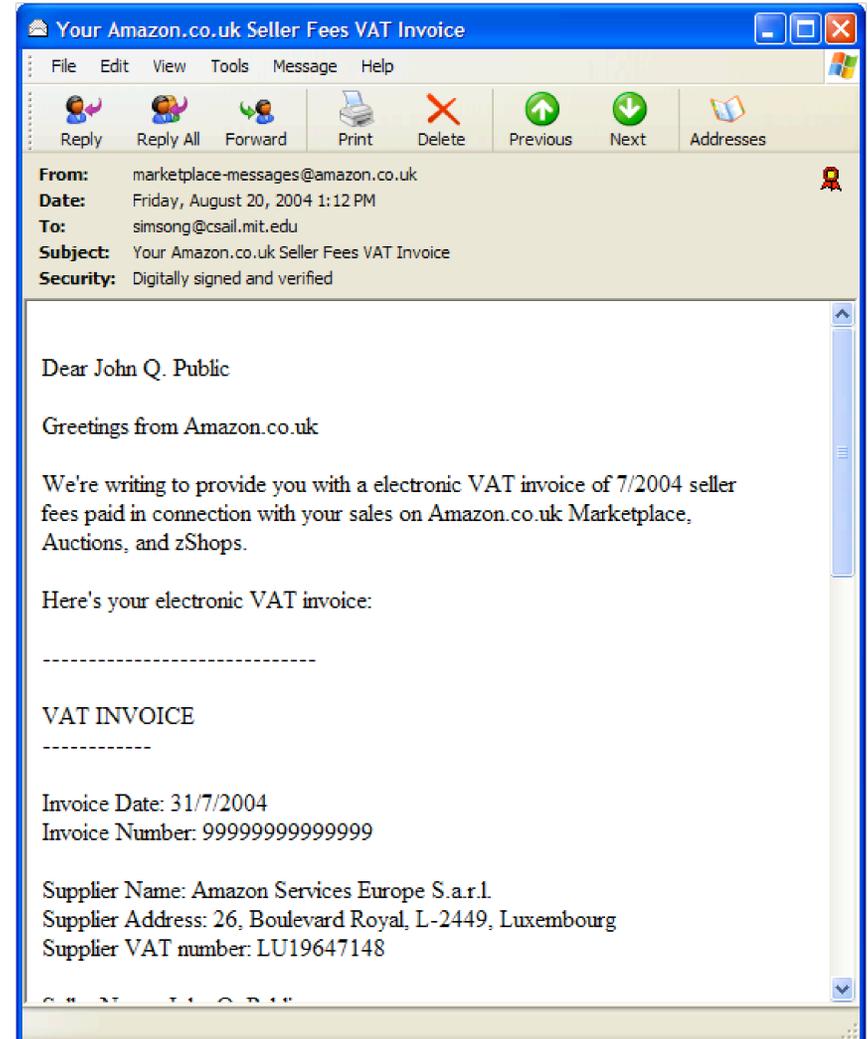


# How to make Secure Email Easier to use

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



<http://www.simson.net/smime-survey.html/>

## **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.**

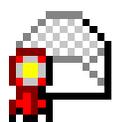
## “Email Security” means different things to different people.

■ 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---"
```

Message Header  
(RFC 822)

```
---xxx---
Content-Type: text/plain

This is a signed message.
```

Message Body

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

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGGUAMI
AGCSqGSIb3DQEHAQAoIIGQTCCAvoeggJjoAMCAQICAw0E
ZzANBgkqhkiG9w0BAQQFADBIMQswCQYDVQQGEwJaQTElMC
...
LjEsMCoGA1UEAxMjVGhhd3RlIFB1cnNvbWFsIEZyZWVt
---xxx---
```

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)

