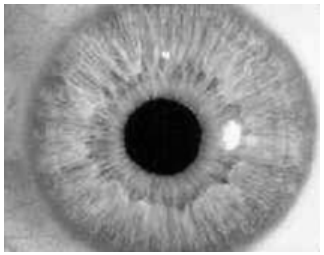
It has long been recognized that end-user security and usability are at odds in modern computer systems.

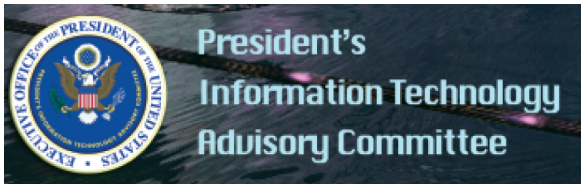


Username: simsong
Password: ••••••

ACCESS DENIED

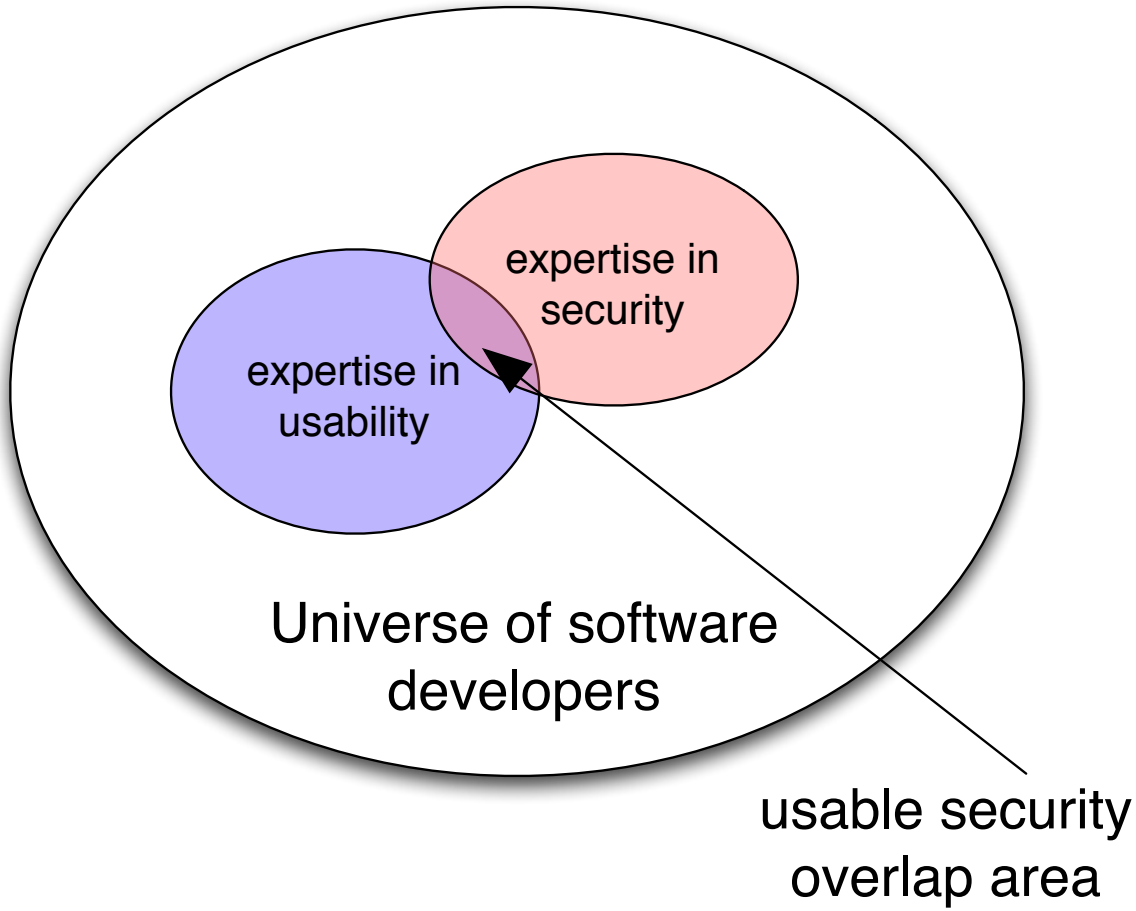
The need to align end-user security and usability is recognized as a priority for both computing and the nation.

- CRA 2003 “Grand Challenge”
- PITAC 2005 “priority”
- Special publications
  [IEEE S&P 2004] [O’Reilly 2005]
- CHI 2005; SOUPS 2005

