SANS Institute
Information Security Reading Room

Securing E-mail

Sharipah Setapa

SECURING E-MAIL

By Sharipah Setapa

(As part of the requirement of GSEC Examination)

Table Of Contents

SECURING E-MAIL

By Sharipah Setapa

(As part of the requirement of GSEC Examination)

I. Introduction

Security has been an issue in mail from ancient times. Security is still important today. E-mail is as fast and casual as a voice phone call, but can be save and retrieved with infinitely greater efficiency than paper letters or taped conversations. Security in mail deals first with reliable delivery to the addressee. Security, that is confidential, reliable and known delivery is essential to the success of e-mail. In other words people will not use a mail system that they cannot trust to deliver their messages.

If you are receiving an order through e-mail, how do you determine if it's a legitimate order or a forged order? Unless a company has some type of authenticate system, it is almost impossible to tell a forged order/transmission from a legitimate transmission. The lack of security on the Internet has made it painfully obvious that important business information sent as e-mail can be intercepted by hackers or forged if measures are not taken to ensure privacy.

The fundamental mechanism for providing security for binary encoded messages in an open network is encryption. It enables us to emulate all of the control that we have historically relied upon. Encryption has become one of the main tools for security as more and more information travels over larger area networks. Public-key cryptography enables us to emulate not only envelopes but also signatures.