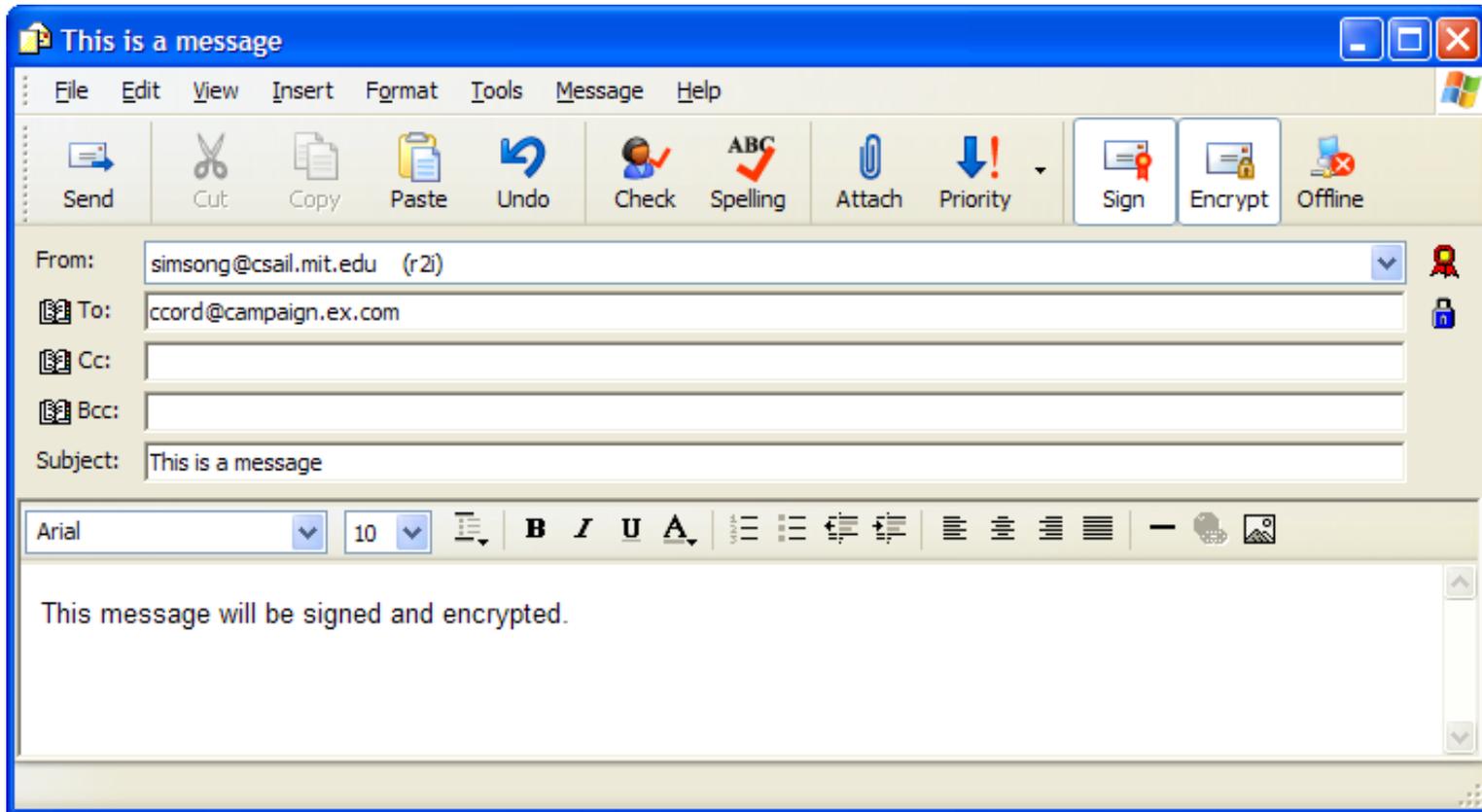
```
MIAGCSqGSIb3DQEHA6CAMIACAQAxggGFMIIBgQIBADBpMG
IxCzAJBgNVBAYTAlpBMSUwIwYDVQQKExxUaGF3dGUgQ29u
c3VsdGluZyAoUHR5K5SBMdGQuMSwwKgYDVQQDEyNUaGF3dG
UgUGVyc29uYWwgRnJlZW1haWwgSXNzdWluZyBDQQIDDQTb
MA0GCSqGSIb3DQEBAQUABIIBALdHEexS9RbvmCo5G0nWZ4
HaQSCzgDDLj jgvW7+4M0iPkuec+XE1nn4p5x+++2C0gReY
XvGC3ZEKgpSgFoQPGr0YXKHh3AHc1FN5DABcyVFwtc9xlq
VwZHNXJd24ltAq0V0oiX8rmJK1t3sn1haWwgSXNzdWluZy
BDQQIDDQTbMA0GCSqGSIb3DQEBAQUABIIBALdHEexS9Rbv
mCo5G0nWZ4HaQSCzgDDLj jgvW7+4M0iPkuec+XE1nn4p5x
+++2C0gReYXvGC3ZEKgpSgFoQPGr0YXKHh3AHc1FN5DABc
yVFwtc9xlqVwZHNXJd24ltAq0V0oiX8rmJK1t3sns8UjjX
1dt2g+JZx9wMCZkKsu3b+600up4WGHYE6NxLLGzJWc6yTh
graiZs4KUS8ujBm9rTIqc4VZ1+kJeKWbCC0UEuMZdc0gCU
vpCzkPr5C1XYuIDy6JWYjF2HaEUj7ecu12DB4u1oYljtVF
...
fLQRouON1ia2p5fTP6FqFNjnT0IJNzPqwMmaV7jT2T98D
2mBAhklyg9h/6e4gAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
```

S/MIME Message  
Encrypted MIME

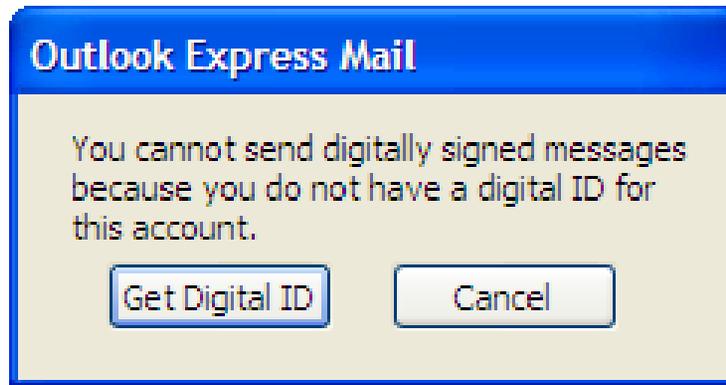
(75 lines; not to scale)

