SMTP Service Extension for Returning Enhanced Error Codes	http://www.ietf.org/rfc/rfc2034.txt	
2045	ST	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies	http://www.ietf.org/rfc/rfc2045.txt	RFC 1521, RFC 1522, RFC 1590
2046	ST	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types	http://www.ietf.org/rfc/rfc2046.txt	RFC 1521, RFC 1522, RFC 1590
2047	ST	MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text	http://www.ietf.org/rfc/rfc2047.txt	RFC 1521, RFC 1522, RFC 1590
2049	ST	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples	http://www.ietf.org/rfc/rfc2049.txt	RFC 1521, RFC 1522, RFC 1590
2061	IT	IMAP4 Compatibility with IMAP2BIS	http://www.ietf.org/rfc/rfc2061.txt	
2062	IT	Internet Message Access Protocol – Obsolete Syntax	http://www.ietf.org/rfc/rfc2062.txt	
2087	ST	IMAP4 QUOTA extension	http://www.ietf.org/rfc/rfc2087.txt	
2088	ST	IMAP4 non-synchronizing literals	http://www.ietf.org/rfc/rfc2088.txt	
2177	ST	IMAP4 IDLE command	http://www.ietf.org/rfc/rfc2177.txt	

[67] Each RFC is in one of four categories: Best Current Practice (BCP), Informational Track (IT), Standards Track (ST), or Standard (STD, followed by the standard number).

RFC No.	RFC Cat.[67]	RFC Title	URL	Replaced/ Updated
2180	IT	IMAP4 Multi-Accessed Mailbox Practice	http://www.ietf.org/rfc/rfc2180.txt	
2192	ST	IMAP URL Scheme	http://www.ietf.org/rfc/rfc2192.txt	
2193	ST	IMAP4 Mailbox Referrals	http://www.ietf.org/rfc/rfc2193.txt	
2195	ST	IMAP/POP AUTHorize Extension for Simple Challenge/Response	http://www.ietf.org/rfc/rfc2195.txt	RFC 2095
2221	ST	IMAP4 Login Referrals	http://www.ietf.org/rfc/rfc2221.txt	
2268	IT	A Description of the RC2 Encryption Algorithm	http://www.ietf.org/rfc/rfc2268.txt	
2311	IT	S/MIME Version 2 Message Specification	http://www.ietf.org/rfc/rfc2311.txt	
2312	IT	S/MIME Version 2 Certificate Handling	http://www.ietf.org/rfc/rfc2312.txt	
2313	IT	PKCS #1: RSA Encryption Version 1.5	http://www.ietf.org/rfc/rfc2313.txt	
2314	IT	PKCS #10: Certification Request Syntax Version 1.5	http://www.ietf.org/rfc/rfc2314.txt	
2315	IT	PKCS #7: Cryptographic Message Syntax Version 1.5	http://www.ietf.org/rfc/rfc2315.txt	
2342	ST	IMAP4 Namespace	http://www.ietf.org/rfc/rfc2342.txt	
2384	ST	POP URL Scheme	http://www.ietf.org/rfc/rfc2384.txt	
2440	ST	OpenPGP Message Format	http://www.ietf.org/rfc/rfc2440.txt	
2442	IT	The Batch SMTP Media Type	http://www.ietf.org/rfc/rfc2442.txt	
2449	ST	POP3 Extension Mechanism	http://www.ietf.org/rfc/rfc2449.txt	RFC 1939 (updates)
2505	BCP	Anti-Spam Recommendations for SMTP MTAs	http://www.ietf.org/rfc/rfc2505.txt	
2554	ST	SMTP Service Extension for Authentication	http://www.ietf.org/rfc/rfc2554.txt	
2595	ST	Using TLS with IMAP, POP3 and ACAP	http://www.ietf.org/rfc/rfc2595.txt	
2630	ST	Cryptographic Message Syntax	http://www.ietf.org/rfc/rfc2630.txt	
2632	ST	S/MIME Version 3 Certificate Handling	http://www.ietf.org/rfc/rfc2632.txt	
2633	ST	S/MIME Version 3 Message Specification	http://www.ietf.org/rfc/rfc2633.txt	
2634	ST	Enhanced Security Services for S/MIME	http://www.ietf.org/rfc/rfc2634.txt	
2645	ST	On-Demand Mail Relay (ODMR) SMTP with Dynamic IP Addresses	http://www.ietf.org/rfc/rfc2645.txt	
2683	IT	IMAP4 Implementation Recommendations	http://www.ietf.org/rfc/rfc2683.txt	
2821	ST	Simple Mail Transfer Protocol	http://www.ietf.org/rfc/rfc2821.txt	RFC 821, RFC 974, RFC 1869, RFC 1123 (updates)
2822	ST	Internet Message Format	http://www.ietf.org/rfc/rfc2822.txt	RFC 822
2846	ST	GSTN Address Element Extensions in E-mail Services	http://www.ietf.org/rfc/rfc2846.txt	
2852	ST	Deliver By SMTP Service Extension	http://www.ietf.org/rfc/rfc2852.txt	RFC 1894 (updates)
2920	STD 60	SMTP Service Extension for Command Pipelining	http://www.ietf.org/rfc/rfc2920.txt	RFC 2197
2971	ST	IMAP4 ID extension	http://www.ietf.org/rfc/rfc2971.txt	

RFC No.	RFC Cat.[67]	RFC Title	URL	Replaced/ Updated
3030	ST	SMTP Service Extensions for Transmission of Large and Binary MIME Messages	http://www.ietf.org/rfc/rfc3030.txt	RFC 1830
3156	ST	MIME Security with OpenPGP	http://www.ietf.org/rfc/rfc3156.txt	RFC 2015 (updates)
3191	ST	Minimal GSTN address format in Internet Mail	http://www.ietf.org/rfc/rfc3191.txt	RFC 2303, RFC 2846 (updates)
3192	ST	Minimal FAX address format in Internet Mail	http://www.ietf.org/rfc/rfc3192.txt	RFC 2304, RFC 2846 (updates)
3206	ST	The SYS and AUTH POP Response Codes	http://www.ietf.org/rfc/rfc3206.txt	
3207	ST	SMTP Service Extension for Secure SMTP over Transport Layer Security	http://www.ietf.org/rfc/rfc3207.txt	RFC 2487
3348	IT	The Internet Message Action Protocol (IMAP4) Child Mailbox Extension	http://www.ietf.org/rfc/rfc3348.txt	
3461	ST	Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)	http://www.ietf.org/rfc/rfc3461.txt	RFC 1891
3462	ST	The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages	http://www.ietf.org/rfc/rfc3462.txt	RFC 1892
3463	ST	Enhanced Mail System Status Codes	http://www.ietf.org/rfc/rfc3463.txt	RFC 1893
3464	ST	An Extensible Message Format for Delivery Status Notifications	http://www.ietf.org/rfc/rfc3464.txt	RFC 1894
3501	ST	Internet Message Access Protocol - Version 4rev1	http://www.ietf.org/rfc/rfc3501.txt	RFC 2060
3502	ST	Internet Message Access Protocol (IMAP) – MULTIAPPEND Extension	http://www.ietf.org/rfc/rfc3502.txt	
3503	ST	Message Disposition Notification (MDN) profile for Internet Message Access Protocol (IMAP)	http://www.ietf.org/rfc/rfc3503.txt	
3516	ST	IMAP4 Binary Content Extension	http://www.ietf.org/rfc/rfc3516.txt	
3691	ST	Internet Message Access Protocol (IMAP) UNSELECT command	http://www.ietf.org/rfc/rfc3691.txt	
3798	ST	Message Disposition Notification	http://www.ietf.org/rfc/rfc3798.txt	RFC 2298, RFC 2046 (updates), RFC 3461 (updates)
3848	ST	ESMTP and LMTP Transmission Types Registration	http://www.ietf.org/rfc/rfc3848.txt	
3865	ST	A No Soliciting Simple Mail Transfer Protocol (SMTP) Service Extension	http://www.ietf.org/rfc/rfc3865.txt	
3885	ST	SMTP Service Extension for Message Tracking	http://www.ietf.org/rfc/rfc3885.txt	RFC 3461 (updates)
3886	ST	An Extensible Message Format for Message Tracking Responses	http://www.ietf.org/rfc/rfc3886.txt	RFC 3463 (updates)
3974	IT	SMTP Operational Experience in Mixed IPv4/v6 Environments	http://www.ietf.org/rfc/rfc3974.txt	