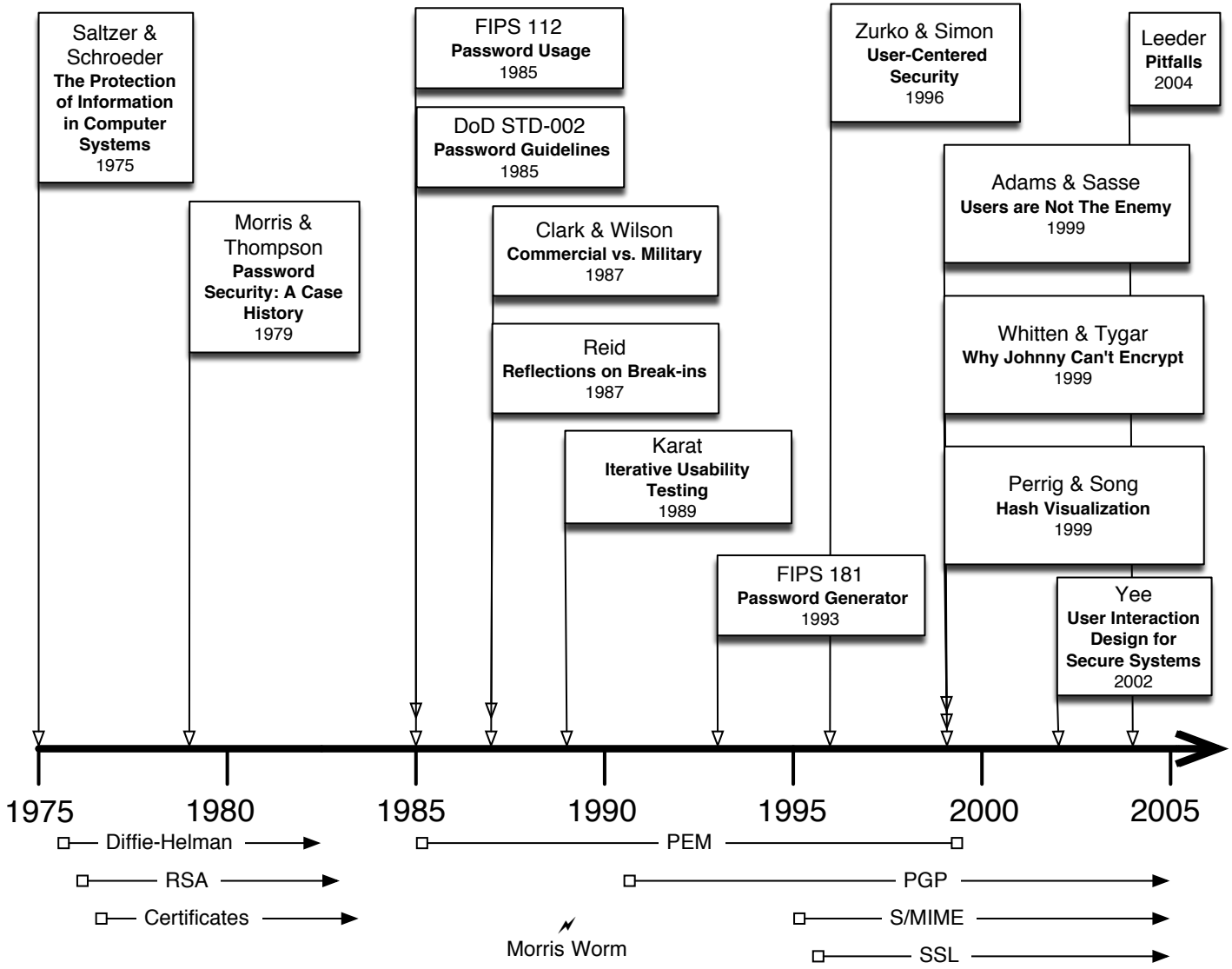


HCI-SEC is the emerging field that seeks to align Human Computer Interfaces with Security.

The root of the conflict: security and usability *must both be applied from the beginning*—but they are *different skills*.



HCI-SEC seems hard because little work has been done!



Work to date has focused on authentication and secure email.

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	Solution
#1	People don't have the software	Distribute with the OS
#2	The software is too hard to use	Make it automatic
#3	People don't want to use it!	Automate & Educate

This is what the industry did with SSL/TLS, and it worked pretty well.

Most work in email security has focused on encryption.

Email security traditionally meant:

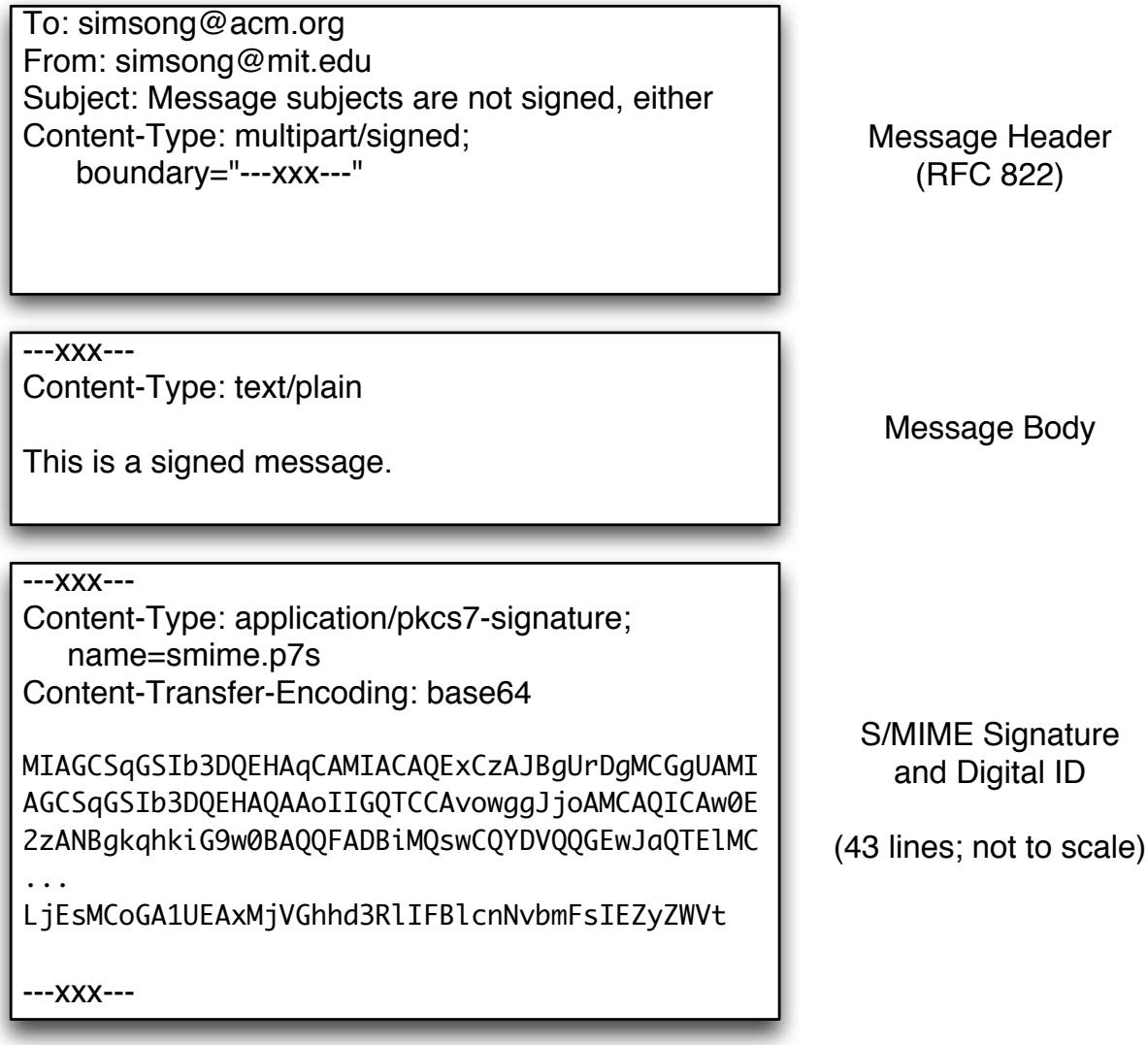
Preventing Eavesdropping. Recipients needs keys

Today email security means:

Stopping Spam and Phishing. Senders need keys.

By focusing on a few senders who send a lot of mail, we can make significant progress.

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



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)