## Sealed Message

# S/MIME is built into many modern email programs.



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



**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 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

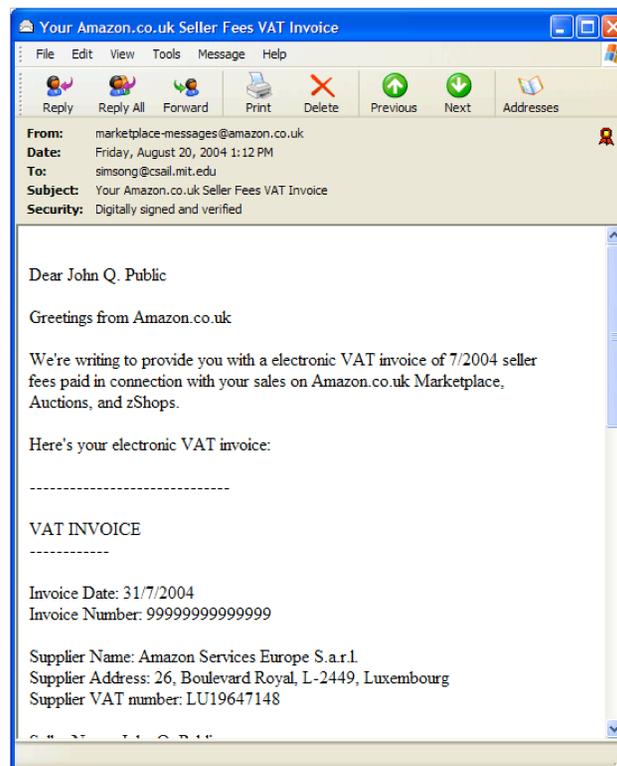
- ✓ Background on “Email Security”.
  - Survey Results: Merchants understand and can use technology that’s already deployed.
  - Improving Web Mail Security.
  - Moving forward with Key Continuity Management.

## Mail Security Survey.

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

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.**



## Survey respondents:

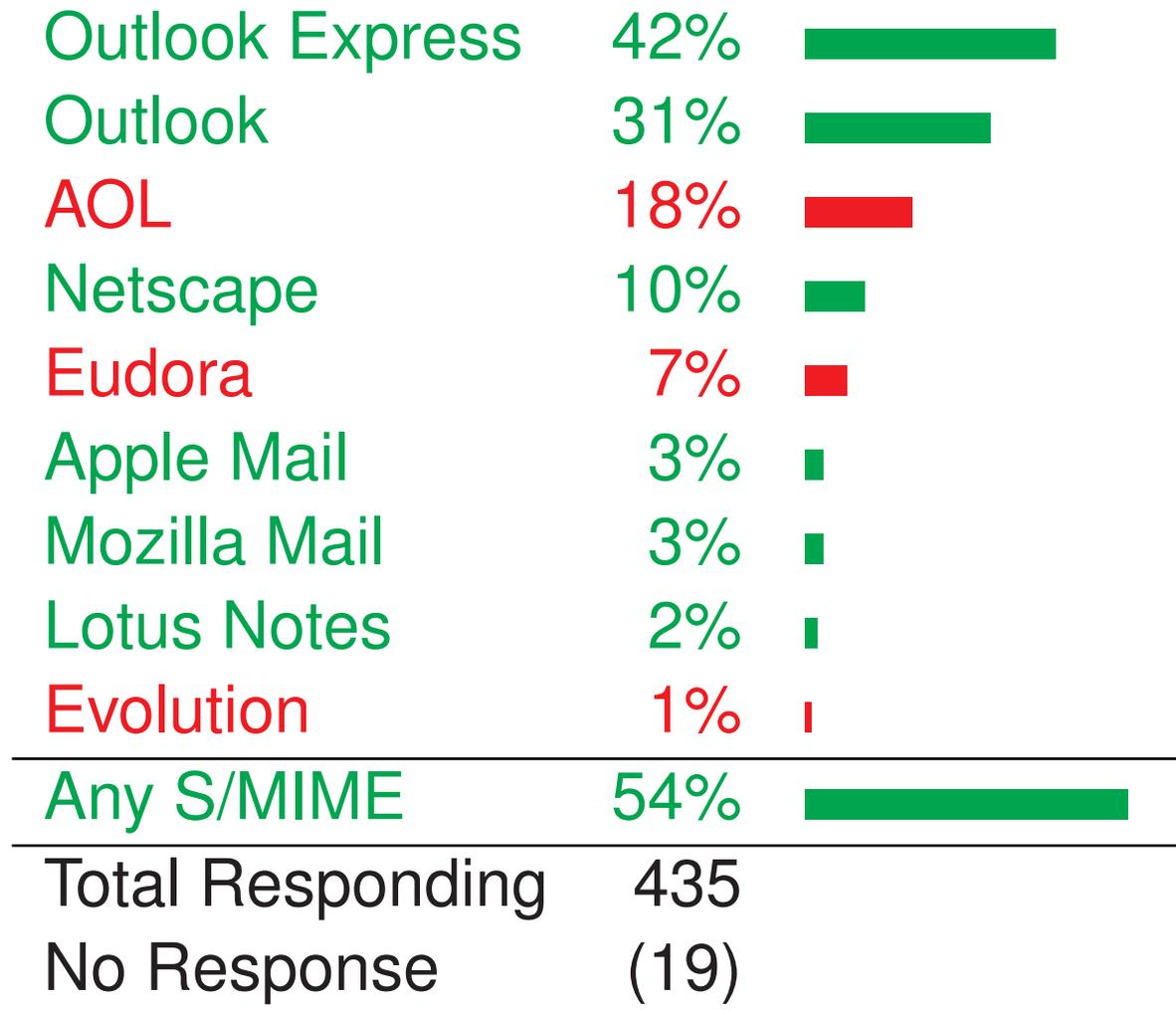
- 1083 sellers clicked on the link
  - 470 submitted the first web page.
  - 417 (89%) completed all five pages.
- Sellers were very educated:
  - 26% advanced degree
  - 35% college degree
- Sellers were very computer literate:
  - 18% “very sophisticated” computer user
  - 68% “comfortable” using computers

