realtimepublishers.com™

The Definitive Guide™ To

Email Management and Security

Kevin Beaver

Copyright Statement

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

Chapter 5: Email Security In-Depth

Email is one of our most critical business applications, but it is also one of the most vulnerable. Beyond malware, spam, and content filtering, another class of email risks affects how we deploy, use, and manage our electronic communications. This risk is partly due to the fact that email servers have to communicate with internal and external systems simultaneously—all while housing some of an organization's most critical assets.

Many useful resources provide technical theory about email protocols, information risk assessments, and encryption; I've included references to some of my favorite technical resources throughout the chapter. In this chapter, rather than focus on technical theory, we'll explore practical aspects of email security that you can immediately apply in your environment—assessing email risks, employing best practices for hardening servers and clients, and using incident response tools and techniques that can help you when your email system is attacked.

The Need for Strong Email Security

An Ohio man attacks a rival company's computer system, shuts down the email server, and reads email messages of executives to obtain information that would give his employer commercial advantage (for more information, see http://www.cybercrime.gov/doppsPlea.htm). This incident, reported in a U.S. Department of Justice press release, represents the tip of the iceberg when it comes to attacks against email systems. The number of known attacks is enormous, and there are many that go either unnoticed, unreported, or both.

The need for in-depth email security is obvious, but different organizations will require varying degrees. For example, a construction company that communicates highly sensitive information to suppliers, builders, and contractors will need security but not the level of privacy required by a hospital. The necessary degree of email security depends on factors such as government regulations and the amount of perceived and actual risk to email within an organization.

> No two organizations are alike. The email security concepts I present in this chapter, including the steps for performing risk assessments and responding to email security incidents, are flexible and scalable to your specific needs.

Email Security Background

The Simple Mail Transfer Protocol (SMTP) was introduced in 1982. According to the Internet Engineering Task Force (IETF) Request for Comments (RFC) 821, which outlines the SMTP specification, SMTP was developed to "ensure a more reliable and efficient way to transport messages." Its original design and use did not take into consideration the widespread public use of the Internet, and SMTP is inherently insecure—something we figured out about 15 years after its introduction.

Since the early days, email usage has evolved considerably, but messaging protocols have remained basically the same. The popularity of email combined with the inquiring minds of hackers has resulted in the discovery of serious security shortcomings in SMTP and its associated protocols. Therefore, we must take certain precautions to ensure the three cornerstones of email security—confidentiality, integrity, and availability.

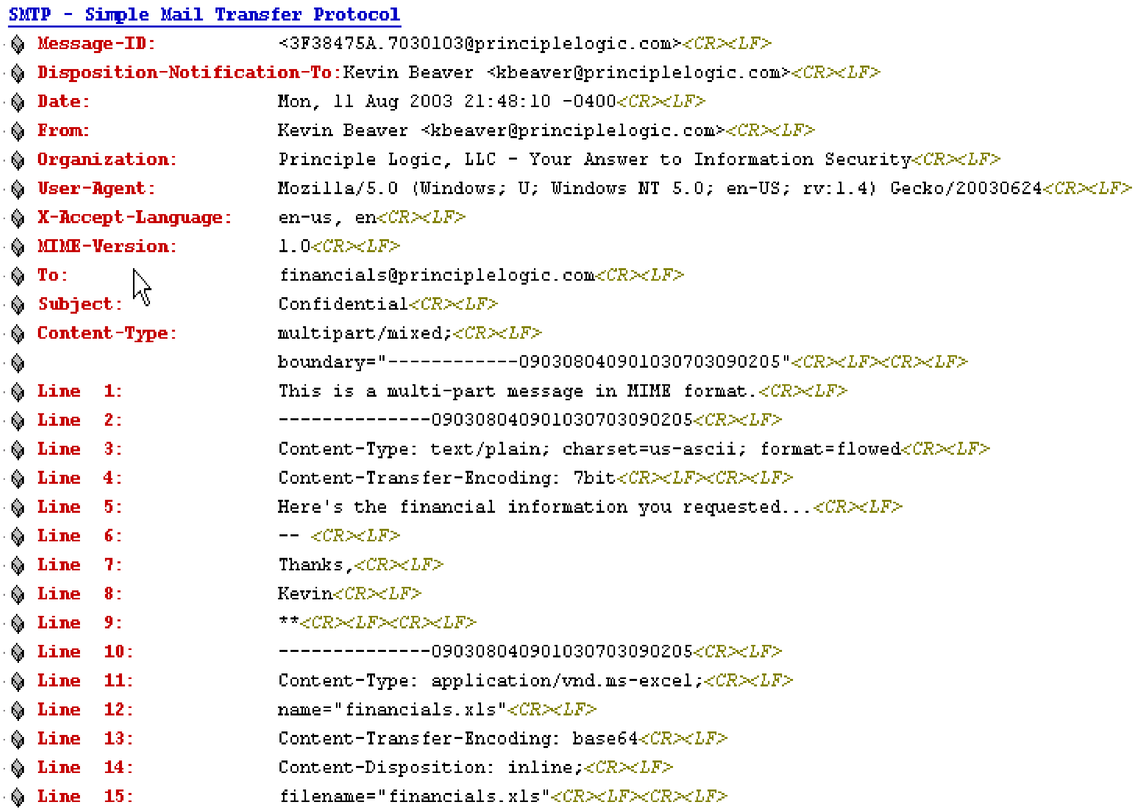
According to the CERT/CC Vulnerability Notes Database (http://www.kb.cert.org/vuls), since 2001, there have been eight major SMTP-related vulnerabilities that affect various well-known email software vendors.