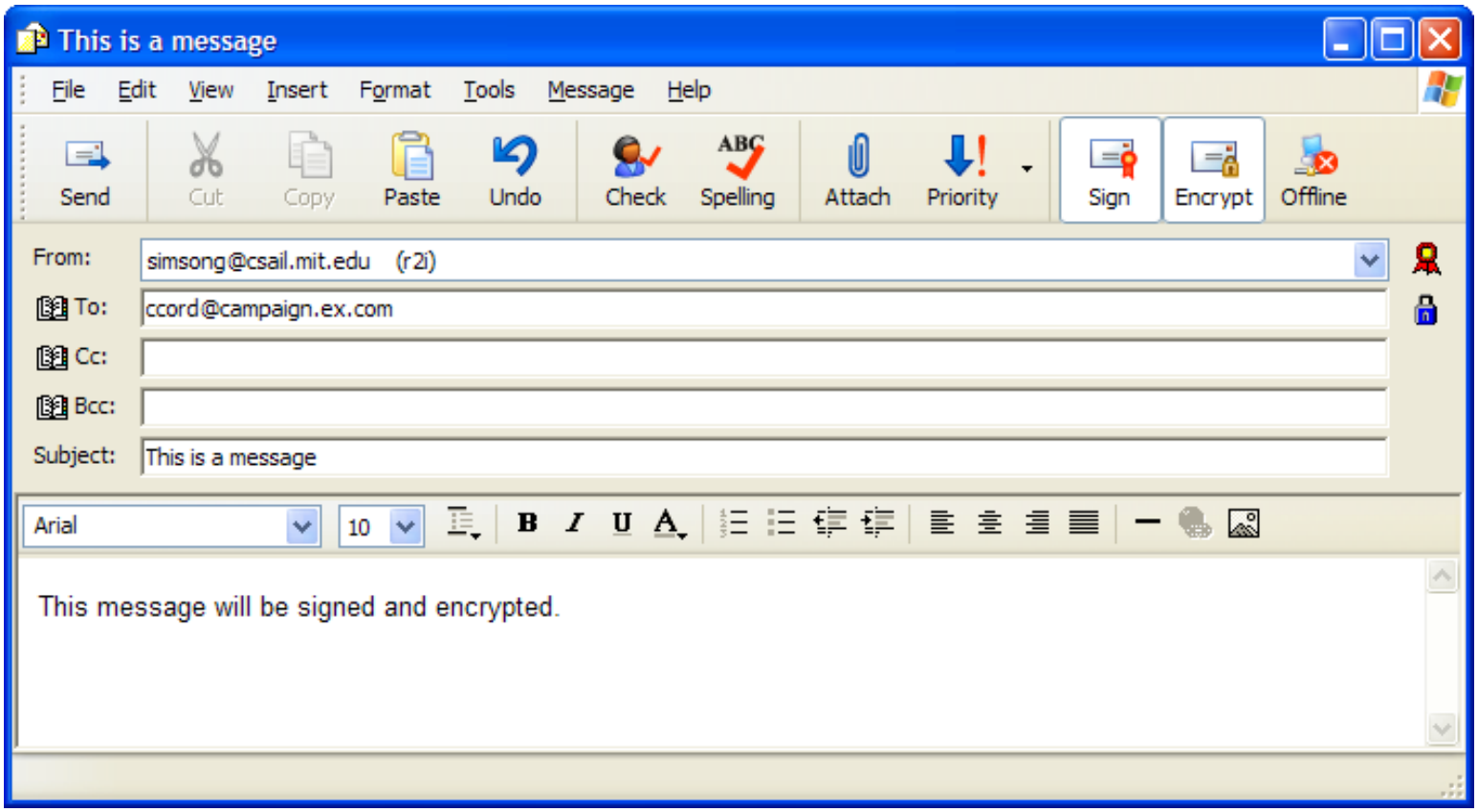
```
MIAGCSqGSIb3DQEHA6CAMIACAQAxggGFMIIBgQIBADBpMG
IxCzAJBgNVBAYTAlpBMSUwIwYDVQQKExxUaGF3dGUgQ29u
c3VsdGluZyAoUHR5KSBMdGQuMSwwKgYDVQQDEyNUaGF3dG
UgUGVyc29uYWwgRnJlZW1haWwgSXNzdWluZyBDQQIDDQTb
MA0GCSqGSIb3DQEBAQUABIIBALdHEexS9RbvmCo5G0nWZ4
HaQSCzgDDljjgvW7+4M0iPkuec+XE1nn4p5x+++2C0gReY
XvGC3ZEKgPsgFoQPGr0YXKHh3AHc1FN5DABcyVFwtc9xlq
VwZHNXJd24ltAq0V0oiX8rmJK1t3sn1haWwgSXNzdWluZy
BDQQIDDQTbMA0GCSqGSIb3DQEBAQUABIIBALdHEexS9Rbv
mCo5G0nWZ4HaQSCzgDDljjgvW7+4M0iPkuec+XE1nn4p5x
+++2C0gReYXvGC3ZEKgPsgFoQPGr0YXKHh3AHc1FN5DABc
yVFwtc9xlqVwZHNXJd24ltAq0V0oiX8rmJK1t3sns8UjjX
1dt2g+JZx9wMCZkKsu3b+6OOup4WGHYE6NxLLGzJWc6yTh
graizs4KUS8ujBm9rTIqc4VZ1+kJeKWbCC0UEuMZdcOgCU
vpCZkPr5C1XYuIDy6JWYjF2HaEUj7ecu12DB4u1oYljtVF
...
fLQRouON1ia2p5fTP6FqFNnjnTOIJNzPqwMmaV7jT2T98D
2mBAhklyg9h/6e4gAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
```

S/MIME Message
Encrypted MIME

(75 lines; not to scale)

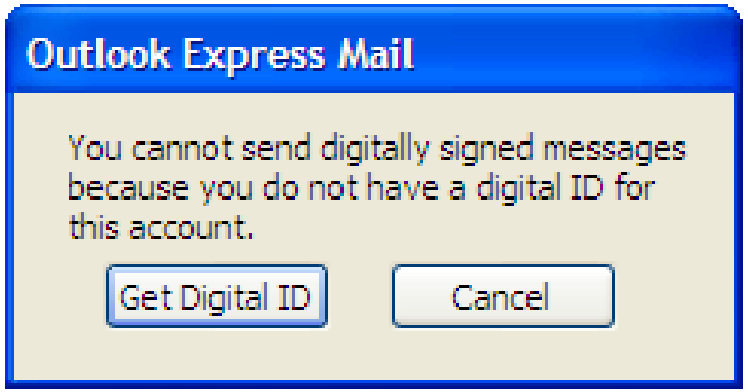
Sealed Message

S/MIME is built into many modern email programs.



Just click “sign” to sign and “encrypt” to seal.

But you need a Digital ID to send signed mail or receive mail that's sealed.



You have to get this from a trusted web site.

We *think* S/MIME clients are widely used...

... but until recently we didn't have answers to some important questions:

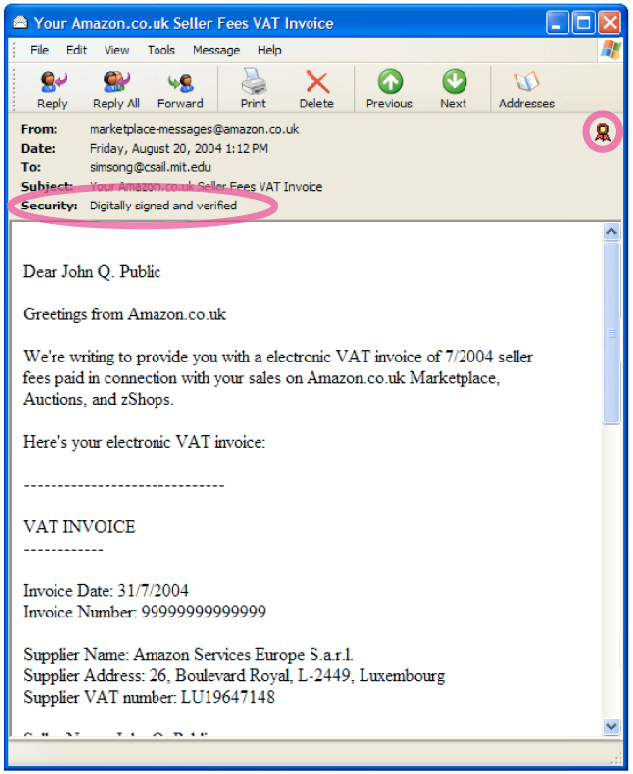
- Can people receive S/MIME-signed messages?
- Do they understand what a signed message means?
- What other security measures are possible today?