# 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.

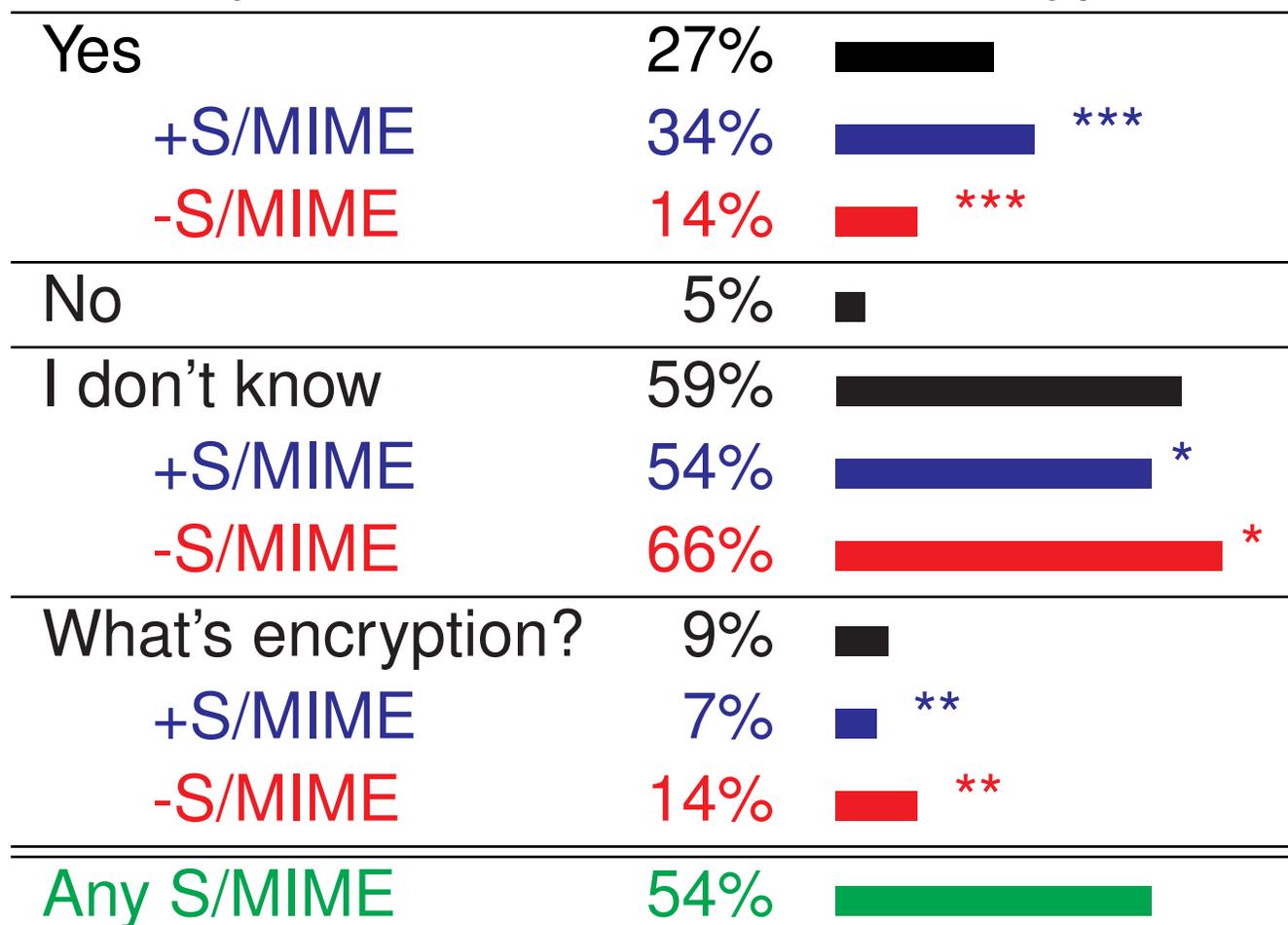
## More than half of our respondents read their mail with programs that support S/MIME

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



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

“Does your email client handle encryption?”