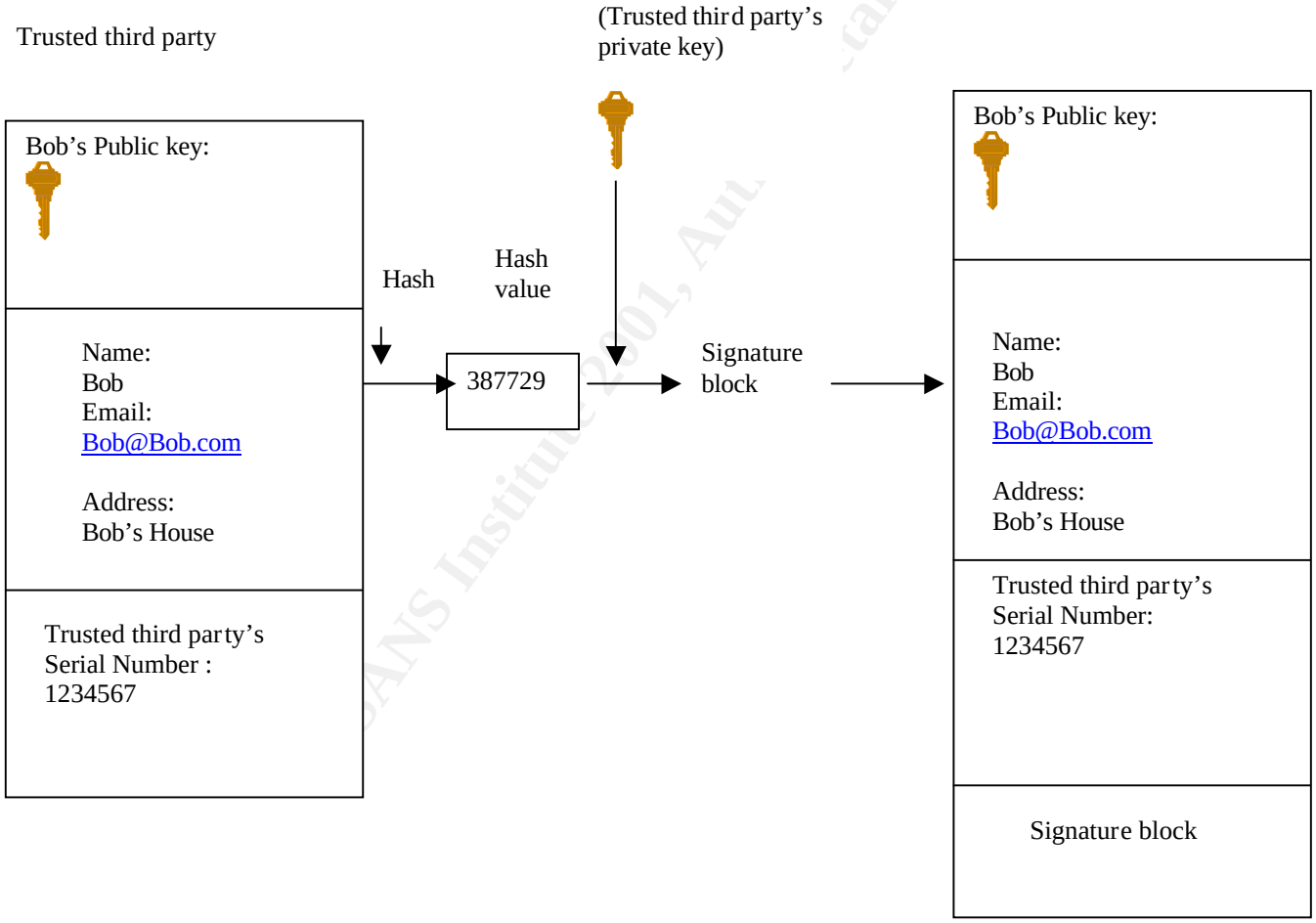
II. Encryption and Decryption

Encryption has become one of the main tools for security as more and more information travels over larger area networks. We encrypt messages using algorithms that are public and known-DES, IDEA, etc and secret keys. Assuming those algorithms are secure, then messages encrypted with them are as secure as the key. The security on an encryption algorithm is based on the security of the key. It is not based on the secrecy of the algorithm, the inaccessibility of the ciphertext, or even the inaccessibility of the plaintext. Assuming that the algorithm is a good one, its security is no more or no less than security of the key

In conventional cryptography, also called *secret-key* or *symmetric-key* encryption, one key is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystem Conventional encryption has benefits. It is very fast. It is especially useful for encrypting data that is not *going* anywhere.

However, conventional encryption alone as a means for transmitting secure data can be quite expensive simply due to the difficulty of secure key distribution. The problems of key distribution are solved by *public key cryptography*. Public key cryptography is an asymmetric scheme that uses a *pair* of keys for encryption: a *public key*, which encrypts data, and a corresponding *private,* or *secret key* for decryption.

How trusted third party creates a digital signatures for Bob using public key crytography



III. E-mail security program

An e-mail security program needed to provide

- Confidentiality
- Data origin authentication
- Message integrity
- Nonrepudiation of origin
- Key management

In an electronic-mail security program, there are a lot of links to worry about:

- Conventional(secret-key) algorithm for data encryption(e.g.:DES)
- Public-key algorithms for key management(e.g. RSA)
- Public-key algorithms for digital signatures(possibly a different algorithm than the one used for key management)(e.g.: RSA, DSA)
- Random-number generation, for use in generating keys for the conventional (secret-key) algorithm
- Prime-number generation, for use in generating public and private keys
- Storage of private and secret keys
- Key management procedures
- Thorough file erasure
- User interface

The conventional cryptographic algorithm should support a key length of at least 112 bits. The public –key algorithm should support a key length of at least 1024 bits. The answer of key size lies in the method attacker use to crack message that use encryption. The most common way to break encrypted messages is to use a method called "Brute Force attack".

Key generation is a lot harder than choosing and implementing an algorithm. Random-number generation on a personal is an enormous headache. Computer are supposed to be able to do the same task over and over again. Asking them to generate a random number is like asking them to produce a wrong and variable answer. It is possible, but it's very difficult.

Key management is also difficult. There are a lot of possible attacks against key, and a good system has to take them all into account. The system has to guard against false keys substituted for good ones, keys that are stolen, old keys being saved for later reuse, and perhaps a dozen other types of attacks.

IV. Applications

Although there is are no widely accepted electronic commercial standard for encrypted e-mail, this has not stopped software developers from developing software that attempt to address the e-mail security issues. The companies attempting to address this issue includes such as Expressmail, Pgpmail, Secure Mail, SecretAgent, Safe-Mail, PrivacyX, Stealth Message, YNN-Mail, HyperSend and Secure Messenger. It also includes some of the major players in the industry such as Microsoft and Netscape.

- **PGPmail** is a good choice for internet e-mail security. Since PGP is not S/MIME compliant, all receiving your e-mail must also be running PGP. The product originated before S/MIME existed and so sets its own standard. This disadvantage is reduced somewhat by the PEM's close integration with Windows 95 and all the major internal e-mail programs such as Microsoft Windows messaging, Netscape mail and Eudora. In this software a floating tool bar called the encrypter lets you encrypt, sign decrypt, and verify text in the clipboard. You can write your message in any work processor cut to the clipboard, encrypt it with a single button click, and paste it back in.