Additional Email Security Concerns

In previous chapters, we explored malware, spam, and content attacks, so you might be wondering whether there are any email security threats that we haven't covered. Unfortunately, there are plenty! In addition to taking measures to protect your systems from well-known attacks, you must be prepared to contend with email software that is full of security holes when it arrives from the vendor.

Is such a threat truly a possibility? Consider the 2002 source code compromise in the highly popular Sendmail program. Supposedly, a Trojan horse was placed in the Sendmail's source code, which thousands of unknowing users downloaded, compiled, and installed to their production email systems.

In addition, you must deal with the fact that email is transmitted across the wire in clear text by default. Figure 5.1 illustrates the "nakedness" of email across the wire. This figure shows a network analyzer capture of an email message in transit. You can see the From, To, and Subject line information as well as the entire message body and the encoded attachment filename.



```
SMTP - Simple Mail Transfer Protocol
Message-ID:                  <3F38475A.7030103@principlelogic.com><CR><LF>
Disposition-Notification-To:Kevin Beaver <kbeaver@principlelogic.com><CR><LF>
Date:                        Mon, 11 Aug 2003 21:48:10 -0400<CR><LF>
From:                        Kevin Beaver <kbeaver@principlelogic.com><CR><LF>
Organization:                Principle Logic, LLC - Your Answer to Information Security<CR><LF>
User-Agent:                  Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.4) Gecko/20030624<CR><LF>
X-Accept-Language:           en-us, en<CR><LF>
MIME-Version:                1.0<CR><LF>
To:                          financials@principlelogic.com<CR><LF>
Subject:                     Confidential<CR><LF>
Content-Type:                multipart/mixed;<CR><LF>
                             boundary="------------090308040901030703090205"<CR><LF><CR><LF>
Line  1:                     This is a multi-part message in MIME format.<CR><LF>
Line  2:                     --------------090308040901030703090205<CR><LF>
Line  3:                     Content-Type: text/plain; charset=us-ascii; format=flowed<CR><LF>
Line  4:                     Content-Transfer-Encoding: 7bit<CR><LF><CR><LF>
Line  5:                     Here's the financial information you requested...<CR><LF>
Line  6:                     -- <CR><LF>
Line  7:                     Thanks,<CR><LF>
Line  8:                     Kevin<CR><LF>
Line  9:                     **<CR><LF><CR><LF>
Line  10:                    --------------090308040901030703090205<CR><LF>
Line  11:                    Content-Type: application/vnd.ms-excel;<CR><LF>
Line  12:                    name="financials.xls"<CR><LF>
Line  13:                    Content-Transfer-Encoding: base64<CR><LF>
Line  14:                    Content-Disposition: inline;<CR><LF>
Line  15:                    filename="financials.xls"<CR><LF><CR><LF>
```

Figure 5.1: An EtherPeek capture of an email in transit.

As if these threats aren't scary enough, it is not uncommon for a "protected" email server that is behind a firewall to be compromised indirectly by an attacker who takes over a Web server or router and then moves on to the email server. You must also take into account network infrastructure issues, email authentication considerations, and even the remote possibility of someone eavesdropping on your network and viewing your email traffic.

To create a truly secure email environment, you must approach email security from a perspective that goes beyond the stereotypical virus and spam issues. Consider the network, OS, and application attacks that can occur in the email sending, receiving, and storage process, including:

- Malicious port scanning
- Network analyzer captures
- Session hijacking
- Message modification
- Spoofing
- DoS attacks against the network, OS, and email applications
- File system integrity attacks
- Password cracking
- Malicious vulnerability testing
- Vulnerability exploitation
- Log file modification
- Email bombs
- Social engineering
- Dumpster diving
- Passive attempts to glean information off the Internet
- Physical security attacks (such as stealing servers, storage media, and hard copy documents)
- Abuse of SMTP commands such as VRFY (to verify valid email addresses) and EXPN (to expand the delivery addresses of mailing lists and aliases)

In addition to these attacks, you need to consider that email messages contain quite a bit of information that could be used against your systems, including:

- Sender information
- Receiver information
- Time and date stamps
- Server and client software version information
- Internal server names and IP addresses

This type of information can be used to gather trends about email usage that could easily tip off a malicious user. For example, a rogue insider could have access to application, content filtering, or firewall logs and ascertain that certain messages are being sent at specific times or days from certain people. Just out of curiosity, this insider goes a step further to see what's in these emails that seem to be so structured. Anything from a simple password reset or crack to a basic network analyzer inside the network (or just outside the firewall) could reveal that these messages contain highly confidential financial or patient healthcare information. This revelation, in turn, could lead to unauthorized information disclosure, posting of the information on the Internet, blackmail, and so on—you get the picture.

Assessing Email Security Risks

Malware protection, spam blocking, and content filtering are all, by design, reactive in nature. You can implement many email security best practices to help augment this reactive protection. To know which best practices to apply to your environment, start with an assessment of risks that are present in your email system. This assessment will expose what needs to be protected, which, in turn, will reveal specific countermeasures that you can use to minimize risks.

✎ In this section, I will highlight the important areas to consider when performing an email risk assessment. Keep in mind that email security risks are only part of the overall picture. Although the focus is on *email* risks in this chapter, you should consider making this process part of an overall information risk assessment that looks at every IT and business function from both a technical and an organizational perspective.

Before you get started, and to aid in obtaining upper management buy-in for an email risk assessment, it's important to understand the common risks that are present in email systems. A good way to start gathering information is to perform an Internet search for information security surveys and statistics put out by independent research firms and security vendors. Just remember that statistics tell only part of the story—the majority of organizations that experience security breaches do not report those breaches, so more is going on out there than studies reveal.