\* $p < .05$ ; \*\* $p < .01$ ; \*\*\* $p < .001$

## Not surprisingly, few merchants digitally sign their mail.

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



## 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>

## 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.

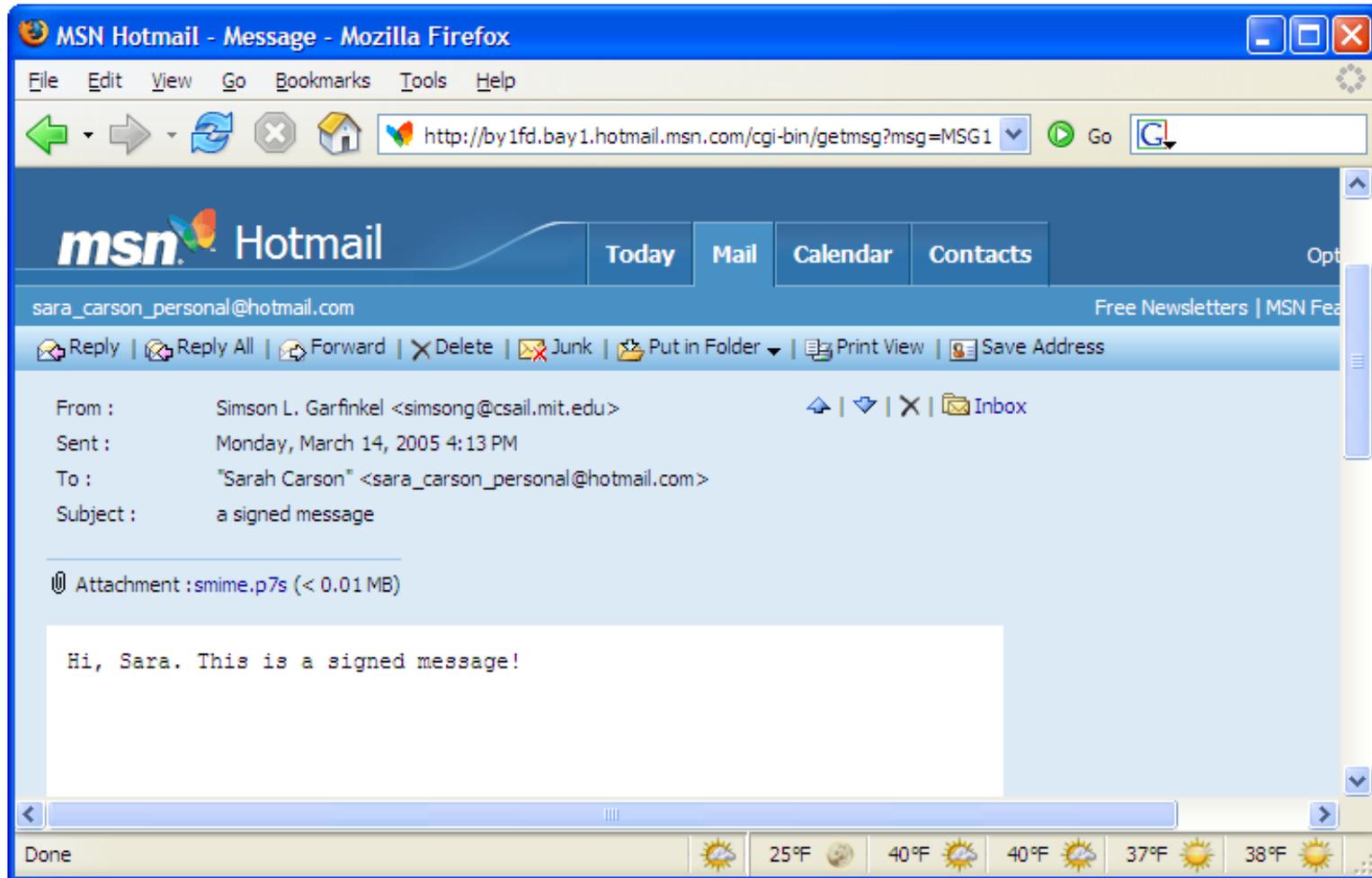
Apple Mail:

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:

From	Subject
 Jeffrey I. Schiller	Re: S/MIME survey
 David Margrave	Re: proposed survey
 Rob Miller	Re: survey so far

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

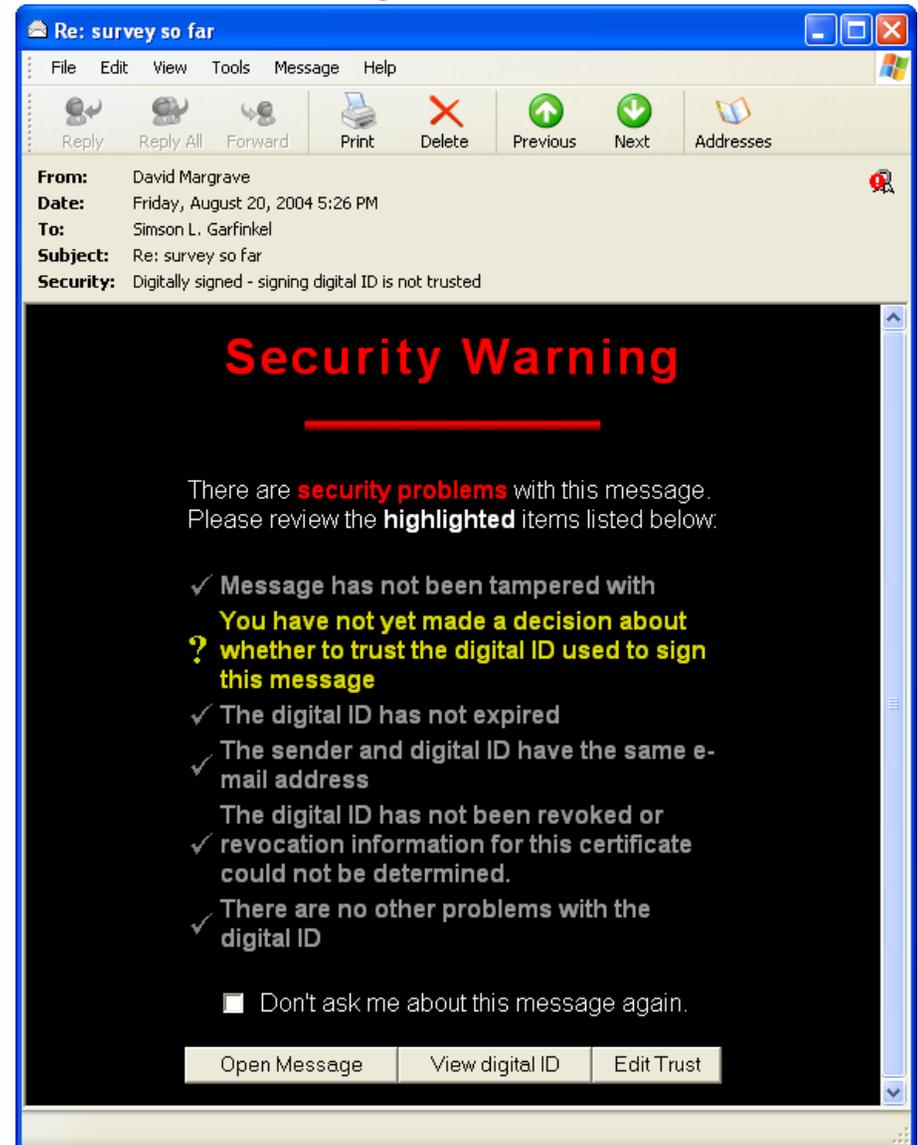


“I couldn’t open that file you sent me. What is it?”