RFC No.	RFC Cat.[67]	RFC Title	URL	Replaced/ Updated
4141	ST	SMTP and MIME Extensions for Content Conversion	http://www.ietf.org/rfc/rfc4141.txt	
4289	BCP	Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures	http://www.ietf.org/rfc/rfc4289.txt	RFC 2048
4314	ST	IMAP4 Access Control List (ACL) Extension	http://www.ietf.org/rfc/rfc4314.txt	RFC 2086
4315	ST	Internet Message Access Protocol (IMAP) - UIDPLUS extension	http://www.ietf.org/rfc/rfc4315.txt	RFC 2359

IMAP-Related RFCs by RFC Number

RFC No.	RFC Cat.	RFC Title	URL	Replaced/ Updated
1731	ST	IMAP4 Authentication Mechanisms	http://www.ietf.org/rfc/rfc1731.txt	
1732	ST	IMAP4 Compatibility with IMAP2 and IMAP2BIS	http://www.ietf.org/rfc/rfc1732.txt	
1733	IT	Distributed Electronic Mail Models in IMAP4	http://www.ietf.org/rfc/rfc1733.txt	
2061	IT	IMAP4 Compatibility with IMAP2BIS	http://www.ietf.org/rfc/rfc2061.txt	
2062	IT	Internet Message Access Protocol – Obsolete Syntax	http://www.ietf.org/rfc/rfc2062.txt	
2087	ST	IMAP4 QUOTA extension	http://www.ietf.org/rfc/rfc2087.txt	
2088	ST	IMAP4 non-synchronizing literals	http://www.ietf.org/rfc/rfc2088.txt	
2177	ST	IMAP4 IDLE command	http://www.ietf.org/rfc/rfc2177.txt	
2180	IT	IMAP4 Multi-Accessed Mailbox Practice	http://www.ietf.org/rfc/rfc2180.txt	
2192	ST	IMAP URL Scheme	http://www.ietf.org/rfc/rfc2192.txt	
2193	ST	IMAP4 Mailbox Referrals	http://www.ietf.org/rfc/rfc2193.txt	
2195	ST	IMAP/POP AUTHorize Extension for Simple Challenge/Response	http://www.ietf.org/rfc/rfc2195.txt	RFC 2095
2221	ST	IMAP4 Login Referrals	http://www.ietf.org/rfc/rfc2221.txt	
2342	ST	IMAP4 Namespace	http://www.ietf.org/rfc/rfc2342.txt	
2595	ST	Using TLS with IMAP, POP3 and ACAP	http://www.ietf.org/rfc/rfc2595.txt	
2683	IT	IMAP4 Implementation Recommendations	http://www.ietf.org/rfc/rfc2683.txt	
2971	ST	IMAP4 ID extension	http://www.ietf.org/rfc/rfc2971.txt	
3348	IT	The Internet Message Action Protocol (IMAP4) Child Mailbox Extension	http://www.ietf.org/rfc/rfc3348.txt	
3501	ST	Internet Message Access Protocol - Version 4rev1	http://www.ietf.org/rfc/rfc3501.txt	RFC 2060
3502	ST	Internet Message Access Protocol (IMAP) – MULTIAPPEND Extension	http://www.ietf.org/rfc/rfc3502.txt	
3503	ST	Message Disposition Notification (MDN) profile for Internet Message Access Protocol (IMAP)	http://www.ietf.org/rfc/rfc3503.txt	
3516	ST	IMAP4 Binary Content Extension	http://www.ietf.org/rfc/rfc3516.txt	
3691	ST	Internet Message Access Protocol (IMAP) UNSELECT command	http://www.ietf.org/rfc/rfc3691.txt	
4314	ST	IMAP4 Access Control List (ACL) Extension	http://www.ietf.org/rfc/rfc4314.txt	RFC 2086

RFC No.	RFC Cat.	RFC Title	URL	Replaced/ Updated
4315	ST	Internet Message Access Protocol (IMAP) - UIDPLUS extension	http://www.ietf.org/rfc/rfc4315.txt	RFC 2359

MIME and S/MIME RFCs by RFC Number

RFC No.	RFC Cat.	RFC Title	URL	Replaced/ Updated
2015	ST	MIME Security with Pretty Good Privacy (PGP)	http://www.ietf.org/rfc/rfc2015.txt	
2045	ST	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies	http://www.ietf.org/rfc/rfc2045.txt	RFC 1521, RFC 1522, RFC 1590
2046	ST	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types	http://www.ietf.org/rfc/rfc2046.txt	RFC 1521, RFC 1522, RFC 1590
2047	ST	MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text	http://www.ietf.org/rfc/rfc2047.txt	RFC 1521, RFC 1522, RFC 1590
2049	ST	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples	http://www.ietf.org/rfc/rfc2049.txt	RFC 1521, RFC 1522, RFC 1590
2268	IT	A Description of the RC2 Encryption Algorithm	http://www.ietf.org/rfc/rfc2268.txt	
2311	IT	S/MIME Version 2 Message Specification	http://www.ietf.org/rfc/rfc2311.txt	
2312	IT	S/MIME Version 2 Certificate Handling	http://www.ietf.org/rfc/rfc2312.txt	
2313	IT	PKCS #1: RSA Encryption Version 1.5	http://www.ietf.org/rfc/rfc2313.txt	
2314	IT	PKCS #10: Certification Request Syntax Version 1.5	http://www.ietf.org/rfc/rfc2314.txt	
2315	IT	PKCS #7: Cryptographic Message Syntax Version 1.5	http://www.ietf.org/rfc/rfc2315.txt	
2630	ST	Cryptographic Message Syntax	http://www.ietf.org/rfc/rfc2630.txt	
2632	ST	S/MIME Version 3 Certificate Handling	http://www.ietf.org/rfc/rfc2632.txt	
2633	ST	S/MIME Version 3 Message Specification	http://www.ietf.org/rfc/rfc2633.txt	
2634	ST	Enhanced Security Services for S/MIME	http://www.ietf.org/rfc/rfc2634.txt	
3156	ST	MIME Security with OpenPGP	http://www.ietf.org/rfc/rfc3156.txt	RFC 2015 (updates)
4141	ST	SMTP and MIME Extensions for Content Conversion	http://www.ietf.org/rfc/rfc4141.txt	
4289	BCP	Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures	http://www.ietf.org/rfc/rfc4289.txt	RFC 2048