✎ Threats are *indications* and vulnerabilities are *weaknesses.* Risk is the likelihood of a threat exploiting a vulnerability and is often determined by multiplying the threat by the vulnerability.

Email Risk Assessment Considerations

Basic information security threats related to email include hackers, malware, disgruntled employees, and so on. The vulnerabilities include a lack of antivirus or spam protection, uneducated users, and so on. These threats and vulnerabilities, when combined, become the specific information risks for an organization. We'll explore key considerations for assessing your organization's email risks and walk through the assessment process.

First, determine how you want to classify risks: quantitatively (using numeric values) or qualitatively (using subjective opinions). The qualitative method is the most popular (and easiest) to perform. Performing a quantitative analysis can be very difficult because it's next to impossible—within a reasonable amount of time—to put a price on the tangible, and especially intangible, assets related to an email system.

In the qualitative method, you look at the specific threats and vulnerabilities found during the assessment process, then determine the likelihood that the threats will become reality as well as their potential impact on the organization. A useful tool in this process is a risk matrix, an example of which Table 5.1 shows.

Risk	Likelihood	Impact
Email server taken offline as a result of poor network placement	High	High
Emails sent over an unsecured wireless LAN	High	Medium
Disclosure of DNS configuration of the email system	High	Low
Exploitation of unpatched email server	Medium	High
Comprised user passwords	Medium	Medium
Personal use of corporate email	Medium	Low
Disclosure of confidential via intercepted emails	Low	High
Opening of a malware attachment	Low	Medium
Cleaning crew use of the email system	Low	Low

Table 5.1: Risk matrix showing likelihood and potential impact for example risks.

The impact and likelihood of each risk is ranked based on high, medium, and low:

- High—Risks that place your information assets in direct danger and can cause catastrophic losses.
- Medium—Risks that place your information assets in potential danger and can cause great losses, especially when combined with other risks.
- Low—Risks that place your information assets in slight danger and can cause minimal losses.

After you determine the impact and likelihood of risks, you can focus on high-risk items for the short term and lower-risk items in the future.

In addition to assessing threats and vulnerability from a technical perspective, consider the business and organizational perspective. Human and business processes pose as many risks to information systems as technical issues present. When taking into account business processes, evaluate using the same level of neutrality and the same criteria whenever possible. Every manager believes his or her systems are the most critical to the organization—rather than looking at your information risks through a social or political lens, look at everything from an outsider's perspective.

The following list highlights questions to consider when performing a technical and organizational risk assessment:

- Are your email server and/or clients publicly accessible via the Internet?
- Are any modems connected to your critical hosts for regular dialup or remote management?
- What other ways can your hosts be accessed—ping, telnet, Simple Network Management Protocol (SNMP), and so on?
- Are current security policies and procedures in place? If so, are users aware of them and are the policies being enforced?
- How many users do you have?
- Do users understand the implications of email threats and vulnerabilities?
- Are passwords required for email access? If so, are there minimum-password strength requirements?
- How many hits does your email server get per day?
- Does your email system store and transmit confidential information?
- Are backups being made of emails?
- What other applications and services are running on the email server—ftp, Web server, telnet, DNS, Web proxy, and so on?
- Have you changed your banners to mask which version of email server software you're running in case someone telnets to your host?
- Has the rule of least privilege been implemented on your firewall, OSs, and applications to minimize access and prevent unauthorized use?
- Does the Whois database give out too much information about your organization and network—information that could be used against you?

> Check out the tools at http://www.samspade.org to determine what information can be gleaned about your domain and hosts.

Email Risk Assessment Process

The following steps walk you through an email risk assessment:

1. Gather as much information as possible about your systems, including network diagram creation, data flow diagram creation, software documentation, documentation of existing security policies and procedures, and so on.
2. Classify data related to the email system so that you'll know which data takes higher priority than others. Consider using the following classifications:
    - Sensitive—Data that is the most critical and should have the most limited access
    - Confidential—Data that is for internal use only
    - Proprietary—Data that is used for competitive advantage

- Private—Data that should be kept private whenever possible
- Public—Data that is publicly disclosed

3. Perform a technical vulnerability assessment using your own tools and/or some of the tools listed in the sidebar “Email Security Assessment Tools.” Perform these tests from both inside your network and outside your network from a hacker’s eye view.

Email Security Assessment Tools

There are many useful utilities available for assessing the technical security of your email server and client networks, OSs, and applications—both freeware and commercial products. The following list provides some of my favorite tools categorized by type:

Vulnerability Assessment Tools

QualysGuard at http://www.qualys.com

GFi LANguard at http://www.gfi.com/languard

SPI Dynamic WebInspect at http://www.spidynamics.com

Microsoft Baseline Security Analyzer at http://www.microsoft.com/technet/security/tools/tools/mbsahome.asp

Nessus at http://www.nessus.org

Port Scanners

Foundstone SuperScan at http://www.foundstone.com

Gibson Research Corporation Shields UP!! at https://grc.com/x/ne.dll?bh0bkyd2

Password Crackers

@stake LC4 at http://www.atstake.com

John the Ripper password cracker at http://www.openwall.com/john

Bindview Pwdump2 at http://razor.bindview.com/tools/desc/pwdump2_readme.html

ElcomSoft Password Recovery Software at http://www.elcomsoft.com/prs.html

Miscellaneous Tools

SecurityFocus NetBIOS Auditing Tool at http://www.securityfocus.com/tools/543

NetScan Tools Pro at http://www.netscantools.com/nstpromain.html

GFI Email Security Testing Zone at http://www.gfi.com/emailsecuritytest

4. Perform interviews with a cross-section of employees from software developers to C-level executives in order to determine how they handle email and what they believe are the greatest risks to the organization’s email systems. As you perform the interviews, you may need to add more questions/categories.
5. Document the threats and vulnerabilities found through the tools and interviews.
6. Prioritize the threats and vulnerabilities into risk categories using a matrix similar to the one that Table 5.1 shows.
7. Document your strategy to mitigate risks, including specific action steps required and countermeasures (technical and procedural) you plan to employ.
8. Implement the necessary countermeasures.