**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.

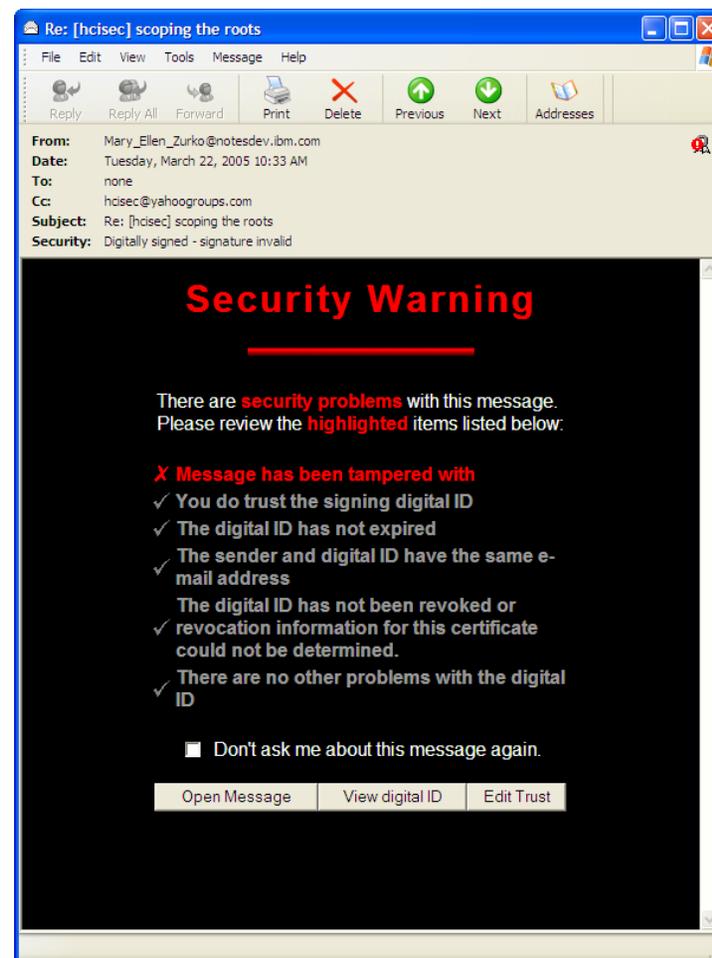
“**Security Warning:** You have not yet made a decision about whether to trust the digital ID used to sign this message”



**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”**

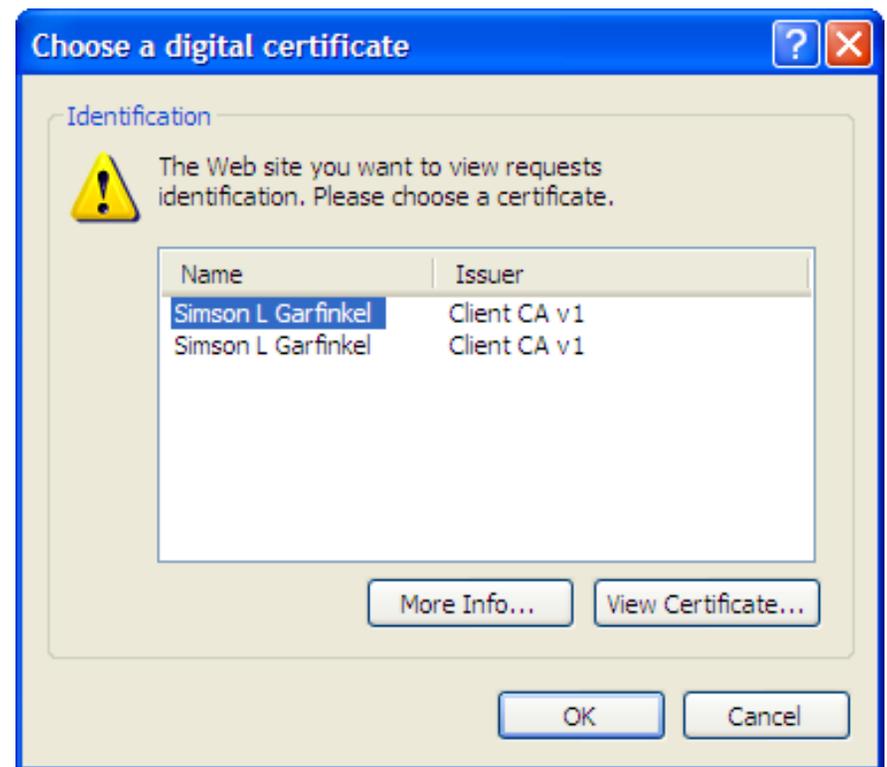
**Recommendation: Put pressure on YahooGroups and other providers to fix these problems!**

