Volume 28, issue 3–4, May/June 2009 ISSN 0167-4048

Computers & Security

The International Source of Innovation for the Information Security and IT Audit Professional

Vol. 28 No. 3–4

COMPUTERS & SECURITY 28 (2009) 105–120

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Understanding the limitations of S/MIME digital signatures for e-mails: A GUI based approach

Albert Levi[*], *Can Berk Güder*

Faculty of Engineering and Natural Sciences, Sabancı University, Orhanli, Tuzla, 34956 Istanbul, Turkey

ARTICLE INFO

Article history:
Received 26 July 2007
Accepted 2 September 2008

Keywords:
E-mail security
Digital signatures
S/MIME
Digital certificates
Security GUI

ABSTRACT

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a well-known standard for secure e-mail exchange. S/MIME builds its identity management on e-mail addresses, rather than real names. This fact may sometimes cause sending a signed e-mail with a bogus name on it. Moreover, header information of a signed e-mail message, such as subject and name, can be altered without affecting the verifiability of the signature. This paper spots the details of such problems of S/MIME and discusses some solutions from both developer and user points of view. Moreover, GUI considerations about these problems are also analyzed in this paper. An ideal GUI is modeled and developed.

1. Introduction

The answer to the question of "Have you received an unexpected e-mail from yourself or from another person that he/she did not send?" would probably be "yes" for a vast majority of the e-mail users. Current standards allow almost no default control on the authenticity of the senders in e-mail messages. Some SMTP (Simple Mail Transfer Protocol) servers prohibit relays and mandate entering username and password even for sending e-mails, so that only legitimate users can send e-mails to others. However, it is always possible to run an independent SMTP server to by-pass authentication controls enforced by the decent SMTP servers and their administrators.

Bogus e-mail problem is unlikely to be prevented by restrictive measures, but receivers should be able to detect bogus messages. Consider the conventional (snail) mail service. Anybody can write any name on a letter and envelope, and mail it. USPS or another postal service has nothing to do to identify the sender. The receiver should identify the sender using the information, especially signature, provided in the letter. A similar situation exists in the case of e-mail. The e-mail message should contain kind of a signature so that the receiver can identify the sender.

Fortunately, cryptographic digital signatures are possible in e-mails. Digital signatures in e-mails are standardized by IETF (Internet Engineering Task Force) as S/MIME (Secure/Multipurpose Internet Mail Extensions). Signing a message is a cryptographic operation that requires the private key of the signer. Since the private key is known only by the signer and not shared, the output of the signing process is considered as signature. Verification of a digital signature requires the corresponding public key. That is why the signer should make his/her public key accessible by other people. Distribution of public keys in S/MIME is performed using digital certificates.

However, S/MIME is not bulletproof. The identity management issues and some design decisions of S/MIME cause some practical problems in perception of signature verification by average users. For example, the name of the sender could be changed by an attacker and the signature is

[*] Tel: +90 216 483 9563; fax: +90 216 483 9550.
E-mail address: levi@sabanciuniv.edu (A. Levi).

0167-4048/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2008.09.003

still shown as verified. Moreover, the original subject may be modified without affecting the verifiability of the signature. In this paper, we detail these types of problems of S/MIME. We propose some solutions and develop criteria for an ideal GUI that carries S/MIME facts to the users in a proper way.

In Section 2, we give an overview the S/MIME effort of IETF. S/MIME prefers to use e-mail addresses as identities, not real names. The reasons of this fact and possible consequences are summarized in Section 2 as well. Section 3 is about demonstration of some practical problems in S/MIME. We also propose some solutions in the same section. Section 4 discusses GUI considerations about S/MIME; defines an ideal GUI and compares to some existing e-mail clients. Discussions and conclusions are given in Section 5.

2. Digital signatures in e-mails and S/MIME effort

S/MIME (Secure/Multipurpose Internet Mail Extensions) (S/MIME Working Group, 2008) is designed for incorporation of cryptographic security techniques in e-mails. Not only digital signatures, but also encrypted e-mails are possible in S/MIME. However in this paper, our interest is only in the signature capability of S/MIME. S/MIME is not a product, but a standard feature that is to be supported by e-mail client programs, like MS Outlook, Outlook Express, Eudora, Mozilla Thunderbird and Netscape Messenger.

S/MIME defines the structure of digital signature blocks to be appended to e-mail messages. A signature block is generated by applying the cryptographic signature generation function over the message. This process uses sender's private key. Upon reception, the recipient verifies the signature using the pubic key of the sender. At this point receiver has an important limitation. The receiver should make sure that the public key used for verification really belongs to the sender; otherwise receiver cannot comment on the identity of the sender. S/MIME proposes using *digital certificates* (ITU-T, 2000; Levi, 2006) for this problem.

