Systems and Network Analysis Center
Information Assurance Directorate

Security Guidance for Using Mail Clients

OVERVIEW

The Challenge

Increasingly, email is becoming a prime avenue for exploiting vulnerabilities in computer systems. This is a function of both their growing complexity and spreading usage. Since attempts to limit those vulnerabilities have been relatively unsuccessful at best, users must act as the first line of defense.

The Solution

By following a few simple guidelines, users can significantly cut their risk of being exploited by common email attacks.

For more information:

www.microsoft.com/security

www.mozilla.org/security

General Issues

1. S/Mime and PGP. In order to encrypt and authenticate email with other users, you, and your correspondents must have a compatible security mechanism. The two current mainstream options are S/Mime and PGP. PGP has been implemented in a number of mail tools for years. Recently, S/Mime capability is spreading. Your choice depends on what your intended recipients use and whether you plan to make use of a Public Key Infrastructure (PKI). With PKI, S/Mime would be the clear choice. With S/Mime, you need to have a PKI certificate loaded in your mail client. With PGP, you usually need to generate and exchange RSA keys with your correspondents, though recently PKI functionality has crept in.

2. Secure mail reading. In many cases, incoming email is stored on a mail server and then retrieved using a protocol such as IMAP or POP. There exist secure versions of both these protocols, which use SSL to encrypt the authentication exchange. One of these two options should be used.

3. Plain text vs. HTML. Most mail clients can be set to send email in either plain text or in some sort of web format like HTML. Besides increasing the size of email massively, HTML also allows the insertion of any number of attacks and nuisance making problems. Unless you have an overwhelming need for web-enabled email, it should be turned off. Alas, it is enabled by default in some mail clients. Some mail clients can be set to automatically turn incoming HTML emails into plain text. In some situations, you may be forced to read incoming HTML mail as is. Some mail clients allow you to preview the message before actually opening it.

4. Remote Load of Images. Spammers, and other malicious types, often embed a remote image link in HTML email. Then, when the email is read, the sender can tell by the fact that the image was accessed that the email was read. This action should be blocked, especially for senders you don't know.

SNAC DoD,9800 Savage Rd Ft.Meade,MD 20755-6704 410-854-6294 DSN 244-6294 FAX: 410-854-7321 **www.nsa.gov/snac**

TOP TEN THINGS TO DO

1. Send Plain Text Email
2. Disable Executable Scripting Languages
3. Turn off Remote Imaging
4. Read HTML as Plain Text
5. Block Dangerous Attachment Types
6. Use S/Mime or PGP to send email
7. Update and patch mail & system software
8. Use spyware & virus scanners
9. Run Outlook & Outlook Express in the restricted zone
10. Access mail servers securely using Secure IMAP

5. Executable Scripting Languages and Formats. This is probably the most common mechanism for email-based attacks. Many scripts and data formats can contain executable content that triggers security issues in the mail client or underlying operating system. Aside from Outlook, most mail clients have very rudimentary functionality in this area. For example, in Thunderbird, only the execution of JavaScript in mail messages is handled. Outlook deals with attachment and format types almost obsessively.

6. SSL/TLS for outgoing mail. Now that STARTTLS is included in the standard SENDMAIL and EXCHANGE mail servers, it is becoming more common. If your outbound email server supports TLS (or SSL), it should be used. Since this is still relatively rare, the specific configuration actions will not be addressed here.

7. Patches and Updates. Both your mail application AND the underlying system it is running on must be kept up to date in security patches. If there is a trustworthy automatic update capability available, use it. It is especially important to be using a current version of Outlook and Outlook express as major security functionality has been added in recent years.

8. Firewalls, Virus scanner, and Spyware scanners. It is extremely important that incoming email be scanned for virus and spyware content at the perimeter to your network. The key is to religiously keep the scanner's malware signature database up to date. However, users often have no control on how thoroughly email is screened at the perimeter. Also, encrypted email cannot be scanned for viruses at the perimeter. So you should also be scanning your email and computer for malicious content.

9. Spam. Unsolicited email has grown from a minor nuisance to become virtually a denial of service attack. And it will only get worse. Some measures can be taken at the perimeter, like rejecting mail from non-existent domains. As a user, you can use the spam filtering capabilities included in many mail clients to divert most of the spam into separate folders. Alas, spam filters are not perfect so false positives and negatives will occur. Lastly, **NEVER REPLY TO SPAM!**

10. Windows Restricted Zone. Active content in Outlook and OE can be run in either the Internet Zone or Restricted Zone. Current versions use Restricted Zone by default. Settings should always be checked to ensure that this is the case.

SNAC DoD,9800 Savage Rd Ft.Meade,MD 20755-6704 410-854-6294 DSN 244-6294 FAX: 410-854-7321 **www.nsa.gov/snac**