- **Expressmail** (Open Soft Inc). Expressmail's enhanced address book contain the public key for the recipient. Messages are decrypted seamlessly with Expressmail. If you are sending secure mail to recipients with and S/MIME e-mail client, or you can send along the bundle Decrypted applet. The product license per RSA requirement, lets you distribute one copy of the Decrypter for each licensed copy of Expressmail. This plug in for Microsoft Windows offers security that complies with the new S/MIME standard for interoperability interne e-mail encryption and authentication.

- **POTP Securemail** is offering an encryption scheme so unbreakable that it would violate US export laws were it a domestic company, Securemail from Elementrix Technologies, an Israeli company, has comprehensive features. Securemail offers quick, strong encryption and ease of use. Its use is not a good choice if interoperability is a requirement, because it's not S/MIME compliant.

- **SecretAgent** is a full featured e-mail security, but its lack of support for S/MIME hampers its utility for internet e-mail security. SecretAgent uses hybrid public key technology for encryption and signatures.. To use Secret Agent with Windows messaging you must leave the address portion of public key blank, set up an alias in your address book that matches the user ID portion of the public key and check the box for mail.

- **Safe-mail** is a secure free e-mail environment developed by Safe-mail Ltd. These features include secure bulletin boards, address book, organizer, real time secure

chats, auto-responds, POP3 mails, filters and chat rooms. It is a complete web-based solution that does require any installation, plug-in or cookies and need SSL-enabled browser.

- **PrivacyX** is an email system which uses anonymous digital certificates to provide maximum levels of privacy and security. It encrypt the e-mail's content, no one other than the intended recipient can open and read the e-mail.

- **Stealth Messages.** Email messages are passed through and stored on random servers, and can always be traced to the sender. Stealth Message gives you anonymous email with self-destruct options through your existing address, and it's also fun to use .

- **YNN**. The service is free and offers a numbers of security and encryption features. It's secure e-mail system is based on verisign's public key security and uses a 40-bit SSL browser encryption technology

- **HyperSend** is a secure delivery platform that provides fast and reliable file transfer through the Internet. As easy to use as email, HyperSend requires only a web browser to send files of any size with confidence. It's take care of interruptible downloads and works in the background while the user's computer is running other applications.

One of the first S/MIME compliant e-mail security programs was Secure Messenger. Secure Messenger includes plug ins for Microsoft e-mail clients and Eudora Pro 3.0 as well as stand alone encryption interface. The address book is organized by person rather than by key, allowing more than one key per person. This is useful because keys can expire or be withdrawn. Secure Messenger will automatically determine which key is valid. The down side of this program is this additional layer make the product a little harder to understand and use.

Most e-mail systems lack built in virus scanning and some use encryption that prevents built in virus scanning on the contents of the mail server. Some companies are now installing virus scanning software on their client and servers. Some security specialists view server based scanning products as a better alternative to desktop scanning alone because they detect viruses before the reach end users. It takes longer keys and more algorithms to be secure against all feasible attacks for at least several decades to come. The problem with this system is that some support staffs have reason to worry about the likely hood that users will encrypt files and then lose or forget their passwords.

V. Threats and Defenses

The most common methods of attack and how organizations can protect themselves should be known to every organization. Some of the threat and defenses are as follows. Masquerading or spoofing: an attacker pretends to be some else. Spoofing attacks can be used to enable one party to masquerade as another party. In such situation, a criminal can set up a storefront and collect thousands or billions of credit card numbers or other information from unsuspecting consumers. The result conjures up images of fly by night insurance companies and financial institutions beyond the reach of any regulatory body. The defense for this attack is authentication. By using an authentication agent or digital certificates, you force the user to prove his or her identity. Through authentication you ensure that only trusted users can engage in sessions.

The man in the middle and session hijacking attack occurs when an attacker inserts itself between two parties and pretends to be one of the parties. Defense:
Digital certificates or digital signatures. The best way to thwart this attack is for both parties to prove to each other that they know a secret that is known only to them. This is usually done by digitally signing a message and sending it to the other party as well as asking the other party to send a digitally signed message.