2.1. *Digital certificates*

Digital certificates (a.k.a. digital identities) are widely used as an enabling mechanism for public key cryptosystem based applications. The certificates used for S/MIME are approved bindings between the identity of the certificate holders and their public keys. Certificates are issued by trusted Certification Authorities (CAs) with their digital signature over the certificate content. Prior to verification of the signature over the e-mail message, the recipient verifies the signature over the sender's certificate to find out his/her public key. In this way, the recipient makes sure about the identity of the person of whom he/she is using public key for signature verification.

Generally a chain of certificates is verified starting with a trusted root-CA, for whom the recipient knows the public key. Public keys (actually self-signed certificates) of well-known root-CAs come with S/MIME enabled e-mail clients.

2.2. *How S/MIME works for digitally signed messages?*

Once the message content is ready, the sender generates his/her digital signature over the content and appends it to the message. Sender generally sends his/her certificate along with the signed message.

The recipient processes the certificate and signed message separately. First the certificate is verified as described in Section 2.1. The public key obtained from certificate verification is used to verify the signature over the e-mail. Moreover, the e-mail address in the certificate is compared to the one in the e-mail message; they must be equal.

Fig. 1 shows the life cycle of a signed message sent from Alice to Bob. If all verifications and controls at the recipient (Bob) are all right, then the e-mail client shows an indicator for a successfully signed and verified message.

2.3. *Standardization efforts related to S/MIME*

Standardization is a must for proper interoperability among different e-mail (SMTP) servers, clients and CAs. S/MIME is an effort of IETF (Internet Engineering Task Force), S/MIME Mail Security working group (S/MIME WG). The WG has proposed several standards track, informational and experimental RFCs and Internet Drafts that can be reached from the WG's website (S/MIME Working Group, 2008).

S/MIME also relies on some other standards and RFCs. For cryptographic processing, PKCS (Public Key Cryptography Standards) (RSA Laboratories, 2008) are referred in several S/MIME documents. S/MIME certificates are based on PKIX (Internet X.509 Public Key Infrastructure) initiative (PKIX Working Group, 2008), and consequently on X.509 standard (ITU-T, 2000).

Regarding basic mail services, S/MIME depends on RFC 2821 (SMTP specification) (Klensin, 2001), RFC 2822 (Message Format Specification) (Resnick, 2001). MIME specifications (Freed and Borenstein, 1996a; Freed and Borenstein, 1996b; Moore, 1996; Freed and Klensin, 2005; Freed and Borenstein, 1996c) have strong relationships with S/MIME as well.

In this paper, we mostly refer to RFC 2632 (S/MIME Version 3 Certificate Handling) (Ramsdell, 1999a) and RFC 2633 (Ramsdell, 1999b) (S/MIME Version 3 Message Specification). S/MIME Version 3.1 of both RFCs is also published as RFC 3850 (Ramsdell, 2004a) and RFC 3851 (Ramsdell, 2004b), respectively. Version 3.1 obsoletes previous version. However, since all of the S/MIME implementations that we are aware of still bear version 3.0 features for digital signature processing, version 3.0 is more relevant than version 3.1 in this paper.

2.4. *Identity management in S/MIME: principles and problems*

S/MIME consistently abstained from using real names as primary identity elements in e-mail signature verification. Instead, it uses e-mail addresses for this purpose. Possible reasons include:

(i) Impossibility of having a globally unique name, thus possible naming ambiguities (for example, there might be two John Smiths in the same country's, same organization's, same organizational unit),