Garfinkel *et al.* Mail Security Survey.

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

EU Directive 99/93/EU calls for the use of “advanced digital signatures” for certain kinds of electronic messages.

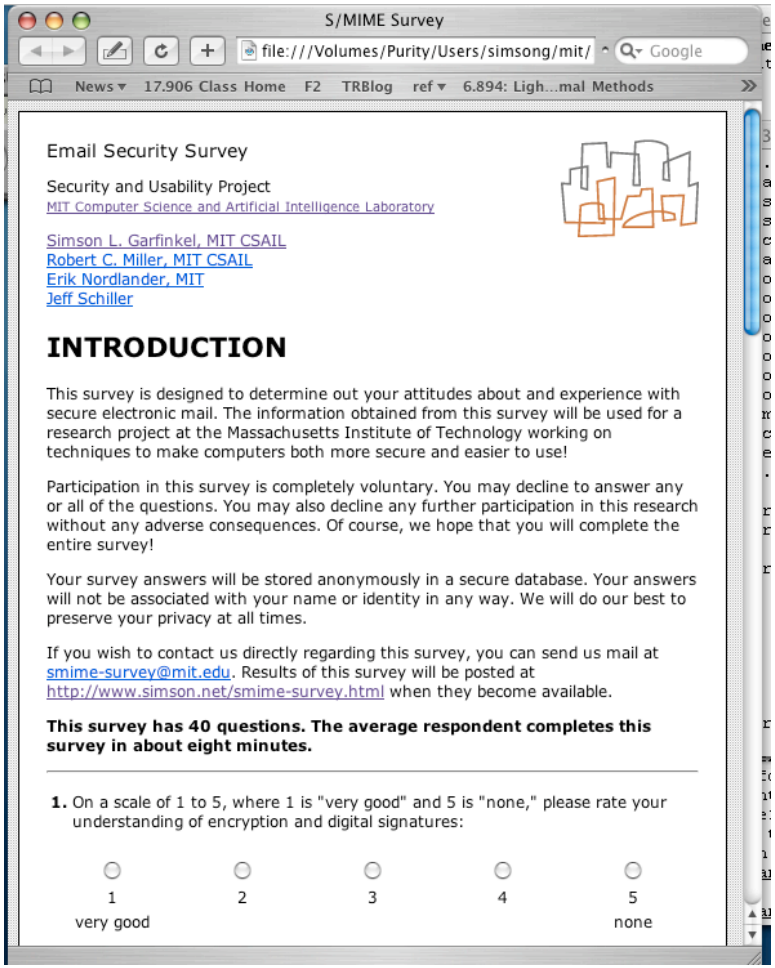
Amazon sent signed mail to Europeans, but not to other merchants.



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

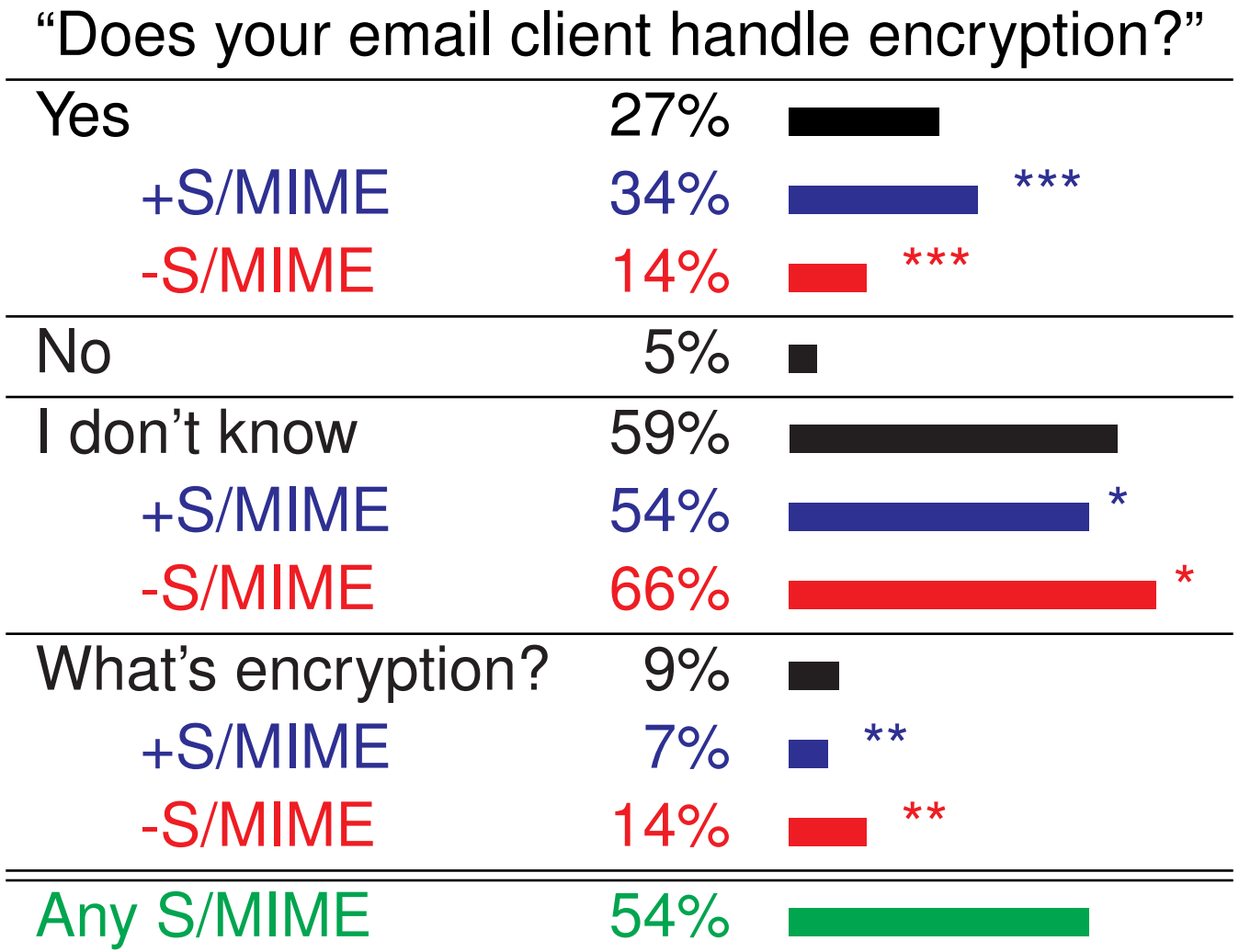
More than half of our respondents read their mail with programs that support S/MIME

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

Outlook Express	42%
Outlook	31%
AOL	18%
Netscape	10%
Eudora	7%
Apple Mail	3%
Mozilla Mail	3%
Lotus Notes	2%
Evolution	1%
Any S/MIME	54%
Total Responding	435
No Response	(19)

Eliminate AOL and Hotmail, and 90% of those remaining are S/MIME compatible.

But most people who have S/MIME support don't know it!



$^{*}p < .05; \quad ^{**}p < .01; \quad ^{***}p < .001$

Not surprisingly, few merchants digitally sign their mail.