In eavesdropping an attacker listens to a private communication. The defense for this attack is encryption. In eavesdropping, the attacker views information as it is sent over the network, either with sniffer program or a vampire attack (a hardware attack that reroutes a portion of the network) by encrypting data, only the authorized recipient will be able to decrypt.

Data diddling is when an attacker changes the data while en route from source to destination. The defense for this attack is a decrypted message digest. An encrypted mess digest records random segment of the original message so that the receiver can compare the received message with the original. In an instance where information might be decrypted, altered, then re-crypted, an encrypted message digest provides a method of authenticating the integrity of the data.

Dictionary attacks are also common. A dictionary attack is when an attacker uses a large set likely combinations to guess a secret. For example, an attacker may choose one commonly used password and try them all until the password is determined. Defense: Strong passwords. Passwords that are not common name, words or references are harder to crack with a brute force attack such as a dictionary attack.

Denial of service occurs when an attacker floods the network or computer with hundred or even million of information or service request. Though the attacker does not benefit, service is denied to legitimate users. This is one of the most difficult attacks to thwart. The defense for this attack is authentication service filtering. By authenticating users on authenticated parties can send message.

VI. Method For Securing E-mail

There are various methods used in securing e-mail today. Although this process is continuing to evolve, the major current standards are secret codes, digital signatures, S/MIME and various plug in systems. Digital signatures perform a function in the electronic world similar to the function paper signatures in the real world. Since the private key of any function or entity is know only to key's owner, using the key is view as constituting proof of identity. This is a message encrypted using a user's private key, it can deduced that the message sent directly by the user. Critical to proper of public key's ability to match specific key to owners. To that end, public certificate are used. Another well known provider offer certificate are thawte (http://www.thawte.com) and verisgn (http://www.cibcverisign.com). These certificates of authority bind public keys to specific entities and allow for a third party to validate this binding.

Encryption can be used to check for tampering and forgery through a technique called digital signatures, or encryption using the sender's private key. To alert the recipient in case of tampering, the security program generates a mathematical summary of the message, called a hash.

The new S/MIME standard is attempting to add interoperability to the decryption standards. Consequently, you don't have to have to be running the same software. S-mime programs are interoperable. A message encrypted by one S/MIME compliant program can be decrypted by any other S/MIME program. Federal law currently regulates strong encryption algorithms and restricts their export. S/MIME has seen the greatest vendor support of late, with companies such a Netscape Communications, Network Computing Devices, Qualcomm, and FTP Software pledging to include S/MIME in forthcoming versions of their e-mail packages.

For now, S/MIME remains an industrial strength standard that is a de facto industry standard. In the meantime you can use a third party product like Pretty Good Privacy's PGPmail to encrypt your e-mail as long as your correspondent uses the same product.

Layering is another method of securing communications. The issue with layering is where to provide security in the layer. By far the more popular session layer protocol is the Secured Sockets Layer (SSL) a protocol for transmitting private documents via the Internet, first introduced by Netscape in late 1994. SSL is layered beneath application protocols such as HTTP, Telnet, FTP, Gopher, and NNTP, and layered above the connection protocol TCP/IP. This strategy allows SSL to operate independently of the Internet application protocols. With SSL implemented on both the client and server, using a combination of public keys and symmetric cryptosystems to provide confidentiality, data integrity, and authentication of the server and the client.

There are also several plug-in products for Microsoft Windows messaging Internet e-mail programs that support S/MIME and LDAP. When they become wide spread,

Internet e-mail security will be the norm rather than the exception. Plug-in enterprise security solutions that gives users secure access to information where ever it resides in the enterprise. It allows information technology executives to future proof network security by implement security today while planning migration paths. Customer can protect investments in security technology by relying on their new products dynamic current product family that hopefully articulate a migration path that incorporates future standards and technologies.

VII. Proposed Standards

Although there are many commercial standards attempting to become the industry e-mail encryption standard, currently there is no industry wide accepted standard. Major standards being proposed currently are MIME Object Security Service (MOSS), PGP/MIME, and Privacy Enhanced Mail (PEM). PGP and PEM are the original standards for securing e-mail. PEM was an early Internet Engineering Task Force (IETF) standard. PGP is not a IETF standard, but is probably the most popular security schemes in use for text messages. This product was designed to sidestep RSA 's monopoly on public encryption. The newest version will use other non RSA based encryption and authentication standards and will allow users to designate a trusted third party for authentication digital certificates, Although it still maintains the web of trust scheme as well.