OpenPGP and PGP-Related RFCs by RFC Number

RFC No.	RFC Cat.	RFC Title	URL	Replaced/ Updated
1991	IT	PGP Message Exchange Formats	http://www.ietf.org/rfc/rfc1991.txt	
2015	ST	MIME Security with Pretty Good Privacy (PGP)	http://www.ietf.org/rfc/rfc2015.txt	
2440	ST	OpenPGP Message Format	http://www.ietf.org/rfc/rfc2440.txt	
3156	ST	MIME Security with OpenPGP	http://www.ietf.org/rfc/rfc3156.txt	RFC 2015 (updates)

POP-Related RFCs by RFC Number

RFC No.	RFC Cat.	RFC Title	URL	Replaced/ Updated
1939	STD 53	Post Office Protocol - Version 3	http://www.ietf.org/rfc/rfc1939.txt	RFC 1725
1957	IT	Some Observations on Implementations of the Post Office Protocol (POP3)	http://www.ietf.org/rfc/rfc1957.txt	RFC 1939 (updates)
2195	ST	IMAP/POP AUTHorize Extension for Simple Challenge/Response	http://www.ietf.org/rfc/rfc2195.txt	RFC 2095
2384	ST	POP URL Scheme	http://www.ietf.org/rfc/rfc2384.txt	
2449	ST	POP3 Extension Mechanism	http://www.ietf.org/rfc/rfc2449.txt	RFC 1939 (updates)
2595	ST	Using TLS with IMAP, POP3 and ACAP	http://www.ietf.org/rfc/rfc2595.txt	
3206	ST	The SYS and AUTH POP Response Codes	http://www.ietf.org/rfc/rfc3206.txt	

SMTP-Related RFCs by RFC Number

RFC No.	RFC Cat.	RFC Title	URL	Replaced/ Updated
1870	STD 10	SMTP Service Extension for Message Size Declaration	http://www.ietf.org/rfc/rfc1870.txt	RFC 1653
1985	ST	SMTP Service Extension for Remote Message Queue Starting	http://www.ietf.org/rfc/rfc1985.txt	
2034	ST	SMTP Service Extension for Returning Enhanced Error Codes	http://www.ietf.org/rfc/rfc2034.txt	
2442	IT	The Batch SMTP Media Type	http://www.ietf.org/rfc/rfc2442.txt	
2505	BCP	Anti-Spam Recommendations for SMTP MTAs	http://www.ietf.org/rfc/rfc2505.txt	
2554	ST	SMTP Service Extension for Authentication	http://www.ietf.org/rfc/rfc2554.txt	
2645	ST	On-Demand Mail Relay (ODMR) SMTP with Dynamic IP Addresses	http://www.ietf.org/rfc/rfc2645.txt	
2821	ST	Simple Mail Transfer Protocol	http://www.ietf.org/rfc/rfc2821.txt	RFC 821, RFC 974, RFC 1869, RFC 1123 (updates)

RFC No.	RFC Cat.	RFC Title	URL	Replaced/ Updated
2822	ST	Internet Message Format	http://www.ietf.org/rfc/rfc2822.txt	RFC 822
2846	ST	GSTN Address Element Extensions in E-mail Services	http://www.ietf.org/rfc/rfc2846.txt	
2852	ST	Deliver By SMTP Service Extension	http://www.ietf.org/rfc/rfc2852.txt	RFC 1894 (updates)
2920	STD 60	SMTP Service Extension for Command Pipelining	http://www.ietf.org/rfc/rfc2920.txt	RFC 2197
3030	ST	SMTP Service Extensions for Transmission of Large and Binary MIME Messages	http://www.ietf.org/rfc/rfc3030.txt	RFC 1830
3207	ST	SMTP Service Extension for Secure SMTP over Transport Layer Security	http://www.ietf.org/rfc/rfc3207.txt	RFC 2487
3461	ST	Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)	http://www.ietf.org/rfc/rfc3461.txt	RFC 1891
3462	ST	The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages	http://www.ietf.org/rfc/rfc3462.txt	RFC 1892
3463	ST	Enhanced Mail System Status Codes	http://www.ietf.org/rfc/rfc3463.txt	RFC 1893
3464	ST	An Extensible Message Format for Delivery Status Notifications	http://www.ietf.org/rfc/rfc3464.txt	RFC 1894
3798	ST	Message Disposition Notification	http://www.ietf.org/rfc/rfc3798.txt	RFC 2298, RFC 2046 (updates), RFC 3461 (updates)
3848	ST	ESMTP and LMTP Transmission Types Registration	http://www.ietf.org/rfc/rfc3848.txt	
3865	ST	A No Soliciting Simple Mail Transfer Protocol (SMTP) Service Extension	http://www.ietf.org/rfc/rfc3865.txt	
3885	ST	SMTP Service Extension for Message Tracking	http://www.ietf.org/rfc/rfc3885.txt	RFC 3461 (updates)
3886	ST	An Extensible Message Format for Message Tracking Responses	http://www.ietf.org/rfc/rfc3886.txt	RFC 3463 (updates)
3974	IT	SMTP Operational Experience in Mixed IPv4/v6 Environments	http://www.ietf.org/rfc/rfc3974.txt	
4141	ST	SMTP and MIME Extensions for Content Conversion	http://www.ietf.org/rfc/rfc4141.txt	

This page has been left blank intentionally.

Appendix C—References

[Alle00] Julia Allen, et al., *Securing Network Servers*, CERT, 2000, http://www.sei.cmu.edu/pub/documents/sims/pdf/sim010.pdf

[Curt01] Matt Curtin, *Developing Trust: Online Privacy and Security*, November 2001

[FTC06a] Federal Trade Commission, *How Not to Get Hooked by a 'Phishing' Scam*, October 2006, http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm

[Kent06] Karen Kent and Murugiah Souppaya, NIST Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006, http://csrc.nist.gov/publications/nistpubs/

[McKi01] Ashley McKinnon, "Web and Email Filtering", *PC Magazine*, December 2001

[Mell05] Peter Mell, et al., NIST Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005, http://csrc.nist.gov/publications/nistpubs/

[NISS99] *National Information System Security Glossary*, NSTISSI No. 4009, January 1999

[Pits01] Trent Pitsenbarger, *Email Security in the Wake of Recent Malicious Code Incidents*, 2001, http://www.nsa.gov/snac/

[Salt75] Jerome H. Saltzer and Michael Schroeder, "The Protection of Information in Computer Systems," *Proceedings of the IEEE*, Volume 63, pages 1278-1308

[Scar07] Karen Scarfone and Peter Mell, NIST Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007, http://csrc.nist.gov/publications/nistpubs/

[Swan06] Marianne Swanson, et al, NIST Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006, http://csrc.nist.gov/publications/nistpubs/

[Wack02a] John Wack, et al., NIST Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002, http://csrc.nist.gov/publications/nistpubs/

[Wack02b] John Wack, et al., NIST Special Publication 800-42, *Guideline on Network Security Testing*, February 2002, http://csrc.nist.gov/publications/nistpubs/

This page has been left blank intentionally.

