Aplura, LLC
4036 Wildwood Way
Ellicott City, MD 21042
301-523-2110 (w)
410-864-8386 (f)

Focused Information Security
www.aplura.com

E-Mail (In)Security:

Risks of Sending Sensitive E-mail

Essay By: Daniel Deighton

November 23, 2009

Although the majority of today's e-mail users started embracing this form of communication within the last ten years, it has actually been around for nearly three decades. SMTP (the protocol used to send mail) was launched in 1981. Unfortunately, this underlying technology that makes up e-mail is showing its age with its lack of built-in security features. While this may have been acceptable when electronic messaging was conceived, today, with the significant number of active attacks, we must consider the security risks that threaten critical e-mail communication. Standard e-mail without additional security precautions is a poor tool for business communication with anything that requires confidentiality, integrity and accountability.

E-mail has too many shortcomings to list in this brief essay, therefore, we will focus on several issues which directly affect security when sending electronic messages. While these points are particularly valuable to business users, personal e-mail users can also benefit from this information.

Although there have been various improvements, SMTP remains a “clear-text” protocol. A clear-text protocol simply means that the data is sent unencrypted. In the case of SMTP, the unencrypted message can be read by anyone who is able to intercept it.

It may appear difficult to intercept an e-mail message, however, that is simply not the case. Using freely available software, it is trivial to capture the message from the sender's network, the recipient's network or any place in between. The Internet Gateway is a great place to intercept all e-mail going to or coming from an organization's network. A network sensor can literally siphon off a copy of every e-mail sent or received. In fact, commercial e-mail archivers exist to do exactly that.

Unfortunately, the risk of interception does not end when the message passes through the sender's Internet Gateway. Since the message is unencrypted, any entity between the sender and the recipient could potentially view that message. This includes technicians at all of the ISPs involved, technicians at any of the telephone companies involved, staff in any of the buildings who have access to the data-lines, and any of the administrative staff of the recipient's network. Additionally, a compromised system could expose any e-mail message that passes through to the attacker who controls the system.

Not only can an e-mail message by viewed by a third party, it is also possible for the message to be altered in transit which could compromise its integrity. This fact highlights another major flaw in the standard e-mail implementation, which is that SMTP lacks a way to determine message authenticity. Without message authenticity, there are several things you must consider when you receive a critical message such as: Who actually sent the message? Is the message intact or has something been changed in transit? Are the attachments the same files the sender intended to include in the message?

Risk Perspective

Today's standard e-mail implementations have no built-in method to ensure confidentiality or integrity of the message. Without these components, an e-mail message may be read or edited in transit, unbeknown to either the sender or the recipient. It is also quite possible that the message did not even originate from the stated sender. These unknowns could cause a problem since, in most organizations, e-mail is a critical tool used to exchange sensitive information.

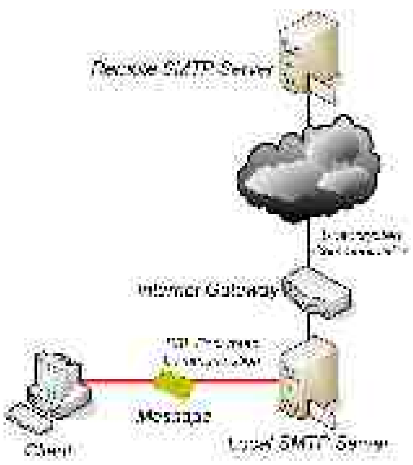

Figure 1: Sending E-mail

In order to reduce some of the risk, SMTP traffic can be encrypted with SSL, much like web traffic. When configured properly, modern e-mail clients can send the message in an encrypted form to the outgoing SMTP server.

Typically, SSL is only used between the client and the local SMTP server (see the red line in Figure 1). Transmission from the local SMTP server to the remote SMTP server is usually unencrypted (see the black line in Figure 1). Also, please note that SSL only encrypts the data while in transit. This means that the message can be read on any of the SMTP servers through which the message travels.

In order to effectively overcome these shortcomings, e-mail messages need to be sent in a secure manner. Encryption provides the confidentiality and integrity that is lacking in most e-mail solutions used today. Message signing guarantees the authenticity of the e-mail. Together, e-mail encryption and signing offer the best method to ensure that the message you sent is the one delivered to the intended recipient without being read by a third party along the way.

Two popular standards have emerged to provide encryption and signing capabilities within e-mail systems. PGP and S/MIME are often used and very well-supported by e-mail clients. Either of these solutions can provide confidentiality, integrity and authenticity of your e-mail messages. The choice between the two will often be determined by what your organization can support and what your recipients can accept. Unfortunately, both of these solutions require extra work to install and configure. Using these technologies require user training and additional steps when sending encrypted and/or signed messages. All of these things must be considered, when moving to an e-mail encryption solution.

Sensitive information should not be sent over e-mail when it is unencrypted. If encryption is not an option, an alternative form of communication, such as a phone call, fax, or traditional mail, should be used. These methods are not without their own risks, but they are often preferable to unencrypted e-mail.

With the insecurities and risks of e-mail, you should consider the types of data that you are comfortable sending over the Internet. Personally Identifiable Information (such as Social Security Numbers and unlisted phone numbers), passwords, credit card numbers and any other sensitive information should be encrypted when sent over e-mail. If you choose not to use a secure e-mail solution, assume your e-mail messages will be read by a third-party. With this thought in mind, you will be able to assess the sensitivity of your information and make an educated decision on whether or not to send it through e-mail.

Resources

- Simple Mail Transfer Protocol - http://tools.ietf.org/html/rfc5321
- OpenPGP Standard - http://tools.ietf.org/html/rfc4880
- S/MIME Message Specification - http://tools.ietf.org/html/rfc3851