How to make Secure Email Easier to use

Simson L. Garfinkel (MIT/Harvard)
Jeffrey I. Schiller (MIT)
Erik Nordlander (MIT)
David Margrave (Amazon)
Robert C. Miller (MIT)

Financial Services Technology Consortium Meeting,
November 30, 2006.
Originally presented at CHI 2005.
Public key cryptography was invented nearly 30 years ago to secure electronic mail.

- 1976 – Public Key Cryptography (Diffie & Hellman)
- 1977 – RSA Encryption (Rivest, Shamir & Adelman)
- 1978 – Certificates (Kornfelder)
- 1987 – Privacy Enhanced Mail
- 1992 – PGP
- 1998 – S/MIME

With so much work and investment, why don’t we use this exciting technology?
Most mail sent over the Internet isn’t secure. Why not?

Theories of Disuse

#1 People don’t have the software
#2 The software is too hard to use
#3 People don’t want to use it!
Most mail sent over the Internet isn’t secure. Why not?

<table>
<thead>
<tr>
<th>Theories of Disuse</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1 People don’t have the software</td>
<td>Distribute with the OS</td>
</tr>
<tr>
<td>#2 The software is too hard to use</td>
<td></td>
</tr>
<tr>
<td>#3 People don’t want to use it!</td>
<td></td>
</tr>
</tbody>
</table>
Most mail sent over the Internet isn’t secure. Why not?

<table>
<thead>
<tr>
<th>Theories of Disuse</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1 People don’t have the software</td>
<td>Distribute with the OS</td>
</tr>
<tr>
<td>#2 The software is too hard to use</td>
<td>Make it automatic</td>
</tr>
<tr>
<td>#3 People don’t want to use it!</td>
<td></td>
</tr>
</tbody>
</table>
Most mail sent over the Internet isn’t secure. Why not?

<table>
<thead>
<tr>
<th>Theories of Disuse</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1 People don’t have the software</td>
<td>Distribute with the OS</td>
</tr>
<tr>
<td>#2 The software is too hard to use</td>
<td>Make it automatic</td>
</tr>
<tr>
<td>#3 People don’t want to use it</td>
<td>Automate &amp; Educate</td>
</tr>
</tbody>
</table>
Most mail sent over the Internet isn’t secure. Why not?

<table>
<thead>
<tr>
<th>Theories of Disuse</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1 People don’t have the software</td>
<td>Distribute with the OS</td>
</tr>
<tr>
<td>#2 The software is too hard to use</td>
<td>Make it automatic</td>
</tr>
<tr>
<td>#3 People don’t want to use it!</td>
<td>Automate &amp; Educate</td>
</tr>
</tbody>
</table>

This is what the industry did with SSL/TLS, and it worked pretty well.
“Email Security” means different things to different people.
“Email Security” means different things to different people.

Email security traditionally meant:

- Preventing Eavesdropping.
- Sealed for the recipient.
“Email Security” means different things to different people.

Email security traditionally meant:

- Preventing Eavesdropping.  Sealed for the recipient

Today email security means:

- Stopping Spam and Phishing.  Signed by the Sender

This creates an opportunity for advancement, because there are some senders that send a lot of mail.
S/MIME was standardized in the 1990s...

To: simsong@acm.org
From: simsong@mit.edu
Subject: Message subjects are not signed, either
Content-Type: multipart/signed;
    boundary="---xxx---"

---xxx---
Content-Type: text/plain
This is a signed message.

---xxx---
Content-Type: application/pkcs7-signature;
    name=smime.p7s
    Content-Transfer-Encoding: base64
MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIIGQTCCAvowggJjoAMCAQICAw0E
ZzANBgkqhkiG9w0BAQQFADBiMQswCQYDVQQGEwJqQTElMC
...
LjEsMCoGA1UEAxMjVGhhd3RlIFBlcnNvbmFsIEZyZWN0
---xxx---

Message Header
(RFC 822)

Message Body

S/MIME Signature
and Digital ID
(43 lines; not to scale)

Signed Message
S/MIME was standardized in the 1990s...

To: simsong@acm.org
From: simsong@mit.edu
Subject: Message subjects are not encrypted
Content-Type: application/pkcs7-mime;
    name=smime.p7m
Content-Disposition: attachment;
    filename=smime.p7m

Message Header
(RFC 822)

S/MIME Message
Encrypted MIME
(75 lines; not to scale)

Sealed Message
S/MIME is built into many modern email programs.

Just click “sign” to sign and “encrypt” to seal.
You cannot send digitally signed messages because you do not have a digital ID for this account.

Get Digital ID  Cancel
A Digital ID is needed to send signed mail or receive sealed mail...
You have to get this from a trusted authority.
We *think* S/MIME clients are widely used...

... but until now, we didn’t have answers to some important questions:

- Can people receive S/MIME-signed messages?
- Do they understand what a signed message means?
- What other security measures are possible today?
Outline of this talk

✔ Background on “Email Security”.
  • Survey Results: Merchants understand and can use technology that’s already deployed.
  • Improving Web Mail Security.
  • Moving forward with Key Continuity Management.
Mail Security Survey.