Appendix D—Email Security Tools and Applications

The lists below provide examples of tools and resources that may be helpful.[68]

Centralized Malware Scanning and Content Filtering Applications

Manufac-turer	Tools	Web Site	Linux/Unix	Win32	Cost
Aladdin Knowledge Systems	**eSafe Gateway, eSafe Mail**	http://www.aladdin.com/esafe/email_security.asp		✓	$$$
Description	*Supports Microsoft Exchange, IBM Lotus Domino, and SMTP-based mail servers.*				
Barracuda Networks	**Barracuda Spam Firewall**	http://www.barracudanetworks.com/ns/products/spam_overview.php			$$$
Description	*Appliance-based solutions for monitoring email messages in transit; separate from mail servers.*				
BorderWare Technologies	**MXtreme Mail Firewall**	http://www.borderware.com/products/mxtreme/			$$$
Description	*Appliance-based solutions for monitoring email messages in transit; separate from mail servers.*				
CipherTrust	**CipherTrust Edge, CipherTrust IronMail**	http://www.ciphertrust.com/products/index.php			$$$
Description	*Appliance-based solutions for monitoring email messages in transit; separate from mail servers.*				
Clearswift	**MIMEsweeper**	http://www.mimesweeper.com/		✓	$$$
Description	*Supports Microsoft Exchange, IBM Lotus Domino, and SMTP-based mail servers.*				
F-Secure	**F-Secure Anti-Virus, F-Secure Internet Gatekeeper, F-Secure Messaging Security Gateway, F-Secure Spam Control,**	http://www.f-secure.com/products/products_a-z.html	✓	✓	$$$
Description	*Supports Microsoft Exchange, SMTP, and POP3.*				
GFI Software	**GFI MailEssentials, GFI MailSecurity**	http://www.gfi.com/mailsecurity/		✓	$$$
Description	*Supports Microsoft Exchange and SMTP-based mail servers.*				
GROUP Technologies	**iQ Suite**	http://www.group-software.com/en/products/iq_suite/iq_suite.php	✓	✓	$$$
Description	*Supports Microsoft Exchange, Microsoft ISA, IBM Lotus Domino, and Microsoft SMTP-based mail servers.*				
IronPort Systems	**IronPort**	http://www.ironport.com/products/			$$$
Description	*Appliance-based solutions for monitoring email messages in transit; separate from mail servers.*				

[68] The applications referenced in this appendix are by no means a complete list of applications to use for email security purposes, nor does this publication imply any endorsement of certain products.

Manufac-turer	Tools	Web Site	Linux/Unix	Win32	Cost
Kaspersky Lab	**Kaspersky Anti-Spam, Kaspersky Anti-Virus, Kaspersky SMTP-Gateway**	http://usa.kaspersky.com/products/corporate-security.php	✓	✓	$$$
Description	*Supports Microsoft Exchange, IBM Lotus Domino, and SMTP-based mail servers (including Sendmail, qmail, Postfix, CommuniGate Pro, and Exim).*				
MailScanner/Julian Field	**MailScanner**	http://www.mailscanner.info/	✓		Free
Description	*Typically used with SpamAssassin and ClamAV; supports various SMTP-based mail servers (including Postfix, Exim, and ZMailer)*				
Marshal	**MailMarshal**	http://www.marshal.com/pages/products.asp		✓	$$$
Description	*Supports Microsoft Exchange and SMTP servers.*				
McAfee	**McAfee GroupShield, McAfee Secure Messaging, McAfee SpamKiller**	http://www.mcafee.com/us/enterprise/products/anti_virus/email_servers/index.html	✓	✓	$$$
Description	*Supports Microsoft Exchange, IBM Lotus Domino, and SMTP-based mail servers.*				
Mirapoint	**RazorGate**	http://www.mirapoint.com/products/			$$$
Description	*Appliance-based solutions for monitoring email messages in transit; separate from mail servers.*				
Panda Antivirus	**EnterpriSecure**	http://www.pandasoftware.com/home/empresas/default	✓	✓	$$$
Description	*Supports Microsoft Exchange, IBM Lotus Domino, and SMTP-based mail servers (including Sendmail, Qmail, and Postfix).*				
Proofpoint	**Proofpoint Messaging Security Gateway, Proofpoint Protection Server**	http://www.proofpoint.com/products/index.php	✓		$$$
Description	*Supports SMTP-based mail servers.*				
Sendmail	**Sendmail Mailstream, Sendmail Sentrion**	http://www.sendmail.com/products/	✓	✓	$$$
Description	*Supports SMTP-based mail servers.*				
SonicWALL	**SonicWALL Email Security**	http://www.sonicwall.com/us/Email_Security.html		✓	$$$
Description	*Supports Microsoft Exchange and SMTP-based mail servers.*				
Sophos	**Sophos ES4000 Email Security Appliance, Sophos MailMonitor, Sophos PureMessage**	http://www.sophos.com/products/es/gateway/	✓	✓	$$$
Description	*Supports Microsoft Exchange, IBM Lotus Domino, and SMTP-based mail servers (including Sendmail, Postfix, Sun Java System Messaging Server, and SunOne Messaging Server).*				
SurfControl	**SurfControl E-mail Filter, SurfControl RiskFilter**	http://www.surfcontrol.com/		✓	$$$

Manufac-turer	Tools	Web Site	Linux/Unix	Win32	Cost
Description	*Supports Microsoft Exchange, IBM Lotus Domino, GroupWise, Sendmail, and other SMTP-based mail servers.*				
Symantec	**Symantec AntiVirus, Symantec Mail Security**	http://www.symantec.com/enterprise/products/index.jsp	✓	✓	$$$
Description	*Supports Microsoft Exchange, IBM Lotus Domino, and SMTP-based mail servers.*				
Trend Micro	**ScanMail**	http://www.trendmicro.com/en/products/email/overview.htm	✓	✓	$$$
Description	*Supports Microsoft Exchange and IBM Lotus Domino.*				
Tumbleweed Communications	**MailGate**	http://www.tumbleweed.com/products/mailgate/index.html		✓	$$$
Description	*Supports Microsoft Exchange and SMTP-based mail servers.*				

$$$=This product involves a fee.