I **always** send my email digitally signed.	2%	
I **sometimes** send email that is digitally signed	4%	
I **rarely** ... because it is **not necessary** for the kind of mail that I send.	19%	
I **usually don't because I don't care enough** ...	10%	
I **don't ever** ... **because I don't know how.**	45%	
...**don't understand what you mean** by "digitally signed."	24%	
Other	4%	
Total Responses	453	
No Response	(17)	

Likewise, few merchants seal their mail with encryption.

I **always** send email that is sealed for the recipient.	1%
I **sometimes** send email that is sealed.	4%
I **rarely** ... because it is **not necessary** for the kind of mail that I send.	17%
I **rarely** ... because **I just don't care.**	8%
I don't ... because it is **too hard to do**.	6%
I don't ... because **I don't know how**.	41%
I don't ... because I am **worried that the recipient won't be able to read it**.	14%
I don't understand what you mean by "sealed" or "encrypted."	22%
Other	3%
Total Responses	454
No Response	(16)

But Amazon's merchants think business-related email *should be signed and sealed!*

What should be digitally signed?	
Bank or credit-card statements	65%
Receipts from online merchants	59%

What should be sealed with encryption?	
Bank or credit-card statements	79%
Tax returns or complaints to regulators	74%
Receipts from online merchants	47%

(After we explained what "signed" and "sealed" meant.)

More than a third of the merchants know how sign their mail and think it is necessary, but they don't 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!"

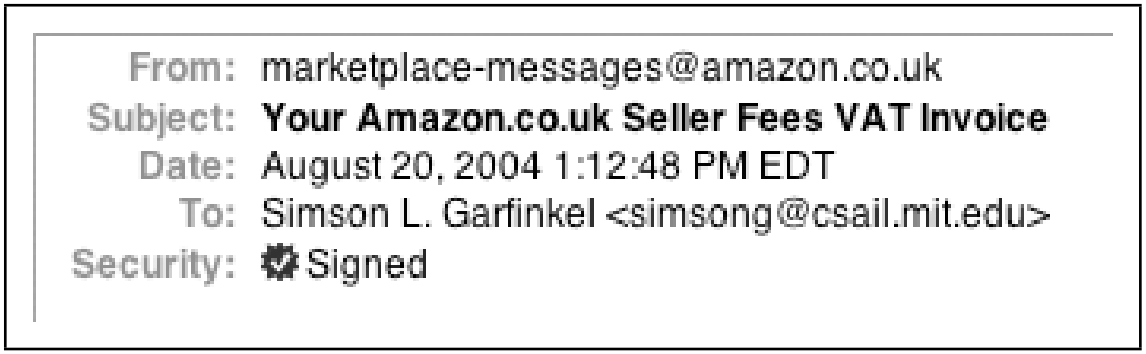
This was a surprise: most security professionals don't think that users are this sophisticated.

Full survey details at

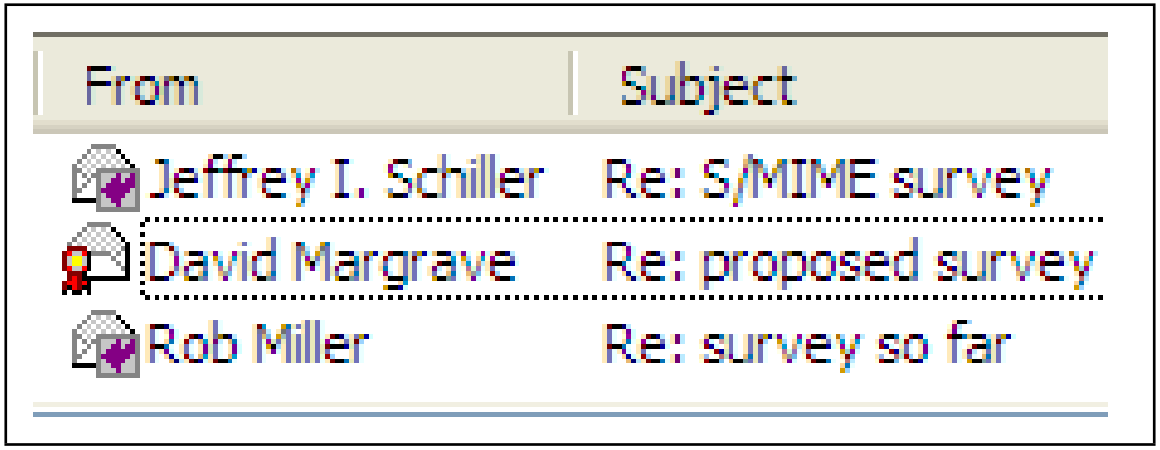
`http://www.simson.net/smime-survey.html`

S/MIME signatures are well-integrated in some mail clients.

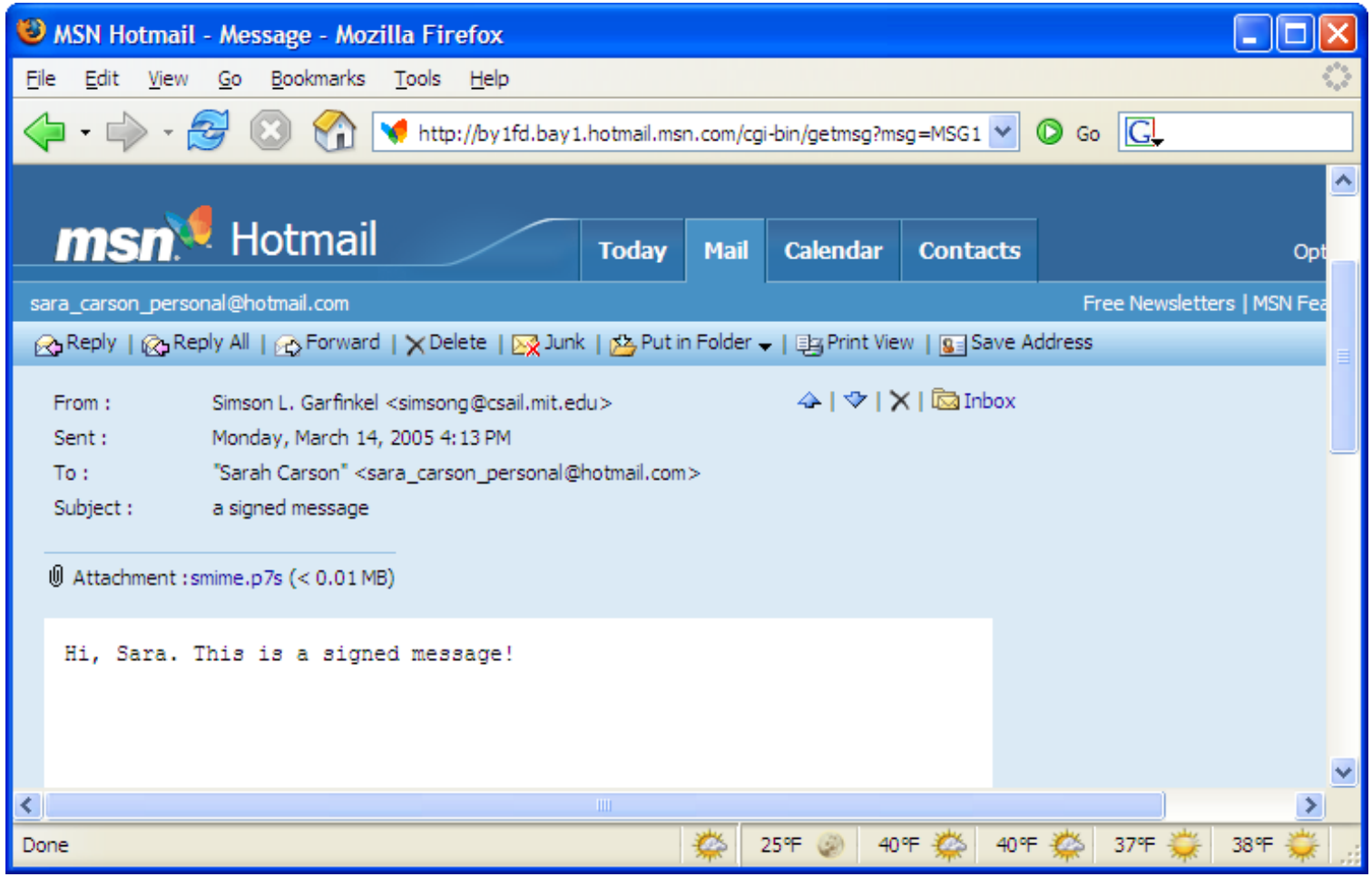
Apple Mail:



Outlook Express:



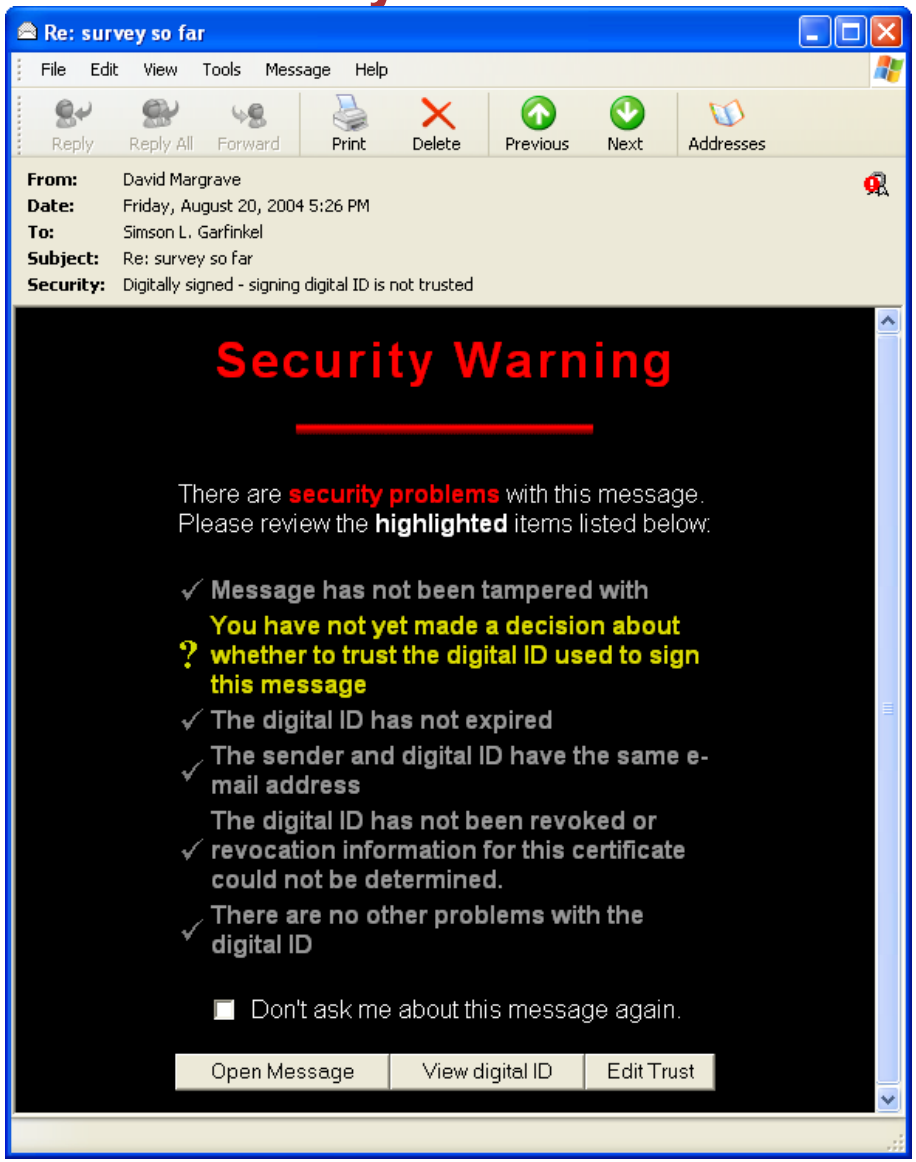
S/MIME signatures appear as attachments on non-S/MIME clients:



"I couldn't open that file you sent me. What is it?"

This is a problem results directly from the use of MIME multipart for signatures.

Mail that is signed with a Digital IDs issued by unknown CA generates a scary warning.

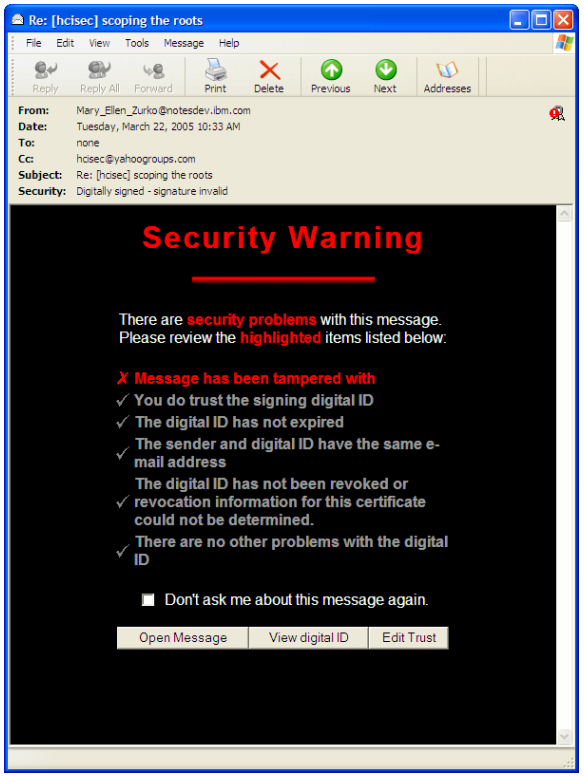


"**Security Warning:** You have not yet made a decision about whether to trust the digital ID used to sign this message"

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



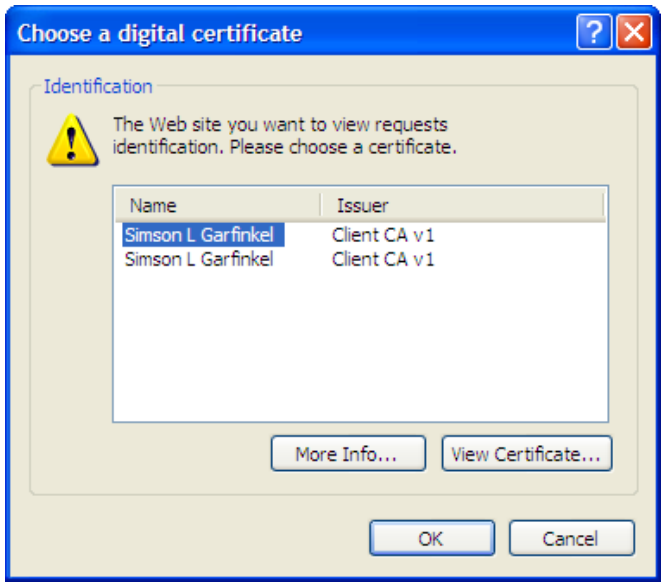
"**Security Warning:** Message has been tampered with"

Recommendation: Put pressure on YahooGroups and other providers to fix these problems!

