

E-mail Security Basics

By Jerry Lawson

lawson@netlawtools.com

© 1999-2000 Netlawtools, Inc.

<http://www.netlawtools.com>

Outline

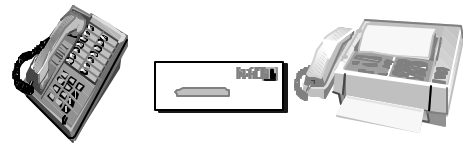
- ◆ Part I -- Why Is E-mail Security An Issue?
- ◆ Part II -- Overview of Encryption and Digital Signatures
- ◆ Part III -- Demonstrations

Part I:

Why Is E-mail Security An Issue?

Examining The Myths

E-mail Alternatives



Nothing Is Perfect, But ...

E-mail Is At Special Risk, Part A

- ◆ Hackers can usually intercept e-mail without excessive difficulty if they have a particular target.
- ◆ Key: take over or get close to mail server computer of sender or recipient.

Example: Taking Over Mail Server



[Visit Amazon.com](http://www.amazon.com)

- ◆ Book describes Price Waterhouse test of sophisticated corporate computer defenses
- ◆ It took hackers only 3 hours to get root access to mail server.
 - Not 3 hours to get one message, 3 hours to give them complete control over all e-mail going into or out of company.

E-mail Is At Special Risk, Part B

- ✦ E-mail spying is attractive to snoops because it is much less risky than alternative spying methods.
- ✦ Law enforcement lacks expertise & is overwhelmed by volume.

E-mail Is At Special Risk, Part D

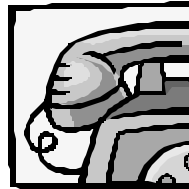
- ✦ New software makes it easier and cheaper to analyze large volumes of intercepted e-mail than intercepted phone calls, etc.
- ✦ Examples:
 - <http://www.assentor.com>
 - <http://www.sra.com>

E-Mail / Postcard Analogy



- ✦ Analogy actually understates the practical insecurity of e-mail where sophisticated snoops are involved.
- ✦ Software allows snooping process to be automated.

E-Mail / Telephone Analogy



- ✦ By comparison to e-mail snooping, installing & listening to voice wiretaps is risky and labor intensive.
- ✦ Effort needed to monitor one voice line could monitor all e-mail for hundreds of lawyers
- ✦ Amazon.com / Alibris example: [DOJ Press Release](#)

ABA Ethics Opinion Widely Misunderstood

Formal Opinion No. 99-413
March 10, 1999
Protecting the Confidentiality of Unencrypted E-Mail
<http://www.abanet.org/cpr/fo99-413.html>

ABA Analysis Issues

- ✦ ABA opinions not binding on any state.
- ✦ Covers only attorney client privilege
 - This privilege merely prevents use of information during court proceedings.
 - Has absolutely no effect on ability of snoops to use intercepted e-mail outside the courtroom.

ABA Analysis Issues, Part II.

- ◆ Basic technical errors reduce credibility of opinion.

ABA Analysis Issues, Part III.

- ◆ Opinion does not cover duty of confidentiality nor possibility of tort liability.
- ◆ Relevant to tort liability:
 - It's easier to provide a very high level of security for your e-mail than it is to protect your phone calls, faxes, snail mail, etc.
 - Cf. Learned Hand opinion in *U.S. vs. Carroll Towing Company*, 159 F.2d 169 (2nd Cir. 1947).

G. Burgess Allison On E-mail

- ◆ "Unless you've been targeted, your Internet e-mail should be at least as secure as a conversation in a crowded restaurant. (Oh, and a special note to high-profile Wall Street firms: You can assume that you've been targeted. Trust me.)"
- ◆ Source: ABA's Law Practice Management Magazine



Conclusion

Part II Encryption and Digital Signatures

Conventional Encryption

- ◆ Encryption = Scrambling by mathematical formula ("algorithm")
- ◆ One key ("password") encrypts
- ◆ Same key needed to decrypt
- ◆ Example: DES (Digital Encryption Standard) (56 bit key)



Public Key Encryption

- ◆ Uses Two Keys:
 - Public Key--can be distributed freely
 - Private Key--kept secret
- ◆ Keys Have Special Mathematical Relationship



Private Key



Public Key

Public Key Encryption, Cont.

- ◆ The Most Important Rule:
- ◆ A Message Encrypted With One Key Can Be Decrypted With The Other Key, and **ONLY** With The Other Key.

How It Works

- ◆ Sending A Message: Encrypt With Recipient's Public Key
 - You don't care if the message is intercepted in transit, because the body of the message will be scrambled (encrypted)
- ◆ Only the Intended Recipient Can Decrypt the Message
 - Because Only He Has The Corresponding Private Key

Public Key Advantages

- ◆ Easier Key Handling
 - No need for separate, secure channel to exchange a secret password
- ◆ Digital Signatures Possible

Digital Signatures: How They Work

- ◆ Simplest form of digital signature: Encrypt a message with your private key
- ◆ If your public key will decrypt the message, recipients will know that it could only have come from you

More Digital Sig. Functions

- ◆ "Message Digests" Allow:
 - Text of digitally signed message can be sent "in the clear"
 - Integrity of body of message can be verified
- ◆ Integrity Verification Not Readily Possible With Other Forms of Signature

Public Key Infrastructure (PKI)

- ◆ Public keys are verified and stored by a trusted third party.
- ◆ “Digital Certificate” = A public key that has been verified and digitally signed by a Certifying Authority (CA)
- ◆ Example: Verisign



Alternatives To PKI

- ◆ Digital Notaries
- ◆ “Web of Trust”

Part III Demonstrations

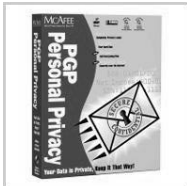
Demo One: Encrypting A Message

What Is Encryption?