☞ Once your initial email risk assessment has been completed, you'll need to continuously focus on ongoing information risk management concepts:

- Assess periodically for new information risks
- Plan out new security strategies
- Implement new countermeasures as appropriate
- Monitor for new threats and vulnerabilities
- Control new information risks with corrective actions on an ongoing basis

The following list highlights tips for a successful email risk assessment:

- Ensure that responsibility and authority has been properly assigned so that the job can be completed without hassle.
- Choose the proper people to perform the work. An email risk assessment is not just for IT personnel—you'll need to involve a good cross-section of people within the organization.
- Use proven risk assessment methodologies such as the CERT OCTAVE program (see the following Cool Tools box)—doing so can save you a lot of time and frustration.
- Make sure the proper tools are available to complete the technical testing.

🖫 The CERT Software Engineering Institute's Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) framework is an excellent information risk assessment tool. This tool is designed for larger organizations, but a version dedicated to small businesses is in the works. Why start from scratch developing your own information risk assessment methodology when OCTAVE may be just what you need. I highly recommend that you look into this tool at http://www.cert.org/octave.

The steps in this section were simplified to encompass the needs of most organizations, which, regardless of their size, have similar issues. This process will grow more complex relative to the size of the organization. A major objective to keep in mind is that every email-related IT function, computer, application, business process, and so on needs a minimal level of security. Determining the minimal level is the goal of your email risk assessment.

Email Encryption

After you determine the minimal level of security for your email systems, you might consider email encryption as part of your information security plan. Email encryption technologies and products have been around for quite some, but still aren't overwhelmingly popular. Encryption technologies offer various benefits including:

- Confidentiality—A guarantee of message privacy
- Integrity—A guarantee that messages will not be modified while in transit
- Authentication—A guarantee that the person who claims to have sent a message actually sent it
- Non-Repudiation—An undeniable guarantee that the sender, and the sender only, actually sent a message

Virtually no email is secured against eavesdropping, and email goes across the wire in clear text by default. Though some argue that this is an obvious vulnerability, the likelihood that an attacker will be able to intercept the necessary data for an attack via in-transit email is miniscule compared with the other threats and vulnerabilities that email faces. Whether you decide to spend time, money, and effort in the development, implementation, and management of encryption technologies depends on your organization.

However, data in transit is not where the greatest vulnerability lies. Attackers that want to truly hack into an email system have a very slim chance of capturing the necessary data to attack as it goes from point A to point B across the Ethernet. Even if a few packets are captured, the captured data is most likely not information that will help much in a potential system attack—millions (and sometimes billions) of packets are traversing the average network every day. What the hacker really wants—and goes for—is the data at rest. Encryption of the email message store (database), individual messages, or even the disk partition on which the messages are located can keep messages safe long after they are sent or received; however, Inboxes that are encrypted to the hilt but have a weak password are still easy targets.

> ✎ Public key infrastructure (PKI) is a technology that allows you to implement and manage data encryption for email, Web, VPNs, and more—an option if you need to deploy email encryption enterprise-wide. Check out the PKI Page at http://www.pki-page.org for links to useful PKI reference material.

Some organizations, such as HIPAA-covered entities, may have to encrypt email if their risk assessment shows that confidential information is a potential vulnerability. Other government regulations, both current and future, are bound to address this issue. If complete security is required for all communications and there can be no chance of message interception, encryption should be implemented. If your organization does so, focus as much effort on securing the actual server, message store, and client systems as you do on encrypting email in transit. A few things to consider when it comes to encrypting email:

- Encrypting emails takes time; whether this longer response time is a problem for your environment depends on your email response time needs.
- Encryption increases the size of email messages, which can, over time, greatly impact your email storage requirements.
- If maximum security is a top priority—as it must be for organizations who require email encryption—choose 3DES or AES as your encryption algorithm as these are the foundation of a secure infrastructure that won't be easily cracked or have to be upgraded in the near future.
- Various export laws and other government regulations affect which type of email encryption system you use; consult with legal counsel or other experts to make sure that your organization is keeping up with the necessary legal requirements.

> 📖 For a comprehensive review of import/export laws that affect cryptography around the world, check out http://rechten.kub.nl/koops/cryptolaw.

SSL/TLS

Secure Sockets Layer (SSL) has been a tried-and-true protocol for supporting encryption of data communications. However, it is being phased out by the newer Transport Layer Security (TLS) protocol. You can configure your SSL or TLS solution to protect all outbound messages, messages traveling between certain servers or domains, and even all inbound requests for email communications. TLS 1.0 is based on SSL 3.0 and provides additional management and security extensions.

> For detailed information about the TLS specification, see RFC 2246 at http://www.faqs.org/rfcs/rfc2246.html.

Trying to enforce SSL usage on your server will undoubtedly cause communications problems with remote servers attempting to connect. By using TLS—the STARTTLS function of Extended SMTP (ESMTP) to be specific—your server and the remote servers connecting can negotiate how communications will occur. If both servers are enabled with ESMTP and STARTTLS functionality, they can encrypt the communications link.