Signed mail is the first step to secure mail. Sealed mail is the second step.

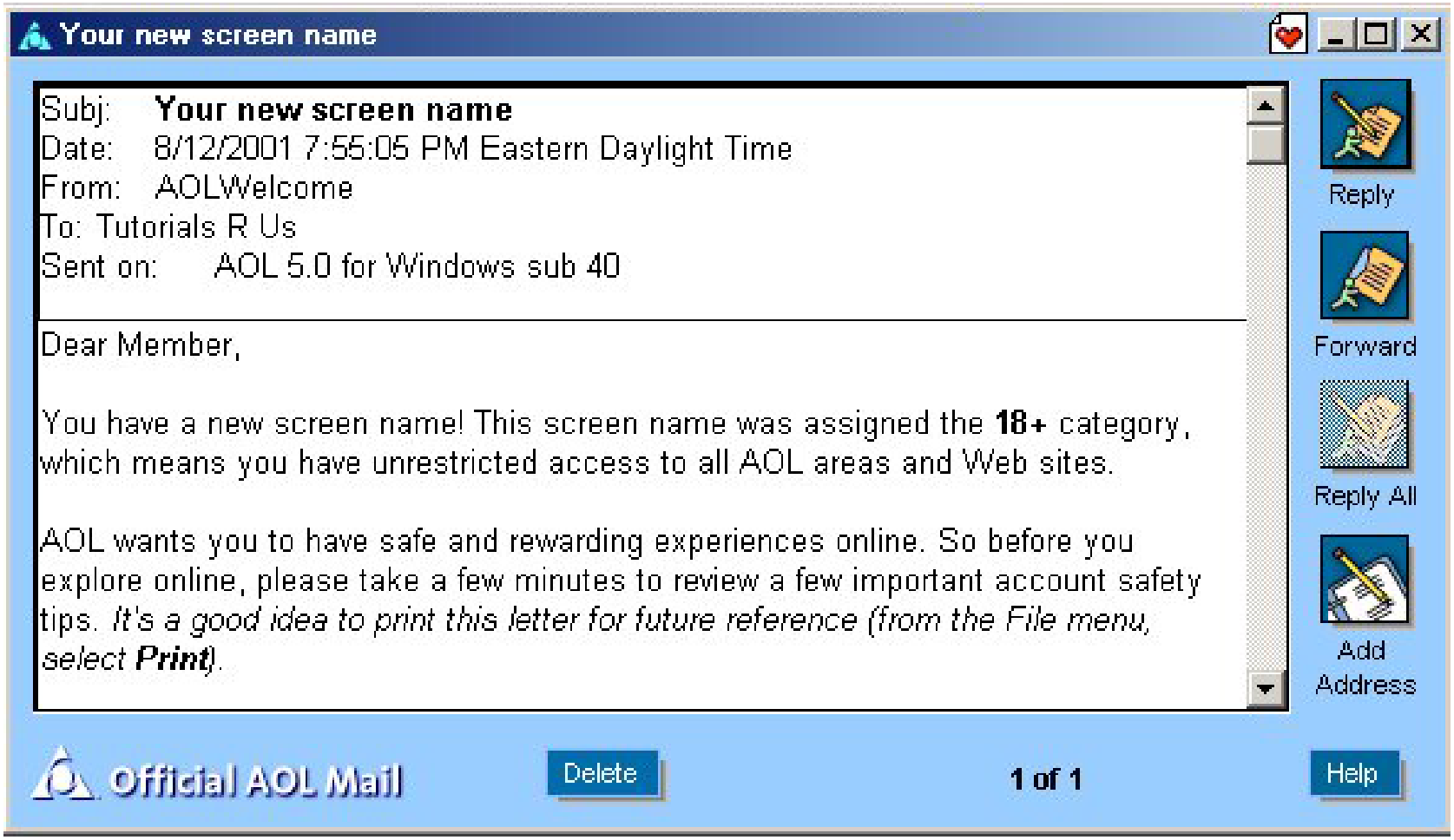
But we aren't ready for it!

- 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.



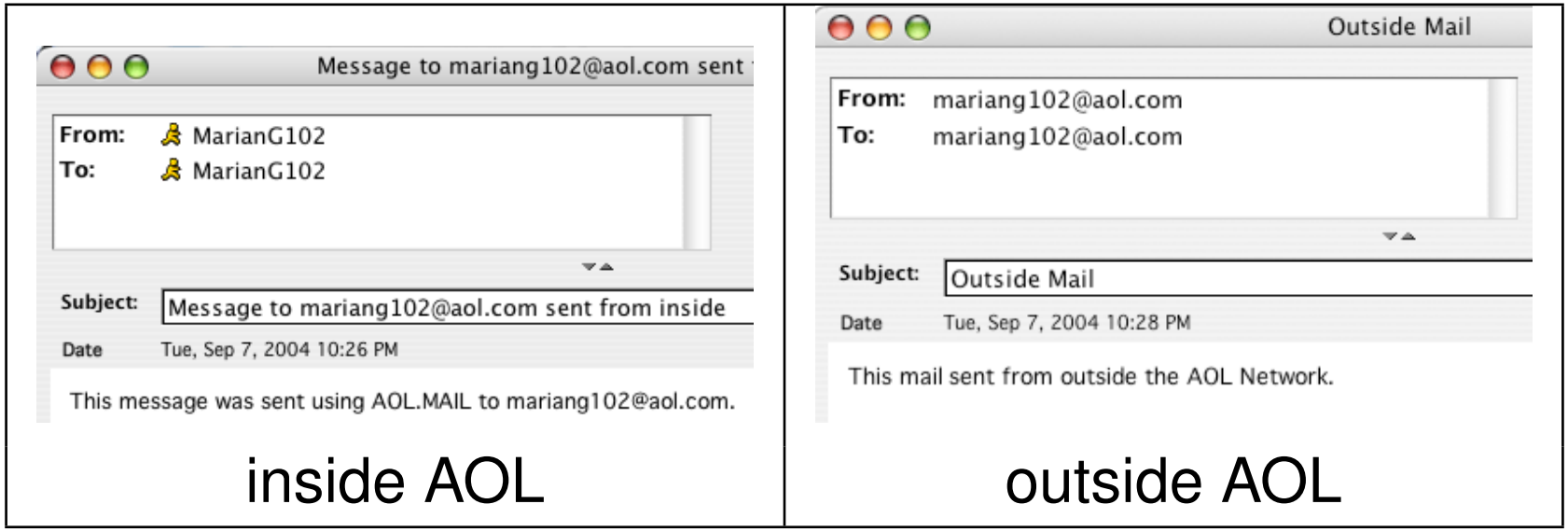
Recommendation: Mail programs should unseal *before storing*.