Scrambling a message so that only the intended recipient can unscramble and read it.

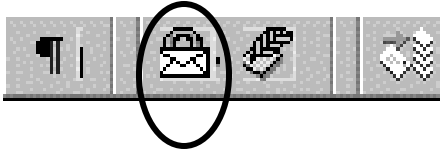
Tools Used

- ✦ Demo uses:
 - Eudora Pro e-mail program and
 - PGP for Personal Privacy Version 5.5
- (Newer version in stores, 6.5, costs about \$20)



Step 1: Press the icon for encrypting e-mail.

Enlargement



3 . COM>

Encryption icon is a combined envelope/lock.



After pressing the icon, a dialog box appears.

Selecting Recipient of Encrypted Message



Step 2: Drag and drop the names of the intended message recipients into the lower box, then press "OK" button.





A PGP Key “Fingerprint”

**FAEA 1F53 83B1 FB89 EA28
978A F174 DAF9 4EC7 C156**

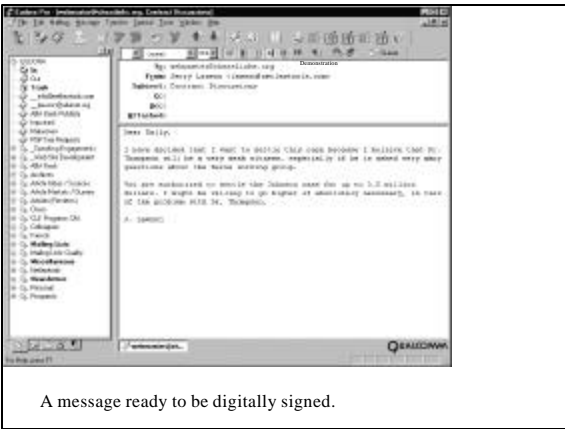
What Is It?
A shorter, mathematically derived representation of a PGP public key.

Purpose:
Used as a convenient aid to help verify that a particular public key belongs to a particular person.

Demo Two: Digitally Signing A Message

What Is Digital Signing?

Attaching a special authentication code to a message so that recipients will know it must have come from you, and was not modified in transit.

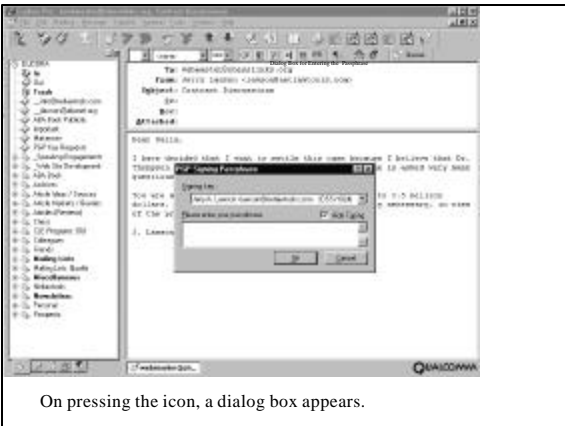


A message ready to be digitally signed.

The Icon for Digital Signing

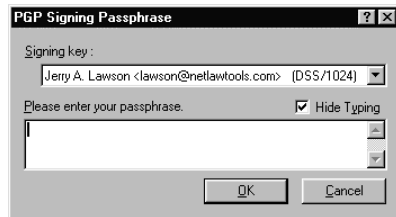
3 . COM >

Step 1: Press the digital signature icon.



On pressing the icon, a dialog box appears.

Your Passphrase Required to Sign A Message (Or Decrypt One Sent To You)



Step 2: Enter your passphrase and press the "OK" button.



The result: A digitally signed message.

Demo Summary

- ◆ Each operation, encrypting and digitally signing, took only two simple steps.
- ◆ In each case, icons and dialog boxes guide the user through those two steps.
- ◆ It doesn't get much easier than this!

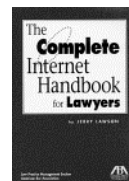
Related Procedures Not Shown In This Demo

- ◆ Encryption AND Digital Signature.
 - Just follow both procedures shown already
- ◆ Decrypting A Message Sent To You
 - Just click on decrypt icon and then enter your passphrase when prompted.

E-mail Security Summary

- ◆ Don't send sensitive info by e-mail without encrypting it.
- ◆ Encryption is very secure, IF
 - Good program used, and
 - Used correctly and consistently
- ◆ Modern software makes encryption easy.

More Information



- ◆ *Complete Internet Handbook for Lawyers* (ABA 1999), Chapter 15
- ◆ Internet Tools for Lawyers web site:
- ◆ <http://www.netlawtools.com>