Open Relay Tools

Tool	Capabilities	Web Site	Web-Based	Cost
Mail Relay Testing Tools				
DNSExit Mail Relay Testing Tool	**Mail Relay Tool**	https://www.dnsexit.com/Direct.sv?cmd=testMailServer	✓	Free
Description	*Attempts to Telnet into a mail server at a specified SMTP port and deliver a message to that server. It will detect whether or not the mail server is configured correctly.*			
Mail Relay Testing Tool	**Mail Relay Tool**	http://abuse.net/relay.html	✓	Free
Description	*Assists administrators in identifying mail relays.*			
Spam Relay Checker	**Spam Relay Tool**	http://www.3dmail.com/spam/	✓	Free
Description	*Assists system administrators to trace spam sources in hopes of tracking from where the spam is being generated. It will assist in the notification to the Postmaster of the server that it is being misused by spammers.*			
Blacklists[69]				
Composite Blocking List (CBL)	**Blacklist**	http://cbl.abuseat.org/	✓	Free
Description	*The CBL takes its source data from very large spam traps, and only lists IPs exhibiting characteristics which are specific to open proxies of various sorts (HTTP, socks, AnalogX, wingate, etc.) which have been abused to send spam, worms and viruses that do their own direct mail transmission, or some types of Trojan horse or "stealth" spamware, without doing open proxy tests of any kind.*			

[69] For additional blacklist resources, see http://dmoz.org/Computers/Internet/Abuse/Spam/Blacklists/.

Tool	Capabilities	Web Site	Web-Based	Cost
Distributed Server Boycott List (DSBL)	**Blacklist**	http://dsbl.org/main	✓	Free
Description	*The DSBL lists contain the IP addresses of servers which have relayed special test messages to listme@listme.dsbl.org; this can happen if the server is an open relay, an open proxy, or has another vulnerability that allows anybody to deliver email to anywhere through that server.*			
NJABL.ORG	**Blacklist**	http://njabl.org/	✓	Free
Description	*NJABL.ORG maintains a list of known and potential spam sources (open relays, open proxies, open form to mail HTTP gateways, dynamic IP pools, and direct spammers) for the purpose of being able to tag or refuse email and prevent at least some spam.*			
The Spamhaus Block List (SBL)	**Blacklist**	http://www.spamhaus.org/sbl/	✓	Free
Description	*The SBL is a real-time database of IP addresses of verified spam sources (including spammers, spam gangs, and spam support services), maintained by the Spamhaus Project team and supplied as a free service to help mail administrators better manage incoming email streams.*			
MX Record Lookup				
DNS MX record lookup	**MX Record Lookup**	http://airlinknetworks.com/exchange/MXrecordLookup.html	✓	Free
Description	*This tool allows for lookup of a domain's MX servers.*			
Domain Mail Server/ Exchanger (MX Records) Lookup	**MX Record Lookup**	http://www.hashemian.com/tools/domain-email.php	✓	Free
Description	*This tool attempts to identify the mail servers used by a specified email address. This can be useful to check an email's authenticity, or check who handles email for a certain address.*			
MX Record Lookup	**MX Record Lookup**	http://www.webmaster-toolkit.com/mx-record-lookup.shtml	✓	Free
Description	*The MX Record Lookup tool attempts to find out the mail servers used by a specified email address. This can be useful to check an email's authenticity, or check who handles email for a certain address.*			

Appendix E—Online Email Security Resources

This appendix contains lists of online resources that may be helpful to mail server administrators and others in achieving a greater understanding of email security and in securing their mail servers, clients, and other mail system components.

General Security Resources

Resource/Title	URL
Center for Education and Research in Information Assurance and Security (CERIAS)	http://www.cerias.purdue.edu/
CERT/CC	http://www.cert.org/
Computer Security Resource Center (CSRC)	http://csrc.nist.gov/
National Information Assurance Partnership (NIAP)	http://www.niap.nist.gov/
National Vulnerability Database (NVD)	http://nvd.nist.gov/
Office of Management and Budget Circular No. A-130	http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
Open Source Vulnerability Database (OSVDB)	http://www.osvdb.org/
RISKS Forum	http://catless.ncl.ac.uk/Risks/
Security Configuration Checklists Program for IT Products	http://checklists.nist.gov/
SecurityFocus Vulnerability Database	http://www.securityfocus.com/vulnerabilities
U.S. Computer Emergency Response Team (US-CERT)	http://www.us-cert.gov/
U.S. Department of Energy Computer Incident Advisory Capability (CIAC)	http://www.ciac.org/ciac/

General Email and Email Security Resources

Resource/Title	URL
Email Issues, SANS Reading Room	http://www.sans.org/rr/whitepapers/email/
Internet Mail Consortium	http://www.imc.org/
Tips and Tricks Guide to Secure Messaging	http://www.microsoft.com/securemessaging/ebook/default.mspx

Email Encryption Resources

Resource/Title	URL
Guide to Using S/MIME	http://www.mozilla.org/projects/security/pki/psm/smime_guide.html
IETF OpenPGP Working Group	http://www.ietf.org/html.charters/openpgp-charter.html
IETF S/MIME Working Group	http://www.ietf.org/html.charters/smime-charter.html
OpenPGP Alliance	http://www.openpgp.org/
S/MIME Gateway Certification	http://www.opengroup.org/smg/cert/
Securing Email Through Proxies: Smap and Stunnel	http://www.sans.org/reading_room/whitepapers/email/579.php
Securing POP Mail on Windows Clients	http://sewpsc.sewp.nasa.gov/documents/pop.mail.pdf
Securing POP Mail on Windows Clients	http://csrc.nist.gov/fasp/FASPDocs/SecurPOPwSSH.htm

Malware and Spyware Resources

Resource/Title	URL
Anti-Spyware Coalition (ASC)	http://www.antispywarecoalition.org/
Anti-Virus Information Exchange Network (AVIEN)	http://www.avien.org/
Common Malware Enumeration (CME)	http://cme.mitre.org/
Computer Antivirus Research Organization (CARO)	http://www.caro.org/
European Institute for Computer Antivirus Research (EICAR)	http://www.eicar.org/
SecurityFocus Virus	http://www.securityfocus.com/virus/
Spywaredata.com	http://www.spywaredata.com/
Virus Bulletin	http://www.virusbtn.com/
Viruslist.com	http://www.viruslist.com/en/
WildList Organization International	http://www.wildlist.org/

Phishing Resources

Resource/Title	URL
Anti-Phishing Working Group (APWG)	http://www.antiphishing.org/
FTC, "How Not to Get Hooked by a 'Phishing' Scam"	http://ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm
Internet Crime Complaint Center (ICCC)	http://www.ic3.gov/
Phish Report Network	http://www.phishreport.net/

Spam Resources

Resource/Title	URL
Coalition Against Unsolicited Commercial Email (CAUCE)	http://www.cauce.org/
Distributed Server Blackhole List (DSBL)	http://www.dsbl.org/
Federal Trade Commission (FTC) Spam Home Page	http://www.ftc.gov/spam/
GetNetWise	http://spam/getnetwise.org/
Messaging Anti-Abuse Working Group	http://www.maawg.org/
Not Just Another Bogus List	http://njabl.org/
OnGuard Online	http://onguardonline.gov/index.html
Open Relay Database	http://www.ordb.org/
Spam.abuse.net	http://spam.abuse.net/
Spamhaus	http://www.spamhaus.org/
Spam Prevention Early Warning System (SPEWS)	http://www.spews.org/
SPAM-L Mailing List Frequently Asked Questions (FAQ)	http://www.claws-and-paws.com/spam-l