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

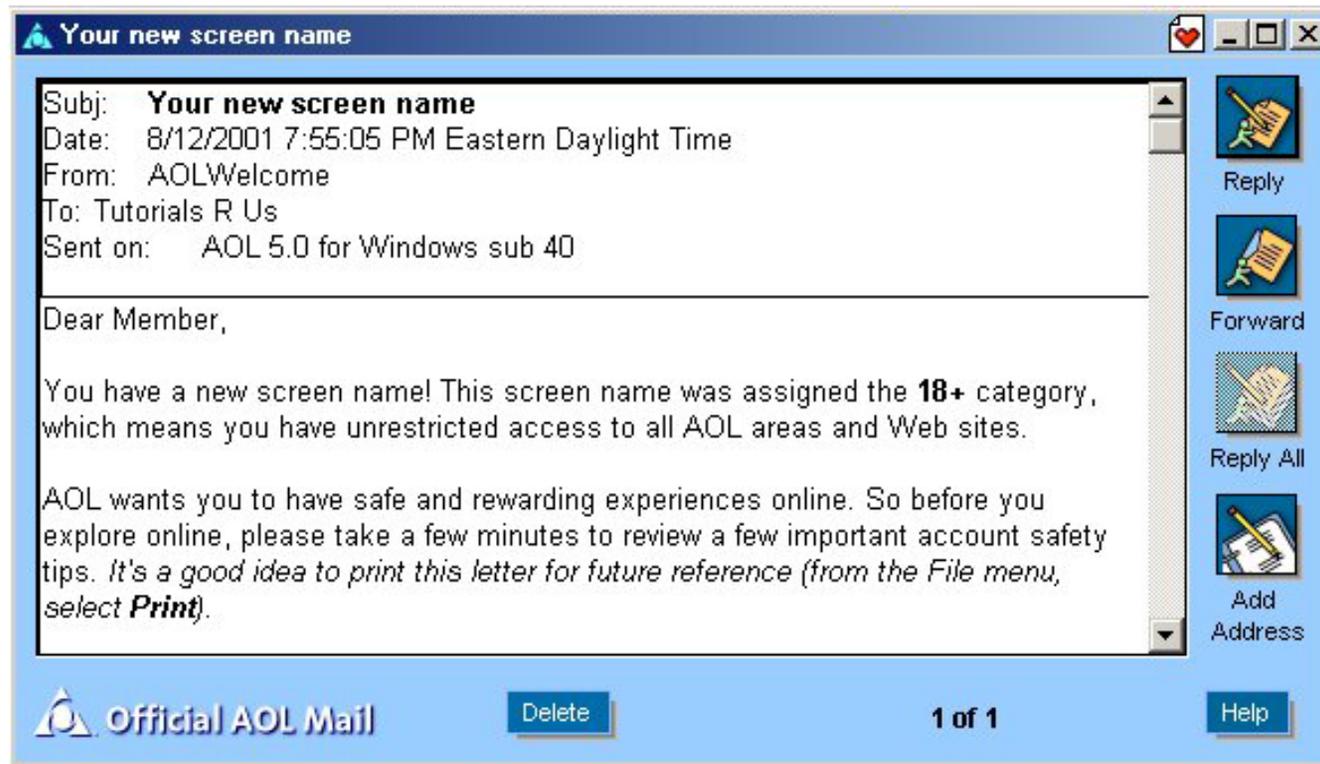
But we aren't ready for it!

- 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*.**

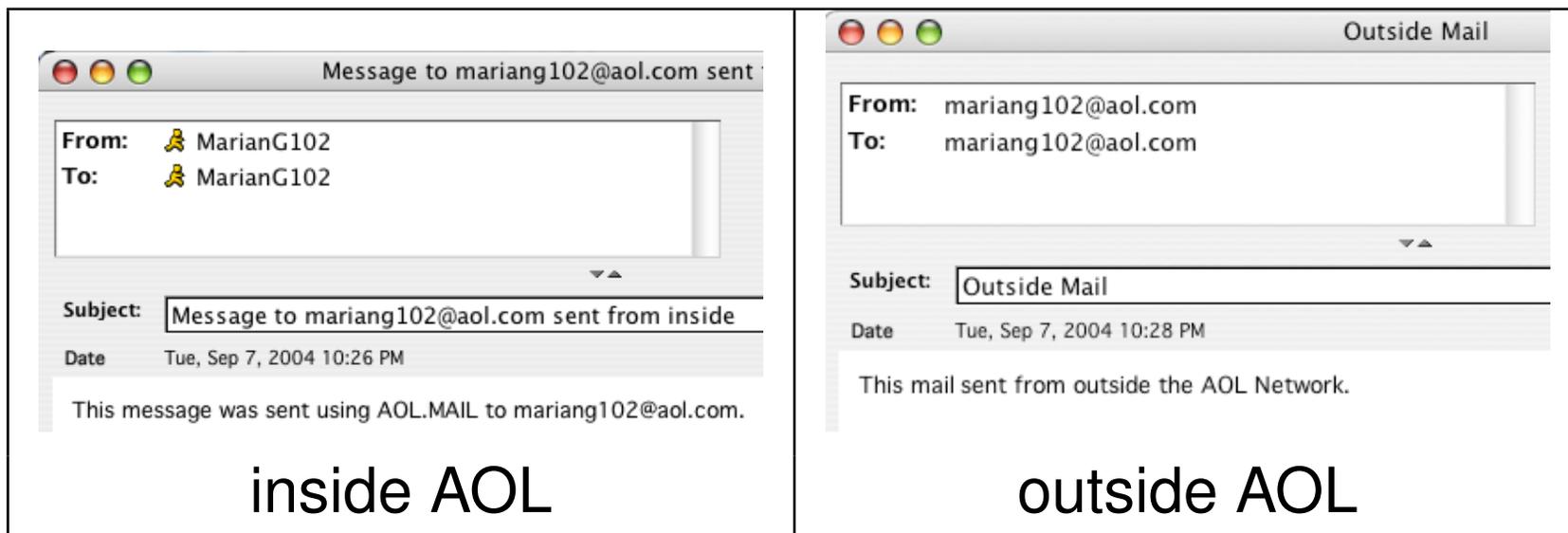


# Walled Gardens: Today's web mail systems can provide significantly more security than they do.



AOL's anti-phishing "blue mail" is official mail from AOL.