This solution is similar to S/MIME in that the entire email session is encrypted—headers, message body, and attachments. (For more information about S/MIME, see the sidebar "PGP or S/MIME.") The only drawback to using this solution is that the link is only encrypted from server to server unless the email client can support end-to-end encryption via TLS. Thus, the final communication that takes place between the server and the client is unencrypted and susceptible to interception, which results in a vulnerability.

> Not sure whether your server supports TLS? Telnet to your email server on port 25 either from a command prompt by typing
>
> ```
> telnet your_mail_server_name_or_address 25
> ```
>
> or using your favorite telnet application within your desktop environment. You might need to enable local echo of characters in your telnet application in order to see what you're typing. You should receive some sort of welcome banner. Type
>
> ```
> EHLO yourdomain.com
> ```
>
> and press Enter. You should receive a 250 OK or similar message. If the server responds with a list that includes STARTTLS, then your server supports TLS.

Secure TLS-based message communications are becoming popular with email server software such as Microsoft Exchange, email security appliances such as CipherTrust IronMail, and ASP-based email security solutions such as Singlefin. This type of perimeter-based protection offers the following benefits:

- Communications work as SMTP proxies accepting and generating requests on behalf of email servers.
- Administrators can configure messaging requirements based on policies that are directed by HIPAA, GLBA, and other government regulations.
- Communications might not need to be placed behind the firewall because they are typically already running on hardened systems.

- Communications are based on Internet Protocol standards rather than vendor email solutions, so they can be used in any environment independent of the email server software.
- Communications can work in conjunction with non-TLS–based email communications such as standard SMTP.
- Communications do not require an internal or external PKI configured—these solutions handle encryption internally.

PGP or S/MIME

When it comes to standalone or desktop-focused encryption solutions, PGP and S/MIME are useful—and the most popular—applications. Whether you use PGP or S/MIME depends on your organization's specific needs. If you're looking for (almost) seamless integration with your email client software, S/MIME is a better solution because PGP requires an email client plug-in in order to work. However, the standalone version of PGP doesn't require a Certificate Authority (CA), which S/MIME requires, because you generate and manage your own certificates internally within the program. In addition, PGP supports the emerging AES standard for data encryption—but S/MIME support is coming soon.

The standalone version of PGP is more suitable for individuals and smaller organizations as a result of the operation and management methodology of the standalone version of PGP. The newer commercial version includes support for enterprises through a standard PKI-type configuration. S/MIME has broader compatibility between more organizations, perhaps making it easier to interoperate with clients and business partners. A downside to both is that they require the user to remember to encrypt each message that needs to be protected—something that you should not rely on when implementing a security measure.

Whichever solution you choose, keep in mind that most antivirus, spam, and content filtering applications are rendered useless when dealing with encrypted emails. A perimeter or ASP-based email security solution that manages its own encryption might be a better option for your organization.

Implementing Email Encryption

The preferred method of implementing email encryption is to automate it on the servers or at the network perimeter. Doing so eliminates the inconvenience and responsibility of handling encryption for end users, which results in a more effective email encryption implementation. However, automated encryption might lead to a false sense of security—with enough time and computing resources, virtually any encryption key can be broken, regardless of the length. That said, if you implement email encryption, don't go overboard. The Triple Data Encryption Standard (3DES) and AES provide sufficient encryption.

If you're not sure whether to implement email encryption, focus first on securing the true vulnerabilities that lie within the server and email application. In addition, concentrate on ensuring that end users are security conscious. Doing so can go a long way toward protecting your email investment and intellectual property. If neither of these measures is sufficient, move forward with your encryption efforts.

Email Security Best Practices

In addition to assessing and addressing your risks and determining whether your organization will benefit from email encryption, there are various ways to secure email servers beyond firewalls and antivirus protection programs. The following sections provide email security best practices that can be employed by every organization.

Email Server Security

First, consider is the placement of your email server, which is often the weakest link in an email server's configuration. Figure 5.2 shows the most common email server setup—an email server that resides on the internal network behind a firewall.

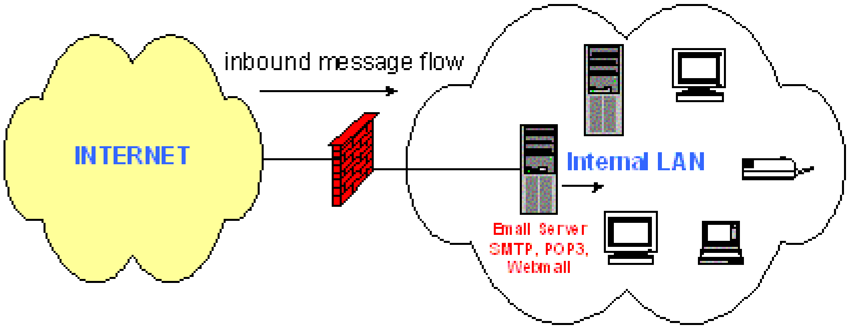


Figure 5.2: A typical email server configuration—on the internal LAN behind a firewall.

This configuration might be workable for small organizations on a budget, but there are some serious security issues presented by this configuration:

- The only level of network protection is the firewall, and firewalls cannot be relied upon for true SMTP security.
- Running all email services on one host results in a single point of failure for all messaging services.
- Running Web mail services increases the chances of a Web vulnerability being exploited and the server being taken down.
- If another internal host is compromised, there is a good chance that the email server will also be compromised from behind the firewall.

Figure 5.3 illustrates a more secure email server configuration.