Mail Server Security Patch Resources

Server/Manufacturer	URL
602LAN Suite (Software602)	http://www.software602.com/products/ls/
ArGoSoft Mail Server (ArGoSoft)	http://www.argosoft.com/rootpages/Download.aspx
CommuniGate Pro (Stalker Software)	http://www.stalker.com/CommuniGatePro/
Eudora Internet Mail Server (EIMS) (Glenn Anderson)	http://www.eudora.co.nz/updates.html
Eudora WorldMail Server (Qualcomm)	http://www.eudora.com/download/worldmail/
Exim (Exim)	http://www.exim.org/
IMail Server (Ipswitch)	http://www.ipswitch.com/support/imail/patch-upgrades.asp
inFusion Mail Server (CoolFusion)	http://www.coolfusion.com/downloads/
Kaspersky SMTP Gateway for UNIX (Kaspersky)	http://www.kaspersky.com/productupdates/
Kerio MailServer (Kerio Technologies)	http://www.kerio.com/subscription.html
Lotus Domino (IBM)	http://www-132.ibm.com/content/home/store_IBMPublicUSA/en_US/Upgrades.html
MailEnable (MailEnable)	http://www.mailenable.com/hotfix/default.asp
MailMax (Smartmax Software)	http://www.smartmax.com/mmupgradecenter.aspx
MailSite (Rockliffe)	http://www.rockliffe.com/userroom/download.asp
MDaemon (alt-n Technologies)	http://www.altn.com/download/default.asp?product_id=MDaemon
Merak Mail Server (Merak)	http://www.merakmailserver.com/Download/
Microsoft Exchange (Microsoft)	http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2003/default.mspx
Postfix (Wietse Venema)	http://www.postfix.org/download.html
Sendmail (commercial version) (Sendmail, Inc.)	http://www.sendmail.com/support/
sendmail (freeware version) (Sendmail Consortium)	http://www.sendmail.org/
Xmail (Davide Libenzi)	http://www.xmailserver.org/

Mail Client Security Patch Resources

Client/Manufacturer	URL
Balsa (GNOME Project)	http://balsa.gnome.org/download.html
Barca (Poco Systems)	http://www.pocosystems.com/home/index.php?option=content&task=category&sectionid=2&id=21&Itemid=38
Eudora (Qualcomm)	http://www.eudora.com/download/
Eureka Email	http://www.eureka-email.com/Download.html
GNUMail.app (Collaboration-world.com)	http://www.collaboration-world.com/cgi-bin/project/release.cgi?pid=2
GyazMail (GyazSquare)	http://www.gyazsquare.com/gyazmail/download.php
i.Scribe (Memecode Software)	http://www.memecode.com/scribe.php
InScribe (Memecode Software)	http://www.memecode.com/inscribe.php
KMail	http://kmail.kde.org/download.html
Mac OS X Mail (Apple)	http://www.apple.com/support/panther/mail/

Client/Manufacturer	URL
Mailsmith (Bare Bones Software)	http://www.barebones.com/support/mailsmith/updates.shtml
Mercury Mail Transport System (David Harris)	http://www.pmail.com/patches.htm
Mozilla	http://www.mozilla.org/security/
Mutt	http://www.mutt.org/download.html
Nisus Email (Nisus Software)	http://www.nisus.com/NisusEmail/FAQ.php?PHPSESSID=0ba9f9639672d1fdf836a97f3ad29383#HowUpgradeOS9
Outlook (Microsoft Corporation)	http://office.microsoft.com/en-us/officeupdate/default.aspx
Outlook Express (Microsoft Corporation)	http://www.microsoft.com/downloads/search.aspx?displaylang=en&categoryid=7
Pegasus Mail (David Harris)	http://www.pmail.com/patches.htm
Pine (University of Washington)	http://www.washington.edu/pine/getpine/
PocoMail (Poco Systems, Inc.)	http://www.pocosystems.com/home/
Sylpheed	http://sylpheed.good-day.net/en/
Thunderbird (Mozilla)	http://www.mozilla.com/thunderbird/
VM	http://www.wonderworks.com/vm/download.html

NIST Publications on System and Network Security[70]

Publication	URL
SP 800-18 Revision 1, *Guide to Developing Security Plans for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf
SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf
SP 800-27, *Engineering Principles for Information Technology Security*	http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf
SP 800-28, *Guidelines on Active Content and Mobile Code*	http://csrc.nist.gov/publications/nistpubs/800-28/sp800-28.pdf
SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*	http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf
SP 800-34, *Contingency Planning Guide for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf
SP 800-37, *Federal Guidelines for the Security Certification and Accreditation of Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf
SP 800-40 Version 2, *Creating a Patch and Vulnerability Management Program*	http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
SP 800-41, *Guide to Firewall Selection and Policy Recommendations*	http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
SP 800-42, *Guideline on Network Security Testing*	http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf
SP 800-43, *Guide to Securing Windows 2000 Professional*	http://csrc.nist.gov/itsec/guidance_W2Kpro.html

[70] The primary Web site for all of these publications is located at http://csrc.nist.gov/publications/index.html.

Publication	URL
SP 800-44, *Guidelines on Securing Public Web Servers*	http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf
SP 800-46, *Security for Telecommuting and Broadband Communications*	http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf
SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security Implementations*	http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf
SP 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems*	http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf
SP 800-61, *Computer Security Incident Handling Guide*	http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
SP 800-63, *Electronic Authentication Guideline*	http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf
SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals*	http://csrc.nist.gov/itsec/download_WinXP.html
SP 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*	http://csrc.nist.gov/itsec/guidance_WinXP_Home.html
SP 800-83, *Guide to Malware Incident Prevention and Handling*	http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf
SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*	http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
SP 800-92, *Guide to Computer Security Log Management*	http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*	http://csrc.nist.gov/publications/nistpubs/

This page has been left blank intentionally.

Appendix F—Email Security Checklists

Planning and Managing Mail Servers

Completed	Action
	Plan the installation and deployment of mail server
☐	Identify functions of the mail server
☐	Identify categories of information that will be stored on, processed on, and transmitted through the mail server
☐	Identify security requirements of information
☐	Identify requirements for continuity of mail services
☐	Identify a dedicated host to run the mail server
☐	Identify network services that will be provided or supported by the mail server
☐	Identify users and categories of users of the mail server and determine privilege for each category of user
☐	Determine how the mail server will be managed (e.g., locally, remotely)
☐	Identify user authentication methods for the mail server
☐	Identify security or privacy requirements for email address-related information
	Choose appropriate operating system for mail server
☐	Minimal exposure to vulnerabilities
☐	Ability to restrict administrative or root level activities to authorized users only
☐	Ability to deny access to information on the server other than that intended to be available
☐	Ability to disable unnecessary network services that may be built into the operating system or server software
☐	Ability to log appropriate server activities to detect intrusions and attempted intrusions
☐	Availability of trained, experienced staff to administer the server and server products
	Plan the location of the mail server
☐	Appropriate physical security protection mechanisms
☐	Appropriate environmental controls to maintain the necessary temperature and humidity
☐	Backup power source
☐	Preparation for known natural disasters

