Global Information Assurance Certification Paper

Sean Stark
December 21, 2000

Secure Messaging

Introduction

There was a time when business-to-business secure messaging meant licking the envelope, hiring a courier and stamping a big red "confidential" on it prior to being sent. Those days soon to be long gone. Today, businesses are demanding that their IT departments provide them with a means to send highly confidential documents and information across highly efficient digital mediums. Currently only 5-10 percent of electronic messages are encrypted, yet the information being transmitted may include legal documents, customer information, trade secrets, etc. Regardless of the type of information being sent, it must travel from the sender to the intended recipient without being viewed or tampered with by unauthorized individuals. When implemented properly, this can be accomplished through policies and applications.

Policy

Even though most IT departments are busy enough just trying to maintain day to day operations and support the needs of the business, policy is a necessity to ensure security in an organization. This also holds true for secure messaging. Policies need to be established in order to maintain order and continuity for any secure messaging system. They also outline acceptable and unacceptable behavior so that employees can be appropriately reprimanded. These policies should be comprehensive, specific to the business, and specific to the technology implemented. Some examples of what secure messaging policies can include are:

- Proper use of company messaging systems
- Communication of trade secrets
- Proper handling of confidential documents
- Appropriate care/uses of customer/vendor information

System Solutions

In the world of secure messaging systems, there are basically three different ways of implementing it. They are 3rd Party proprietary systems, RSA's S/MIMEv2, and Pretty Good Privacy (PGP) from Network Associates. These systems are all similar since they are all implemented on the client side, yet they each use different certificate formats and encryption algorithms. These differences make them completely incompatible with each other.

A. PGP *(Pretty Good Privacy)*

PGP is a program that allows end users to encrypt files and e-mail messages.

Since its release in the early 1990s it has been a standard for sending and receiving encrypted e-mail. It is a public key based encryption scheme where each user generates a public and private key pair. The public key is used to encrypt messages for other users to authenticate messages. Once encrypted, the file can only be deciphered using the corresponding private key and pass phrase.

- PGP can be used on most computer platforms
- Can be used to encrypt files and e-mail messages
- Protected by a pass phrase created by the user
- Keys may be either 512, 768, or 1024 bits
- Uses digital signatures to authenticate senders and to ensure that the message has not been modified
- Relies on public encryption technologies

PGP is a very reliable method for encrypting files and e-mail messages. It's main drawback is its lack of certificate revocation and the heavy reliance of certificate management that is placed on the user. PGP will most likely remain fairly popular throughout the IT community, yet its widespread use as an enterprise-wide secure messaging system has yet to be seen.

B. RSA's S/MIMEv2

Secure Multipurpose Internet Mail Extension protocol (S/MIME) is becoming a very popular method of securing e-mail messages. Many large software companies including Microsoft, Netscape, Novell, and Lotus currently support S/MIME. In addition to e-mail, S/MIME is enabling secure messaging/communication for EDI systems, electronic commerce, and applications. S/MIME has some of the following features:

- Uses the industry-standard X.509 certificate and PKI
- S/MIME can be used on most computer platforms
- Reasonable cost of implementation

S/MIME is also very reliable. Its main drawback is that it requires a full implementation of a PKI with its use of external key management, similar to that of PGP. Additionally, recovery keys are not a standard part of a S/MIME implementation, which can create issues with archiving of messages or retrieving messages of terminated employees. With its strong support of many large software companies, the marketplace should begin to more widely adopt this method of secure messaging.

C. Third Party Outsourcing

The most widely used method of secure messaging in the marketplace is through outsourcing this functionality to a third party. Many application service providers (ASP) as well as secure messaging companies have begun to offer

secure messaging services on a subscription basis. These companies include ZixIT, Certia, CertifiedMail.com, PostX, Entrust, and Private Express.

- Secure messaging services can be accessed through “internet browsers, mail clients equipped with ASP-provided plug-ins, or ASP provided stand-alone secure mail clients”
- Remove burden of maintaining a PKI system internally
- No key management for end users
- Ease of use for end users (much like using normal e-mail)
- Third parties are being able to offer these services for a reasonable price

Although it is appearing that the best solution for many companies to ensure secure messaging is outsourcing functionality to a third party, there are still drawbacks that have hampered their widespread adoption in the marketplace. One reason is that these vendors have not made themselves well enough know in the marketplace, so many companies are not even aware of their services. Another reason is that many companies are reluctant to uses third parties for such sensitive application. However, the largest drawback to outsourcing of secure messaging systems is that there are no standards within the industry. No two service providers are using the same technical approach and they are not interoperable, which means users might need to use several different systems to ensure secure messages with different external parties.

Conclusion

In conclusion, secure messaging is and will continue to be a hot topic within the security and IT industry. There are currently many players and technologies out there striving to take control, yet in the end the winner or winners will be those that learn to work together and develop some standards amongst themselves. They will have to provide a quality service that ensures confidentiality, integrity, authentication, and non-repudiation of messages. Also, they must be provided in a cost-effective manner that will be easy for end users to adopt into their day-to-day business activities. Only time will be able to determine what the end result will be; yet, in the mean time, it will be a very interesting and exciting time to be involved in the security field watching these developments.

References

Backman, Dan. "PGP Grows Up." URL: http://www.networkcomputing.com/907/907fl.html (19 December 2000).

"Encryption for Secure Messaging." December 2000. URL: http://www.tda.ecrc.ctc.com/kbase/Encryption/encryp.htm (18 December 2000).

Hilton, Ron. "Secure Messaging." 7 November 2000. URL: http://www.sans.org/infosecFAQ/messaging.htm (19 December 2000).

Jackson-Higgins, Kelly. "E-Mail Security—Secure Messaging Moves Forward." (3 March 1999). URL: http://www.internetwk.com/trends/trends032999.htm (19 December 2000).

Kobielus, James. "Universal Secure Messaging will rely on Outsourcers." Network World. (11 December 2000).

"PGP Help Page." URL: http://www.research.umbc.edu/pgp/pgpmain.html (19 December 2000).

"Promises, Promises." URL: http://www. networkcomputing.com/920/920fl3.html (19 December 2000).

"What is Secure Messaging?." 31 October 2000. URL: http://www.ssimail.com/Secure_messaging.htm (18 December 2000).