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.

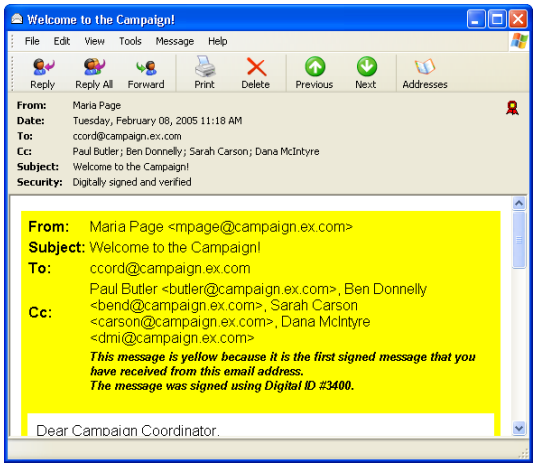
AOL distinguishes between inside-mail and outside mail:



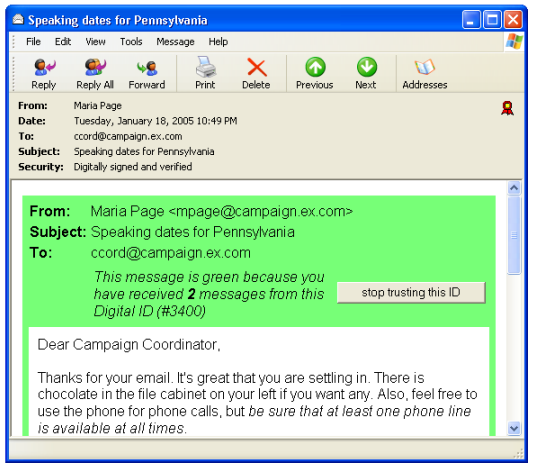
AOL should also:

- Distinguish internal mail from external.
- Verify S/MIME signatures
- Send messages signed.

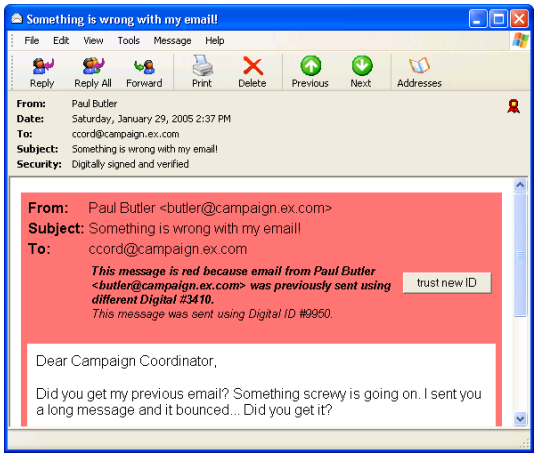
Bridging the Gap with Key Continuity Management.



FIRST TIME



OKAY!

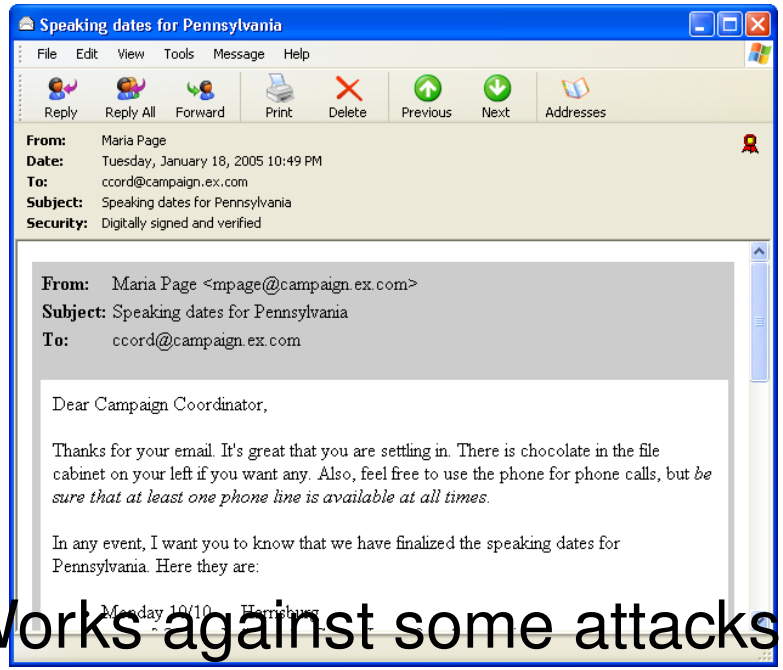


CHANGED.

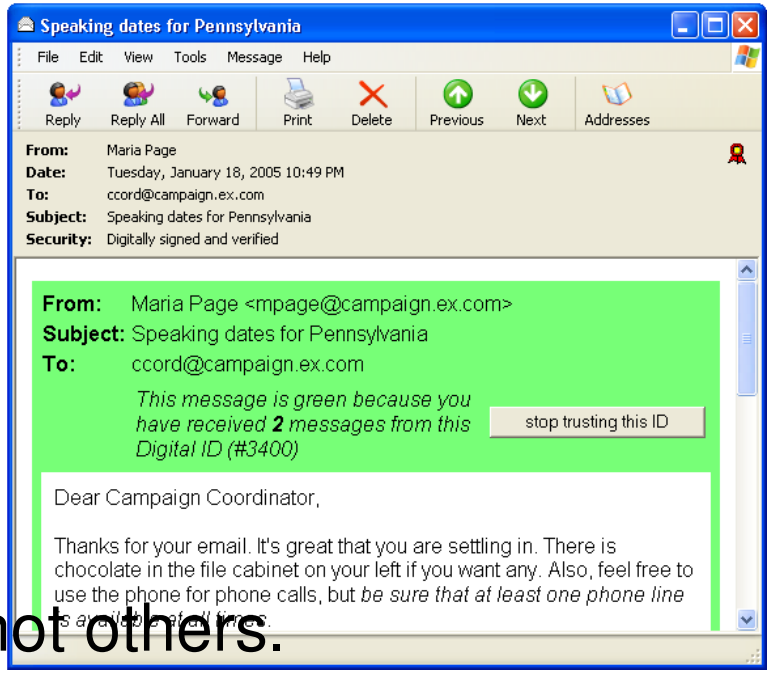
KCM automates what a security expert would do when faced with a self-signed certificate. (SSH Model)

We've tested KCM in the lab.

No KCM



KCM



- Works against some attacks, not others.
- Paper in the works.
- We're making the testing protocol available to others.

Complete details in [Garfinkel '05]

In Summary, here's how to make secure email easier to use:

- ✔ Start sending signed mail now, especially bulk-mailers.
- ✔ 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?