Securing the Mail Server Operating System

Completed	Action
	Patch and upgrade operating system
☐	Create and implement a patching process
☐	Identify, test, and install all necessary patches and upgrades to the operating system
	Remove or disable unnecessary services and applications
☐	Remove or disable unnecessary services and applications
☐	Use separate hosts for Web servers, directory servers, and other services
	Configure operating system user authentication
☐	Remove or disable unneeded default accounts and groups
☐	Disable non-interactive accounts
☐	Create the user groups for the particular computer
☐	Create the user accounts for the particular computer
☐	Check the organization's password policy, and set account passwords appropriately (e.g., length, complexity)
☐	Configure computers to prevent password guessing
☐	Install and configure other security mechanisms to strengthen authentication
	Configure resource controls appropriately
☐	Set access controls for files, directories, devices, and other resources
☐	Limit privileges for most system-related tools to authorized system administrators
	Install and configure additional security controls
☐	Select, install, and configure additional software to provide needed controls not included in the operating system
	Test the security of the operating system
☐	Test operating system after initial install to determine vulnerabilities
☐	Test operating system periodically to determine new vulnerabilities

Securing Mail Servers and Content

Completed	Action
	Harden the mail server application
☐	Install the mail server software on a dedicated host (if Web-based mail access is desired, install the mail server software on a different host from the Web server)
☐	Apply any patches or upgrades to correct for known vulnerabilities
☐	Create a dedicated physical disk or logical partition (separate from operating system and mail server application) for mailboxes, or host the mailboxes on a separate server
☐	Remove or disable all services installed by the mail server application but not required (e.g., Web-based mail, FTP, remote administration)

Completed	Action
☐	Remove or disable all unneeded default login accounts created by the mail server installation
☐	Remove all manufacturer documentation from server
☐	Remove any example or test files from server
☐	Apply appropriate security template or hardening script to the server
☐	Reconfigure SMTP, POP and IMAP service banners (and others as required) NOT to report mail server and operating system type and version
☐	Disable dangerous or unnecessary mail commands (e.g., VRFY and EXPN)
	Configure operating system and mail server access controls
☐	Limit the access of the mail server application to a subset of computational resources
☐	Limit the access of users through additional access controls enforced by the mail server, where more detailed levels of access control are required
☐	Configure the mail server application to execute only under a unique individual user and group identity with restrictive access controls
☐	Ensure the mail server is not running with root or system/administrator privileges
☐	Configure the host operating system so that the mail server can write log files but not read them
☐	Configure the host operating system so that temporary files created by the mail server application are restricted to a specified and appropriately protected subdirectory
☐	Configure the host operating system so that access to any temporary files created by the mail server application is limited to the mail server processes that created these files
☐	Ensure that the mail server cannot save files outside of the specified files structure dedicated to the mail server
☐	Configure the mail server to run in a chroot jail on Linux and Unix hosts
☐	Install users' mailboxes on a different server (preferred), hard drive, or logical partition than the operating system and mail server application
☐	Configure the mail server application so it cannot consume all available space on its hard drives or partitions
☐	Limit the size of attachments that are allowed
☐	Ensure log files are stored in a location that is sized appropriately
	Protect email from malware
☐	Determine which types of attachments to allow
☐	Consider restricting the maximum acceptable size for attachments
☐	Determine if having access to personal email accounts from organizational computers is appropriate
☐	Determine which types of active content should be permitted within email messages
☐	Implement centralized malware scanning (on the firewall, mail relay, mail gateway, and/or mail server)
☐	Install malware scanners on all client hosts
☐	Implement centralized content filtering

Completed	Action
☐	Configure content filtering to block or tag suspicious messages (e.g., phishing, spam)
☐	Configure content filtering to strip suspicious active content from messages
☐	Configure lexical analysis if required
☐	Take steps to prevent address spoofing, such as blocking emails from external locations using internal “From” addresses
☐	Create a security policy that addresses content filtering
☐	Have the security policy reviewed by appropriate legal, privacy, and human resources authorities
☐	Add a legal disclaimer to emails, if required
☐	Educate users on the dangers of malware and how to minimize those dangers
☐	Notify users when an outbreak occurs
	Block spam-sending servers
☐	Configure mail gateways or firewalls to use LDAP lookup to confirm the existence of email recipients
☐	Configure mail server to block email from open relay blacklists or DNS blacklists, if required
☐	Configure mail server to block email from specific domains, if required
	Use authenticated mail relay
☐	Configure authenticated mail relay on the server
	Secure access to the mail server
☐	Configure mail server to use encrypted authentication
	Enable Web access to email
☐	Configure mail server to support Web access only via SSL/TLS and only if such access is deemed necessary

Implementing a Secure Network Infrastructure

Completed	Action
	Network location
☐	Mail server is located on the internal network and protected by a mail gateway and/or firewall, or Mail server is located in a DMZ
	Firewall configuration
☐	Mail server is protected by a firewall
☐	Mail server, if it faces a higher threat or if it is more vulnerable, is protected by an application layer firewall
☐	Firewall controls all traffic between the Internet and the mail server
☐	Firewall blocks all inbound traffic to the mail server except the necessary ports, such as TCP ports 25 (SMTP), 110 (POP3), 143 (IMAP), 398 (LDAP), 636 (secure LDAP), 993 (secure IMAP), and 995 (secure POP)

Completed	Action
☐	Firewall blocks (in conjunction with the intrusion detection or prevention system) IP addresses or subnets that the IDS or IPS reports are attacking the organizational network
☐	Firewall blocks known "blacklisted" networks or subnets, as identified by a trusted external security response center
☐	Firewall notifies the network administrator or mail server administrator of suspicious activity through an appropriate means
☐	Firewall provides content filtering and malware scanning
☐	Firewall is configured to protect against DoS attacks
☐	Firewall logs critical events
☐	Firewall and firewall operating system patched to latest or most secure level
	Intrusion detection and prevention systems
☐	IDPS configured to monitor traffic network traffic to and from the mail server
☐	IDPS configured to monitor changes to critical files on mail server (host-based IDPS or file integrity checker)
☐	IDPS configured to monitor the system resources available on the mail server host (host-based IDPS)
☐	IDPS blocks (in conjunction with the firewall) IP addresses or subnets that are attacking the organizational network
☐	IDPS notifies the necessary parties of suspected attacks through appropriate means according to the organization's incident response policy and procedures
☐	IDPS configured to maximize detection with an acceptable level of false positives
☐	IDPS configured to log events and to capture packet header information for network events
☐	IDPS updated with new attack signatures frequently (e.g., on a daily to weekly basis, typically after testing the updates)
	Network switches
☐	Network switches are used to protect against network eavesdropping
☐	Network switches are configured in high-security mode to defeat ARP spoofing and ARP poisoning attacks
☐	Network switches are configured to send all traffic on network segment to network-based IDPS