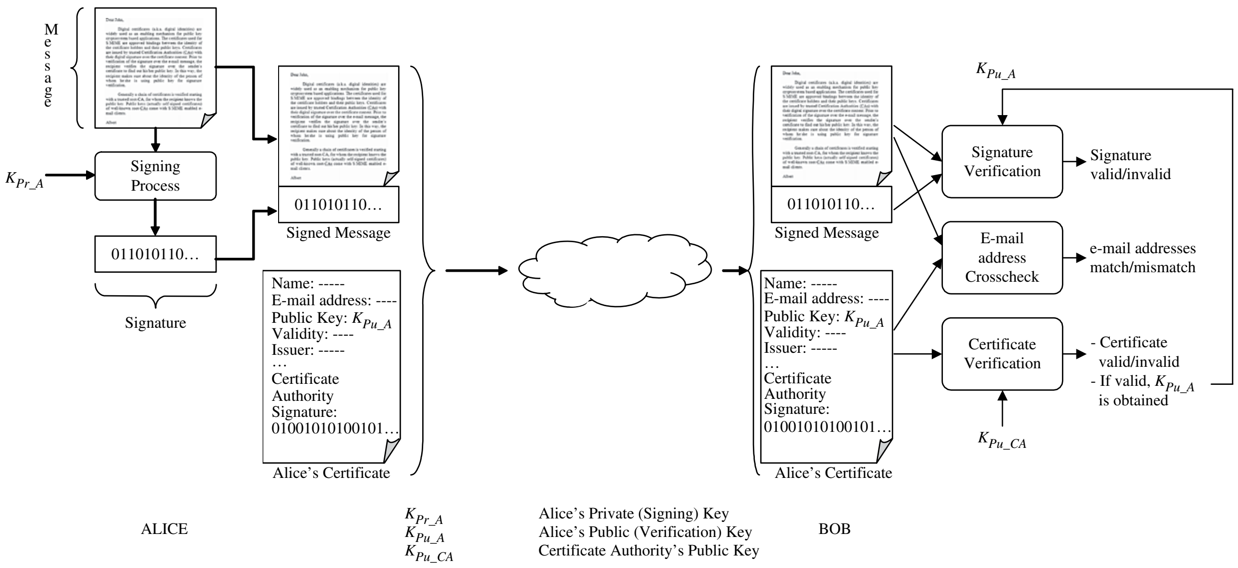


Fig. 1 – Life cycle of a signed message.

(ii) hardness of obtaining a standard name out of complex certificate fields, and
(iii) unbearable attraction of globally unique and application-specific e-mail addresses.

Unfortunately, this design decision triggered two important problems:

1) The name information in the certificate and the name in the e-mail message become independent of each other, so name information in an S/MIME certificate looses its importance in e-mail signature verification.
2) Recipients are enforced to identify people using their e-mail addresses. This may not be the common practice. People tend to identify other people using their real names. Some e-mail clients show only the names in the message windows and/or preview panels.

These problems, together with some flaws in certification practices and the scope of signature in e-mail messages, cause some practical attacks on S/MIME signature scheme. They will be described in Section 3.

3. Practical problems of S/MIME

S/MIME provides strong security services to e-mail messages. However, there are still some practical security problems especially in identity management, certificate handling and header protection. In this section, we explain those problems that exist in S/MIME Version 3, and discuss some solutions and S/MIME WG efforts to solve them in Version 3.1.

We discuss three courses of problems and attacks on S/MIME.

1. Bogus identity usage in class-1 certificates
2. Using a name different than the one in the certificate
3. Header protection issues

3.1. *Bogus identity in class-1 certificates*

CAs perform identity control prior to issuance of a certificate. Although it is not a standard rule, Stallings (2006) discusses three different levels (classes) of identity controls. Here we give a brief overview of these certificate classes that might slightly differ from CA to CA in practice.

□ *Class-1*: Class-1 certificate issuance is an on-line process. Name of the subject entity is not validated. Only an e-mail address control is performed by sending an authentication string to the e-mail address that the subject entity provides in certificate application. In order to complete the certificate issuance process, the subject entity should use this authentication string. This e-mail address appears in the certificate. Some CAs include the name of the subject entity in the certificate as well, but specifying that the name is not validated. However, the appropriate action would be not to include a name in a class-1 certificate, as some other CAs do.

□ *Class-2*: The certification process may or may not be on-line depending on the CA's practice. Subject entity information (such as name and address) is checked against a third party database. Some CAs may ask the subject entity to send a hardcopy signed agreement and/or a hardcopy identity document via facsimile or snail mail. However, personal presence is not required. E-mail address control as in the class-1 certificates is also performed.