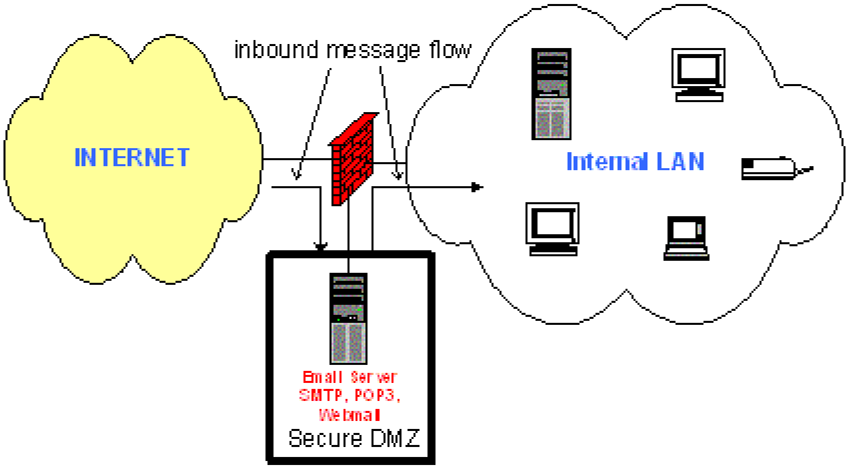


Figure 5.3: A more secure email server configuration using the firewall's DMZ.

This configuration is much more secure because the email server is separated from the internal network. This setup usually takes a more sophisticated firewall with a DMZ or a third connection, but it can be well worth the money from a security standpoint. Figure 5.4 shows yet another common email server configuration—one that is even more secure than the firewall DMZ configuration.

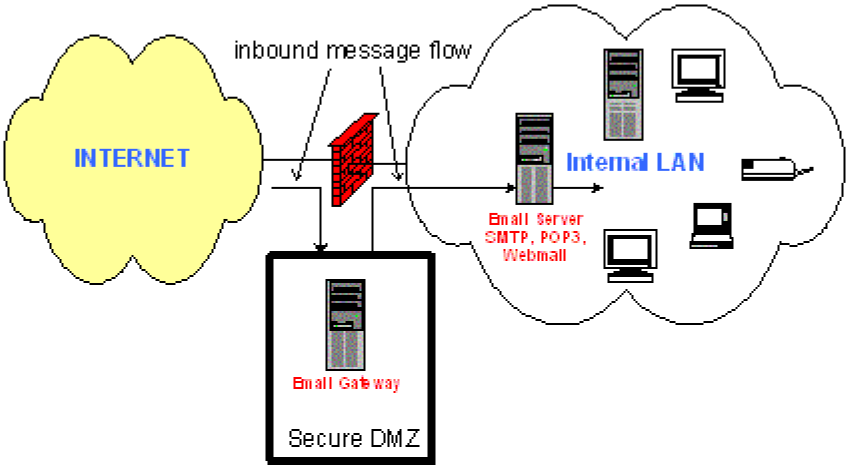


Figure 5.4: An even more robust email server configuration using the firewall's DMZ and an email gateway that adds an extra layer of security.

This last configuration is even more secure because an email gateway adds an extra layer of protection for the main email server, allowing it to take the brunt of the work and malicious attacks. This configuration not only eases the processing requirements of the email server but also provides the security benefit of being better protected against vulnerability exploits.

Ideally, however, this email server should not be hosting the Web mail application. A best practice is to run the Web mail application on a separate Web server in the DMZ. In addition, be aware that some Web mail servers, such as Outlook Web Access (OWA), require you to open various other ports for back-end communications to the email server. Doing so might defeat the purpose of putting the server in the DMZ.

The bottom-line for email server security is that if the server is not adequately protected, nothing is. The server absolutely must be hardened against attacks in every way possible. The following list highlights tips for securing your email server regardless of the platform on which it is running:

- Keep your OS and application patches consistently updated.
- Run your email server on a dedicated machine and disable any unnecessary protocols and services.
- Do not connect your email server directly to the Internet. Instead, use an SMTP gateway that sits in a DMZ or directly in front of your email server to serve as a proxy and front-line system that can be more easily secured from attacks.
- Change your default SMTP, POP3, and so on banners to display a warning message alerting potential intruders that all activity is logged and malicious activity is subject to prosecution (consult with your legal counsel on the wording for this warning).
- Only allow authenticated (user or IP address) email relay.
- Run your email server application using a special system or administrator account that has limited access on the server.
- Run your email server application on a separate share, partition, or drive (whichever is possible) to keep it independent from other system resources and data.
- Limit who has access to the administrator/root account.
- Enable account lockout in the event of a password-guessing attack.
- Limit message sizes so that a malicious outsider cannot send and resend huge attachments that can fill up your hard drive space.
- Set quotas on user storage space.
- Configure your system to deliver mail to only valid recipients or at least have a default mailbox that these wayward messages are dumped into. Also, be sure to check this default account on a periodic basis to clean it out and forward on the legitimate emails.
- Enable SSL and/or TLS support for POP, IMAP, and SMTP on your mail server so that the server can communicate securely with other hosts whenever possible. Refer to your specific application’s administrator guides for information about enabling this functionality.
- Configure your system to require the HELO or EHLO command when establishing an SMTP session in order to obtain the identification of remote systems connecting to your server.