Securing Mail Clients

Completed	Action
	Patch and update mail clients
☐	Update mail client to newest or most secure version
☐	Apply any necessary patches to mail client (in conformance with organizational polices and configuration management)
☐	Apply any necessary patches to Web browser (for mail clients that are integrated with browser)
	Configure mail client security features
☐	Disable automatic message preview
☐	Disable automatic opening of messages
☐	Disable automatic loading of pictures in messages
☐	Disable downloading and processing of active content (if appropriate)
☐	Enable anti-spam and anti-phishing features
☐	Reconfigure portable mail clients, such as those on cell phones and PDAs, to improve their security
☐	Ensure that security policy supports the protection of portable mail clients, such as requiring anti-virus software to be installed and enabled
☐	Limit access to VPN clients and other remote access applications on mobile devices, or remove the clients/applications if they are not needed
	Configure authentication and access
☐	Enable secure authentication and access
☐	Disable ability of mail client to store username and passwords
☐	Configure client to use encryption (TLS) for SMTP, POP, and IMAP communications
☐	Set restrictions on the selection of email addresses, such as ensuring they are unrelated to user account names
	Secure the mail client host operating system
☐	Keep the OS updated to the most secure patch level
☐	Configure the OS to allow only the appropriate user(s) to access locally stored messages and mail client configuration files
☐	Secure or remove Windows Script Host (Windows hosts only)
☐	Change the default action on files associated with the Windows Script Host from execute to edit (Windows hosts only)
☐	Ensure that the OS is configured to show full file extensions (Windows hosts only)
☐	Install an anti-virus application and configure it to scan incoming messages and attachments; also install an anti-spyware application if the anti-virus software does not offer robust anti-spyware capabilities
☐	Install a personal firewall if needed to protect the computer from unauthorized communications
☐	Ensure the OS enforces the concept of least privilege, because malicious code runs in the security context on which it was launched (i.e., the user's access level)

Completed	Action
☐	Ensure that critical components of the operating system are protected from malicious code
☐	Use a file encrypting application to protect the email stored locally on the user's hard drive (especially important for mobile devices)
☐	Configure the OS to automatically lock the current session after a fixed period of inactivity
	Secure message composition
☐	Provide security for email message content (e.g., S/MIME, OpenPGP)
	Use of plug-ins
☐	Enable and install only absolutely necessary plug-ins from trusted sources
	Access to Web-based mail systems
☐	Configure Web-based mail access to only use 128-bit SSL/TLS connections
☐	Make users aware of what they should do before granting them access to Web-based mail

Administering the Mail Server

Completed	Action
	Logging
☐	Log IP stack setup errors
☐	Log resolver configuration problems (e.g., DNS, NIS)
☐	Log mail server configuration errors (e.g., mismatch with DNS, local configuration error, out-of-date alias database)
☐	Log lack of system resources (e.g., disk space, memory, CPU)
☐	Log alias database rebuilds
☐	Log logins (failed, and also successful if adequate space is available)
☐	Log security problems (e.g., spamming)
☐	Log lost communications (network problems)
☐	Log protocol failures
☐	Log connection timeouts
☐	Log connection rejections
☐	Log use of VRFY and EXPN commands
☐	Log send on behalf of
☐	Log send as
☐	Log malformed addresses
☐	Log message collection statistics
☐	Log creation of error messages
☐	Log delivery failures (permanent errors)
☐	Log messages being deferred (transient errors)
☐	Store logs on a separate logging server
☐	Backup and archive logs according to organizational requirements
☐	Review logs daily

Completed	Action
☐	Review logs weekly (for more long-term trends)
☐	Use automated log file analysis tool(s)
	Mail server backups
☐	Create a mail server backup policy
☐	Back up mail server differentially or incrementally on a daily to weekly basis
☐	Back up mail server fully on a weekly to monthly basis
☐	Periodically archive backups
	Recovering from a compromise
☐	Report incident to organization's computer incident response capability
☐	Isolate compromised system(s) or take other steps to contain attack so additional evidence can be collected
☐	Consult, as appropriate, with management, legal counsel, and law enforcement expeditiously
☐	Investigate similar hosts to determine if the attacker has also compromised other systems
☐	Analyze the intrusion
☐	Restore the system
☐	Test system to ensure security
☐	Reconnect system to network
☐	Monitor system and network for signs that the attacker is attempting to access the system or network again
☐	Document lessons learned
	Security testing
☐	Periodically conduct vulnerability scans on mail server and supporting network
☐	Update vulnerability scanner before testing
☐	Correct any deficiencies identified by the vulnerability scanner
☐	Conduct penetration testing on the mail server and the supporting network infrastructure
☐	Correct deficiencies identified by penetration testing
	Remote administration
☐	Use a strong authentication mechanism (e.g., public/private key pair, two factor authentication)
☐	Restrict which hosts can be used to remotely administer the mail server by IP address or by authorized users
☐	Use secure protocols (e.g., SSH, HTTPS) that can provide encryption for both passwords and data
☐	Enforce the concept of least privilege on remote administration (e.g., attempt to minimize the access rights for the remote administration accounts)
☐	Change any default accounts or passwords for the remote administration utility or application
☐	Do not allow remote administration from the Internet unless mechanisms such as VPN are used
☐	Do not mount any file shares on the internal network from the mail server and vice versa

Appendix G—Acronym List

3DES	Triple Data Encryption Standard
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
ARP	Address Resolution Protocol
ARPA	Advanced Research Project Agency
ASCII	American Standard Code of Information Interchange
BCP	Best Current Practice
CA	Certificate Authority
CIO	Chief Information Officer
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CRAM	Challenge-Response Authentication Mechanism
CSE	Communications Security Establishment
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSBL	Domain Name System Blacklist
DoD	Department of Defense
DoS	Denial of Service
DSA	Digital Signature Algorithm
DSN	Delivery Status Notification
DSS	Digital Signature Standard
ESMTP	Extended Simple Mail Transfer Protocol
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBE	Identity-Based Encryption
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISP	Internet Service Provider
ISSO	Information Systems Security Officer
ISSPM	Information Systems Security Program Manager

IT	Information Technology
ITL	Information Technology Laboratory
LDA	Local Delivery Agent
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
MIME	Multipurpose Internet Mail Extensions
MOSS	MIME Object Security Services
MTA	Mail Transfer Agent
MUA	Mail User Agent
NARA	National Archives and Records Administration
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NIS	Network Information System
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OMB	Office of Management and Budget
OpenPGP	Open Pretty Good Privacy
ORB	Open Relay Blacklist
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
POP	Post Office Protocol
RAID	Redundant Array of Inexpensive Disks
RFC	Request for Comments
SAISO	Senior Agency Information Security Officer
SHA-1	Secure Hash Algorithm-1
SHS	Secure Hash Standard
SIEM	Security Information and Event Management
S/MIME	Secure Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOHO	Small Office Home Office
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security

UCE	Unsolicited Commercial Email
UDP	User Datagram Protocol
U.S.	United States
VBScript	Visual Basic Script
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WSH	Windows Scripting Host
WWW	World Wide Web

This page has been left blank intentionally.

Appendix H—Index

N

O

P

R

S

T

U

V

W

X