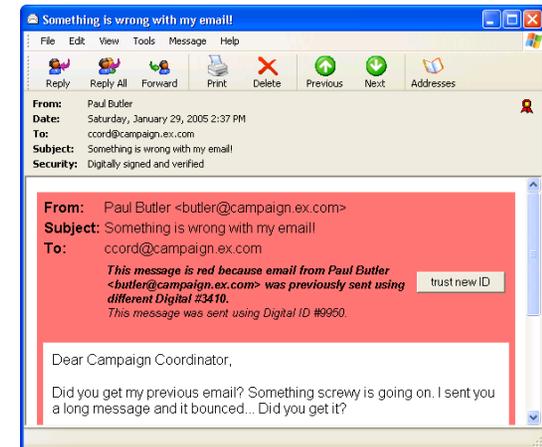
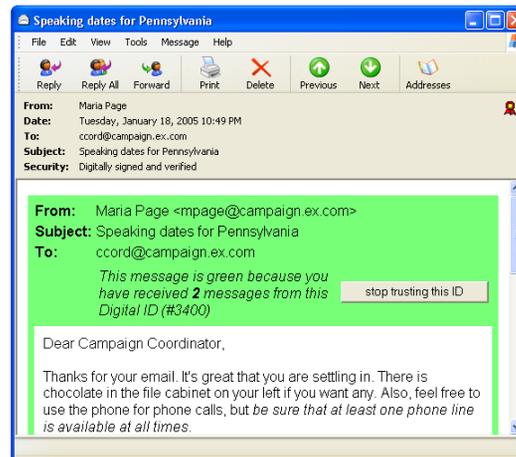
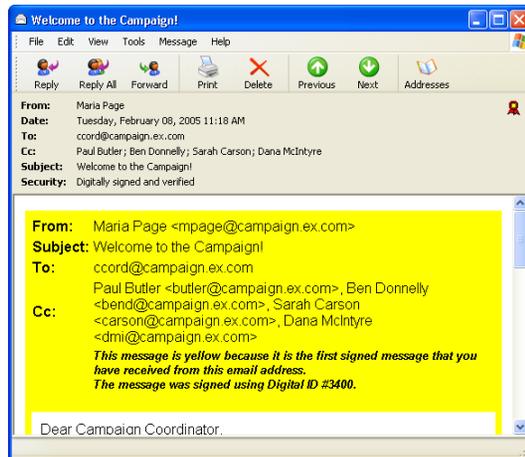
## AOL distinguishes between inside-mail and outside mail:



AOL should also:

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

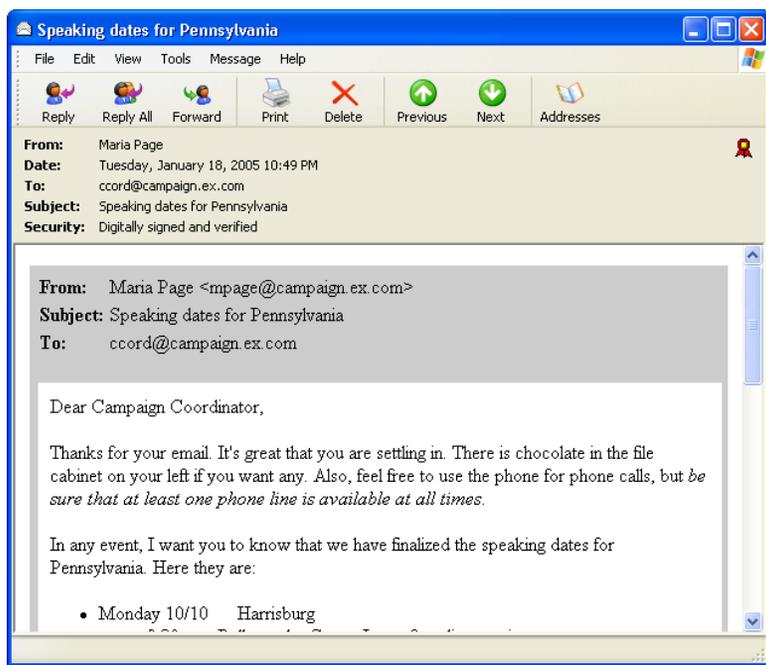
# Bridging the Gap with Key Continuity Management.



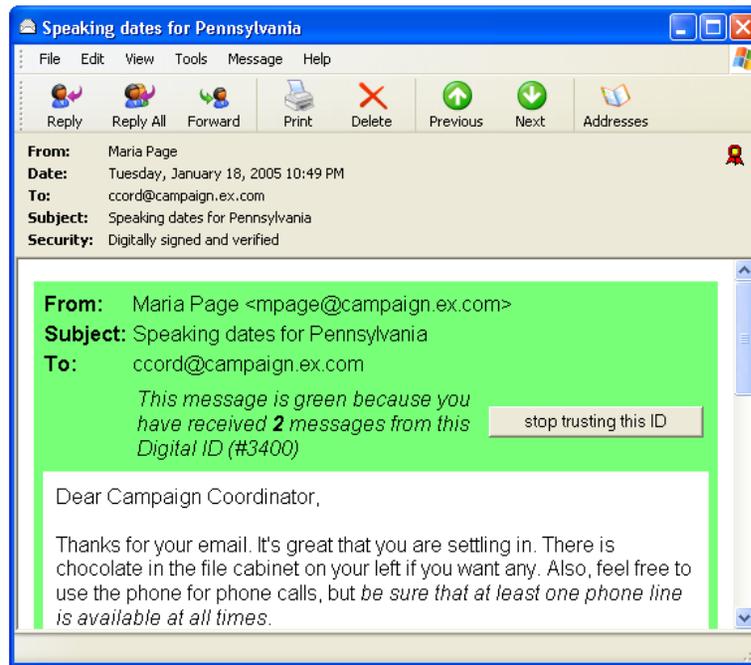
**KCM automates what a security expert would do when faced with a self-signed certificate. (SSH Model)**

# We've actually tested KCM in the lab.

## 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?**