- Disable unneeded SMTP commands, such as VRFY and EXPN, that can be used to obtain account names, aliases, and other configuration information from your system—or, at least, require a HELO or EHLO command first.
- Enable the highest level of logging that is possible (and practical) for your email server application, and log a remote syslog or share whenever possible.
- Limit incoming SMTP processes to prevent DoS conditions.
- If you configure your email server to send emails to a program or service that in turn runs a script or performs a function, monitor closely for attacks.
- Run malware protection software.
- Make sure that your email server is out of the physical reach of potential intruders. A physical security vulnerability can spell disaster for an email server.
- Keep fault tolerance in mind and consider the following:
    - Backup power supply (UPS or generator)
    - Dual power supplies in the server
    - Failover server(s)
    - Failover facilities

Web-Based Email Security

In addition to the email server tips, the most critical part of Web mail security is to ensure that the Web server application is secured from the elements. All of the myriad TCP port 80 (HTTP) vulnerabilities that affect Web servers and applications can affect your email system as well. Everything from cross-site scripting to unexpected user input must be protected against when hosting Web mail.

> For the best of both the Web mail and encryption, get a free encrypted Web mail account through the popular HushMail service at http://www.hushmail.com.

The following list highlights tips for securing Web mail:

- Harden the OS and Web server software using well-known best practices.

> If you’re running Microsoft IIS, be careful what you disable or strip out—you can easily disable OWA altogether.

- Consider implementing an application-level firewall or host-based firewall/intrusion detection system that can check for HTTP and HTTPS protocol anomalies and other attacks that would otherwise slip by a regular firewall system.
- Monitor your Web server log files.
- Host Web mail on a separate server if possible to help limit security vulnerabilities to the local machine and to keep eliminate a single point of failure in your email system.

- Consider enabling SSL (HTTPS) on the Web server and completely disabling HTTP traffic altogether.
- Ensure that Web browser software on the client-side is kept current.

> 📖 For more information about enabling SSL for OWA, refer to the following Microsoft articles:
>
> 📖 "XCCC: Turning On SSL for Exchange 2000 Server Outlook Web Access" at http://support.microsoft.com/default.aspx?scid=KB;en-us;320291&
>
> 📖 How to Force SSL Encryption for an Outlook Web Access 2000 Client at http://support.microsoft.com/default.aspx?scid=KB;en-us;279681&

Email Client Security

You can implement the following client security best practices on your workstations to ensure that the entire email system—not just the server and data communications links—is kept secure. Most of these tips are universal whether you're running Outlook, Eudora, Netscape Mail, Mozilla, and so on:

- Patch your OSs, Web browsers, and email client applications.
- Always run malware protection software.
- Run personal firewall/IDS software.
- Enable and enforce strong email passwords.
- Disable the email Preview Pane where applicable.
- Email clients that use command-line interfaces to access user mailboxes pose a huge security vulnerability, especially for external users. If possible, restrict access to these command-line programs (such as mail and pine) to internal users only or use email clients that support POP or IMAP.
- If dialup access is necessary, don't configure your server for direct dial-in. Instead consider enabling POP3 or IMAP access for the users through their regular ISP dialup accounts. A better alternative is to set up VPN access so that users can use their email client in its native mode without having to worry about any of the security issues associated with POP3, IMAP, and regular dialup. In addition, a VPN solution is much easier to implement and manage than a full-fledged PKI.
- Consider enabling Authenticated Post Office Protocol (POP) or Challenge-Response Authentication Mechanism (CRAM) for IMAP in Eudora clients—and elsewhere when possible—to allow for MD5 encryption of the users' clear-text passwords.

> 📖 For more information about this process, see RFC 1939 at http://www.ietf.org/rfc/rfc1939.txt.

- Consider enabling SSL between your email client and server via POP3S (TCP port 995) or IMAPS (TCP port 993).
- Consider enabling S/MIME support.

There's always a chance that users could be sending anonymous emails out of your network for criminal purposes or simply for fun. Either way, you should look for such activity via a content-filtering application, network analyzer, log files, and so on to help reduce your organization's liabilities and perhaps help eliminate such activity. A simple Google search on "anonymous email" or "email remailer" will reveal the current popular sites that your users may be accessing to do this.

Responding Effectively to Email Incidents

You can have every possible product, policy, and best practice in place to protect your email system, but there will come a time when you'll need to respond to an incident that you had not planned for. Incident response planning, especially related to email applications, is usually an afterthought.

Incident response is a complex topic. An incident response plan is the key element you'll need to successfully respond to email security incidents. This plan is similar to security policies and disaster recovery plans in that it needs to be well-documented, tested, and updated as needed.

There are many useful incident response resources available. I recommend Incident Response: Investigating Computer Crimes (McGraw-Hill Osborne Media) by Chris Prosise and Kevin Mandia.

What constitutes an email security incident? An email security incident is anything that affects the confidentiality, integrity, or availability of email within an organization. Such an incident can be a virus outbreak, a spam flood, a hacker that has remotely compromised your Web mail server, an untrained user that has accidentally deleted his/her email database, or a malicious insider that has gained full access to everyone's email by cracking the passwords on your email server.

Incident Response Plan Elements

Consider including the following standard incident response procedures in your formal incident response plan. However, don't trust that these procedures will be sufficient for your organization when the time comes—tweak them based on the size of your organization, your email system configuration, and so on:

- After you obtain upper management support, develop a formal computer security incident response team (CSIRT) to effectively respond to email security incidents. Your CSIRT should have representatives from upper management, legal, and public relations in addition to technical staff.
- Determine whether you will want to launch a formal investigation with law enforcement officials if you suspect criminal wrongdoing. It is critical that you make this decision before an incident occurs. It is even more important to get to know your local, state, and federal cybercrime investigators.