VIII. Conclusion

The internet is the laboratory where security problem are researched and prototype solutions are conceived. The current state of e-mail communication makes it very clear that secure communications are necessary if an electronic based business is to take care of it's customers. Many of the protocols used in the Internet today should have stronger authentication mechanisms so that they are at least protected from passive attacks. The most frequently successful forms of attack do not rely on interception or cryptanalysis but instead attack areas which are not considered by the security policy.

E-mail security remains unstandardized and unstructured. Even though there are various software programs and schemes on the market to address this issue, most businesses can expend resources on stop gap measures until standards are uniform or do nothing at all. Companies are now forced to choose between hardware solutions such as firewalls or some of the various combination of non-interoperable software. It appears that the best strategy is to address e-mail security as a part of an overall security program that looks at a businesses entire security infrastructure. This method allows the company to address both long term and short term solutions

E-mail security will remain a very vital issue due to the growing number of business and the importance of verifying and preventing unauthorized sources from tampering

with the mail. The standards will eventually mature and reach the point in which e-mail security will be the norm. A good electronic e-mail security program is flexible. It should allow users to send unsigned encrypted messages, signed but unencrypted messages and signed and encrypted. The program should encrypt messages for storage. It should make it possible to send messages to a single receiver or to multiple receivers. The program should be available on all sorts of platforms. It is probably impossible to write one program that does everything, but it is a worthy goal. The more flexible a program is the more useful it is. Eventually, knowing all the threats and defense can serve the ultimate goal of the objective of this paper, which is to secure the e-mail to the lowest level as possible with proper defense mechanism. The ultimate goal of any electronic mail security program is to be ubiquitous. In general, however the security problems are not sufficiently severe to damage the system

IX. References

1."FREQUENTLY ASKED QUESTIONS – FAQs." Hosting and Internet Access URL:http://www.walkontheweb.com/faq/main_faq.htm

2.Tim Richardson . "Simple Notes on Internet Security and Email." May 28, 2001.URL:http://www.tim-richardson.net/misc/security.html

3. NISER/SANS KL. K.1, Information Security KickStart Highlights

4.Schneier, Bruce. E-mail security, How to keep your electronic messages private,(ISBN 0-471-05318-X) John Wiley & Sons,1999

5.Canter,Sheryl . "E-Mail Encryption." PC Magazine. The 1997 Utility Guide.URL http://www.zdnet.com/pcmag/features/utility/encrypt/_open.htm

6. "ExpressMail." OpenSoft Corp. 1997. URL: http://www.zdnet.com/pcmag/features/utility/encrypt/ueu2.htm

7."POTPSecureMail."ElementrixTechnologies Inc 1997.URL:.http://www.zdnet.com/pcmag/features/utility/encrypt/ueu4.htm

8. "Secure Messenger." Deming Internet Security.1997. URL:http://www.zdnet.com/pcmag/features/utility/encrypt/ueu6.htm

9. "SecretAgent." AT&T SecretAgent® Software. URL: http://www.att.com/secure_software/sa_sw.html

10. "PGPmail.", Pretty Good Privacy Inc. 1997.URL: http://www.zdnet.com/pcmag/features/utility/encrypt/ueu3.htm,

11."Security Protocol." Security on Internet " URL: http://www.ifs.univie.ac.at/~os/protokoll.html#Secure Socket Layer

12. Bondi, Richard. Cryptography for visual basic, A programmer's Guide to the Microsoft CryptoAPI, Wiley Computer Publishing.John Wiley& Son, Inc, 2000

13."Welcome to SAFe-mail,the secure free e-mail environment." URL: http://www.safe-mail.net

14."PrivacyX." PRIVACYX.COM CORPORATE,1998.URL: https://www.privacyx.com

15. "StealthMessage." StealthMessage.com. 2001.URL: http:// www.stealthmessage.com

16.”Ynn-mail.” MIBX Incorporated.1997 URL:
http://www.ynnmail.com
17. “Hypersend Secure Internet Delivery.” Hilgraeve Inc . 2001.URL:
http://www.my-hypersend.com