In June 2003, Amazon.COM started using S/MIME to sign the VAT invoices sent to its European Marketplace Sellers.


Amazon sent signed mail to Europeans, but not to other merchants.

This created an excellent opportunity for survey research.
We created a web survey and posted links to it in the Amazon Sellers Forums:

- 5 web pages; 40 questions
- 2 minutes per page
- URLs posted in:
  - US Seller’s Forum
  - European Seller’s Forum

Europe Sellers had received signed messages from Amazon. US Sellers had not!
Survey respondents:

- 1083 sellers clicked on the link
  - 470 submitted the first web page.
  - 417 (89%) completed all five pages.

- Sellers were very educated:
  - 26% advanced degree
  - 35% college degree

- Sellers were very computer literate:
  - 18% “very sophisticated” computer user
  - 68% “comfortable” using computers
Survey Outline

• Experience with sending and receiving secure mail.
• Mail clients used.
• Questions testing knowledge and understanding of encryption.
• Kinds of computers used.
• Appropriate use of signing and sealing. [FC’05 paper]
• Opinions of companies that send signed mail.
• Metaphors for digital signatures.
• Lots of comments.
More than half of our respondents read their mail with programs that support S/MIME

“Which computer programs do you use to read your email? Check all that apply:"

<table>
<thead>
<tr>
<th>Program</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlook Express</td>
<td>42%</td>
</tr>
<tr>
<td>Outlook</td>
<td>31%</td>
</tr>
<tr>
<td>AOL</td>
<td>18%</td>
</tr>
<tr>
<td>Netscape</td>
<td>10%</td>
</tr>
<tr>
<td>Eudora</td>
<td>7%</td>
</tr>
<tr>
<td>Apple Mail</td>
<td>3%</td>
</tr>
<tr>
<td>Mozilla Mail</td>
<td>3%</td>
</tr>
<tr>
<td>Lotus Notes</td>
<td>2%</td>
</tr>
<tr>
<td>Evolution</td>
<td>1%</td>
</tr>
<tr>
<td>Any S/MIME</td>
<td>54%</td>
</tr>
</tbody>
</table>

Total Responding 435
No Response (19)
But most people who have S/MIME support don’t know it!

<table>
<thead>
<tr>
<th>“Does your email client handle encryption?”</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Yes</strong></td>
<td>27%</td>
</tr>
<tr>
<td>+S/MIME</td>
<td>34% ***</td>
</tr>
<tr>
<td>-S/MIME</td>
<td>14% ***</td>
</tr>
<tr>
<td><strong>No</strong></td>
<td>5%</td>
</tr>
<tr>
<td>I don’t know</td>
<td>59%</td>
</tr>
<tr>
<td>+S/MIME</td>
<td>54% *</td>
</tr>
<tr>
<td>-S/MIME</td>
<td>66% *</td>
</tr>
<tr>
<td>What’s encryption?</td>
<td>9%</td>
</tr>
<tr>
<td>+S/MIME</td>
<td>7% **</td>
</tr>
<tr>
<td>-S/MIME</td>
<td>14% **</td>
</tr>
<tr>
<td>Any S/MIME</td>
<td>54%</td>
</tr>
</tbody>
</table>

*\( p < .05 \); **\( p < .01 \); ***\( p < .001 \)
Not surprisingly, few merchants digitally sign their mail.

<table>
<thead>
<tr>
<th>Response</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>I <strong>always</strong> send my email digitally signed.</td>
<td>2%</td>
</tr>
<tr>
<td>I <strong>sometimes</strong> send email that is digitally signed</td>
<td>4%</td>
</tr>
<tr>
<td>I <strong>rarely</strong> ... because it is <strong>not necessary</strong> for the kind of mail that I send.</td>
<td>19%</td>
</tr>
<tr>
<td>I <strong>usually don’t</strong> because I don’t care enough ...</td>
<td>10%</td>
</tr>
<tr>
<td>I <strong>don’t ever</strong> ... because I don’t know how.</td>
<td>45%</td>
</tr>
<tr>
<td>...don’t understand what you mean by “digitally signed.”</td>
<td>24%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
</tr>
<tr>
<td>Total Responses</td>
<td>453</td>
</tr>
<tr>
<td>No Response</td>
<td>(17)</td>
</tr>
</tbody>
</table>
Likewise, few merchants seal their mail with encryption.