- Determine what criteria or metrics you will use to assess whether an email security incident has occurred:
    - Antivirus software alerts
    - Email server not responding
    - Email database is gone
    - Suspicious content entering or leaving your email system
    - Log file alerts

☞ If you're going to potentially launch a formal investigation into an email incident, it's critical that you're already logging system usage and security alerts—turning on logging after the fact might not be admissible evidence in court.

- Determine who will be contacted and when.
- Document detailed contact information for every person involved.
- Specify steps outlining how you will analyze an incident:
    - Use forensics analysis tools
    - Have a public relations plan in mind—know what will be said about the incident and know who will say it—preferably an experienced PR person
    - Determine how evidence will be handled (such as the storage of log files) and who will have custody of the evidence. Again, it is critical to know local cybercrime investigators to help you prepare for these steps.

☞ The following list provides categories of useful email incident response tools. Make sure that you understand how to use such tools and have a plan for how they will be used before they're needed to actually respond to an incident:

- A network analyzer
- Antivirus software
- Personal firewall/IDS software
- A file hash utility
- A disk-imaging utility so that you can save a copy of the original hard drive(s)
- An email database examiner

- Specify procedures for how systems will be restored to their normal state:
    - How you will utilize your data backups
    - How you will utilize failover server(s) or facilities
    - How you will re-install software
    - Who will be brought in to help

- Document the incident.
- Have a follow-up meeting to go over lessons learned and update your incident response plan accordingly.

Tools and Resources

The following list provides resources related to email security including OS, Web server, and vendor-specific email server hardening tools as well as links to technical information about encryption.

Encryption-Related Sites

SSL and TLS: Designing and Building Secure Systems (Addison-Wesley) by Eric Rescorla at http://www.rtfm.com/sslbook

Public Key Cryptography Standards (PKCS) at http://www.rsasecurity.com/rsalabs/pkcs

The International PGP Home Page at http://www.pgpi.org

The GNU Privacy Guard at http://www.GnuPG.org

PGP Corporation home page at http://www.pgp.com

Miscellaneous Documents

National Institute of Standards and Technology (NIST) Special Publication 800-45: Guidelines on Electronic Mail Security at http://cs-www.ncsl.nist.gov/publications/nistpubs/800-45/sp800-45.pdf

IETF standard for email headers at http://www.faqs.org/rfcs/rfc822.html

Microsoft Security Resources

“Hardening Windows 2000” (SystemExperts) a white paper by Philip Cox at http://www.systemexperts.com/tutors/hardenWin2K.pdf

IIS 5.0 Baseline Security Checklist at http://www.microsoft.com/technet/security/tools/chklist/iis5cl.asp

Security Operations Guide for Exchange 2000 Server at http://www.microsoft.com/technet/security/prodtech/mailexch/opsguide/Default.asp

Microsoft Solution for Securing Windows 2000 Server at http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/default.asp

Securing Windows 2000: Step-by-Step (The SANS Institute) at http://store.sans.org/store_item.php?item=22

Windows NT Security: Step-by-Step (The SANS Institute) at http://store.sans.org/store_item.php?item=20

Apache Security Resources

Apache Security Configuration Document by InterSect Alliance at http://www.intersectalliance.com/projects/ApacheConfig/index.html

Apache Security Tips at http://www.megalith.co.uk/manual/misc/security_tips.html

Apache Week Security Links at http://www.apacheweek.com/security

UNIX and Linux Security Resources

Bastille UNIX/Linux hardening utility at http://www.bastille-linux.org

Real World Linux Security by Bob Toxen at http://www.realworldlinuxsecurity.com

Securing Linux—A Survival Guide for Linux Security (The SANS Institute) at http://store.sans.org/store_item.php?item=83

Novell GroupWise Security Resources

Novell GroupWise Best Practices Guide at http://www.novell.com/products/groupwise/bestpractice.pdf

Securing GroupWise at http://www.giac.org/practical/Leslie_Helou_GSEC.doc

Lotus Notes/Domino Security Resources

DominoSecurity.org at http://www.dominosecurity.org

Lotus Notes and Domino R5.0 Security Infrastructure Revealed (IBM) by Soren Peter Nielsen, Frederic Dahm, Marc Lüscher, Hidenobu Yamamoto, Fiona Collins, Brian Denholm, Suresh Kumar, and John Softley at http://www.redbooks.ibm.com/redbooks/pdfs/sg245341.pdf

Sendmail Security Resources

Sendmail.org tips at http://www.sendmail.org/tips

Incident Response Resources

CERT Coordination Center CSIRT development page at http://www.cert.org/csirts

NIST Incident Handling page at http://csrc.nist.gov/topics/inchand.html

InfraGard at http://www.infragard.net

Forum of Incident Response and Security Teams at http://www.first.org

Foundstone forensics tools at http://www.foundstone.com/resources/freetools.htm

Mares and Company forensics tools at http://www.maresware.com

Summary

In this chapter, I've outlined common email security concerns, provided tips for performing an email risk assessment, discussed how to determine whether email encryption is right for your organization, and offered guidelines for what to do when your email system is attacked.

Email security solutions need to leverage existing technologies on both the sender and receiver networks as much as possible. While designing (or redesigning) your email security infrastructure, remember to focus on balancing security and convenience. You don't want to lock down your environment to the point of inaccessibility and inefficiency on the part of your users. Additionally, you'll need to implement countermeasures to your email risks that make good business sense for your organization.

Email security is an ongoing process. An initial risk assessment and implementation of countermeasures is not enough. New threats and vulnerabilities arise practically every day, so you must be vigilant.

In Chapter 6, we'll explore methodologies that can help you manage your email system more effectively. I'll provide further coverage on policy development and management, user awareness, and the issues surrounding email storage, backups, and data retention.