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>I always send email that is sealed for the recipient.</td>
<td>1%</td>
</tr>
<tr>
<td>I sometimes send email that is sealed.</td>
<td>4%</td>
</tr>
<tr>
<td>I rarely ... because it is <strong>not necessary</strong> for the kind of mail that I send.</td>
<td>17%</td>
</tr>
<tr>
<td>I rarely ... because I just don’t care.</td>
<td>8%</td>
</tr>
<tr>
<td>I don’t ... because it is <strong>too hard to do</strong>.</td>
<td>6%</td>
</tr>
<tr>
<td>I don’t ... because I don’t know how.</td>
<td>41%</td>
</tr>
<tr>
<td>I don’t ... because I am worried that the recipient won’t be able to read it.</td>
<td>14%</td>
</tr>
<tr>
<td>I don’t understand what you mean by “sealed” or “encrypted.”</td>
<td>22%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
<tr>
<td>Total Responses</td>
<td>454</td>
</tr>
<tr>
<td>No Response</td>
<td>(16)</td>
</tr>
</tbody>
</table>
But Amazon’s merchants think business-related email should be signed and sealed!

<table>
<thead>
<tr>
<th>What should be digitally signed?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank or credit-card statements</td>
<td>65%</td>
</tr>
<tr>
<td>Receipts from online merchants</td>
<td>59%</td>
</tr>
</tbody>
</table>

What should be sealed with encryption?

<table>
<thead>
<tr>
<th>What should be sealed with encryption?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank or credit-card statements</td>
<td>79%</td>
</tr>
<tr>
<td>Tax returns or complaints to regulators</td>
<td>74%</td>
</tr>
<tr>
<td>Receipts from online merchants</td>
<td>47%</td>
</tr>
</tbody>
</table>

(After we explained what “signed” and “sealed” meant.)
More than a third of the merchants know how to sign their mail and think it is necessary, but they don’t do it anyway!

“I don’t because I don’t care.”

“I doubt any of my usual recipients would understand the significance of the signature.”

“Never had the need to send these kinds of emails.”

“I don’t think it’s necessary to encrypt my email & frankly it’s just another step & something else I don’t have time for!”

This was a surprise: most security professionals don’t think that users are this sophisticated.

Full survey details at
http://www.simson.net/smime-survey.html
Outline of this talk

✔ Background on “Email Security.”

✔ Survey Results: Merchants understand and can use technology that’s already deployed.
  
  • Improving Web Mail Security.
    
    • Digital signatures need to be more smoothly integrated.
    
    • “Walled Gardens” and webmail systems can provide stronger sender authentication.
  
  • Moving forward with Key Continuity Management.
S/MIME signatures are well-integrated in some mail clients.

Apple Mail:

From: marketplace-messages@amazon.co.uk
Subject: Your Amazon.co.uk Seller Fees VAT Invoice
Date: August 20, 2004 1:12:48 PM EDT
To: Simson L. Garfinkel <simsong@csail.mit.edu>
Security: 🔐 Signed

Outlook Express:

<table>
<thead>
<tr>
<th>From</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeffrey I. Schiller</td>
<td>Re: S/MIME survey</td>
</tr>
<tr>
<td>David Margrave</td>
<td>Re: proposed survey</td>
</tr>
<tr>
<td>Rob Miller</td>
<td>Re: survey so far</td>
</tr>
</tbody>
</table>
S/MIME signatures appear as attachments on non-S/MIME clients:

“I couldn’t open that file you sent me. What is it?”

Recommendation:
Don’t send signed mail to Hotmail, AOL, GMail...
Mail that is signed with a Digital IDs issued by unknown CA generates a scary warning.

“Security Warning: You have not yet made a decision about whether to trust the digital ID used to sign this message”

Recommendation: Don’t use self-signed Digital IDs or private CAs
Occasionally, signed mail gets corrupted

- Mailing lists add postscripts and advertisements.
- Virus scanners
- Firewalls strip signatures

“Security Warning: Message has been tampered with”

Recommendation: Pressure Yahoo to fix this problem!
Signed mail is the first step to secure mail. Sealed mail is the second step.

But we aren’t ready for it!

- 40% of people using *cryptography* in our survey didn’t know they needed to keep their private key!
- Keeping your private key is hard.
  - Must move private key when you switch machines.
  - Must not delete expired keys.

**Recommendation:**
Mail programs should unseal *before storing.*
Walled Gardens: Today’s web mail systems can provide significantly more security than they do.

AOL’s anti-phishing “blue mail” is official mail from AOL. Recommendation: Expand to other “trusted senders.”
AOL distinguishes between inside-mail and outside mail:

- Inside AOL
- Outside AOL

AOL should also:

- Distinguish internal mail from external.
- Verify S/MIME signatures
- Send messages signed.
Bridging the Gap with Key Continuity Management.

KCM automates what a security expert would do when faced with a self-signed certificate. (SSH Model)
We’ve actually tested KCM in the lab.

- Works against some attacks, not others.
- Download from [http://www.simson.net/johnny2.tar.gz](http://www.simson.net/johnny2.tar.gz).

Complete details at [http://www.simson.net/thesis/](http://www.simson.net/thesis/)
In Summary, here’s how to make secure email easier to use:

- Start sending signed mail now.
- Fix systems that break S/MIME signatures.
- Clients should store messages unsealed by default.

Web mail providers should:

- Start verifying S/MIME signatures.
- Visually distinguish inside mail from external mail.
- Digitally-signing outgoing mail (S/MIME, not Domain Keys).

Questions?