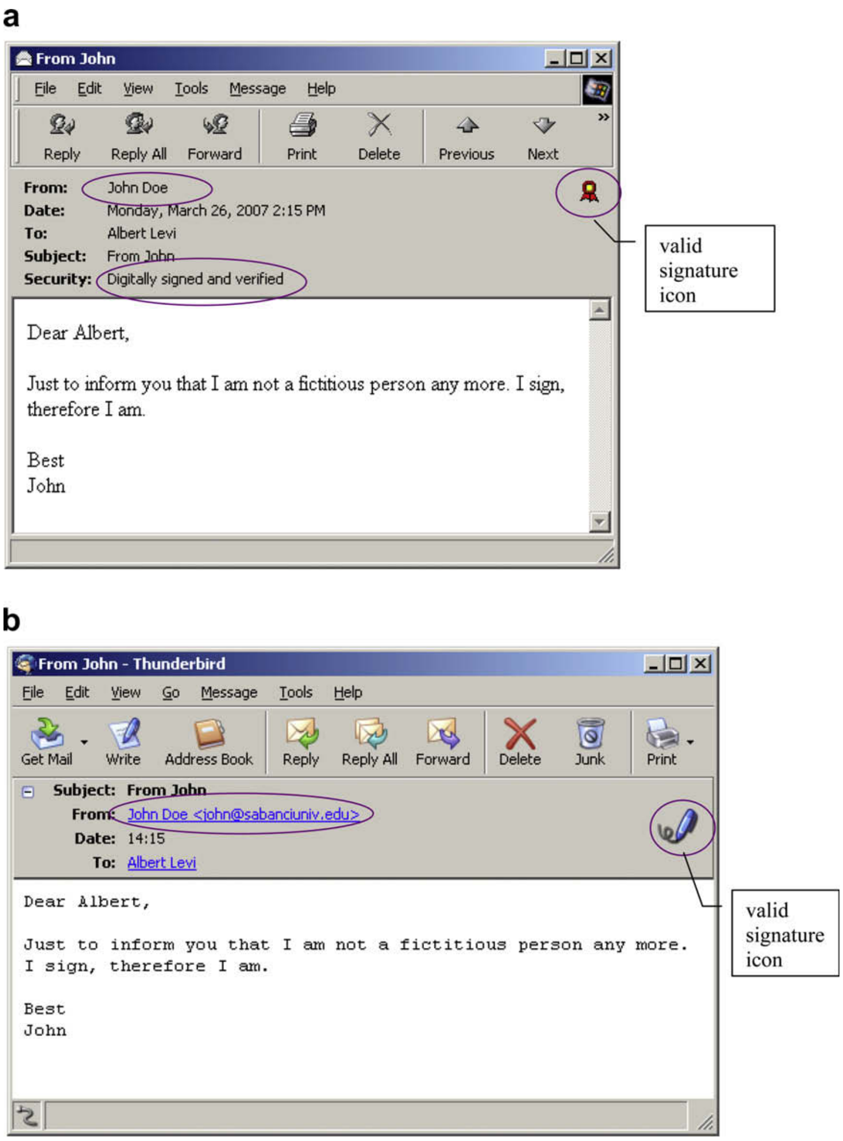
□ *Class-3*: In addition to the e-mail address control, the subject entity should personally present an identity document to a registration authority. The process is off-line and may take some time to be completed.

Class-1 certificates provide lowest degree of identity assurance, but they are the easiest to issue and cheapest. Thus they become very popular among the certificate holders.

The level of assurance given in a certificate is more of a concern of the peer entity, who will verify the certificate, than of the certificate holder. Therefore, certificate holders usually do not care the lack of identity control in class-1 certificates. Root certificates for all certificate classes come with the client software, so practically all certificates are verifiable and there is no striking difference among them from the point of view of an average recipient. Moreover, using a class-3 certificate does not make the certificate owner *cryptographically* more secure; all classes of certificates use the same signature algorithms and are capable of certifying public keys of the same cryptographic strength.

As mentioned above, class-1 certificates do not contain validated names. Indeed, it is possible to obtain a class-1 certificate from a respectable CA with a bogus name on it. Moreover, the e-mail client programs allow using any name while sending an e-mail message. These two facts enable sending an S/MIME signed message with a bogus name. The e-mail clients that we considered (namely Netscape Messenger 7.2, MS Outlook XP and 2007, Mozilla Thunderbird 1.5.0.10, and MS Outlook Express 6) verify this signature successfully and present the signed message as if sent by the bogus name. The S/MIME specifications do not enforce the e-mail client programs to show the signature verification information in a standard way. That is why each client has different GUI to display an e-mail message and the corresponding signature information. We comparatively analyze the GUIs of different e-mail client programs in Chapter 4. Here, we give two example GUIs that belong to MS Outlook Express 6 and Mozilla Thunderbird in Fig. 2; the GUIs say that John Doe has signed the message, which is, of course, not the case.

In this example case, the certificate we obtained includes a bogus name in it. However, most CAs do not include names in class-1 certificates, since they do not assure identity. Our attack is still possible with such class-1 certificates. S/MIME does not enforce a name existence check in certificate verification phase.



From: John Doe
Date: Monday, March 26, 2007 2:15 PM
To: Albert Levi
Subject: From John
Security: Digitally signed and verified

Dear Albert,

Just to inform you that I am not a fictitious person any more. I sign, therefore I am.

Best
John

Subject: From John
From: John Doe <john@sabanciuniv.edu>
Date: 14:15
To: Albert Levi

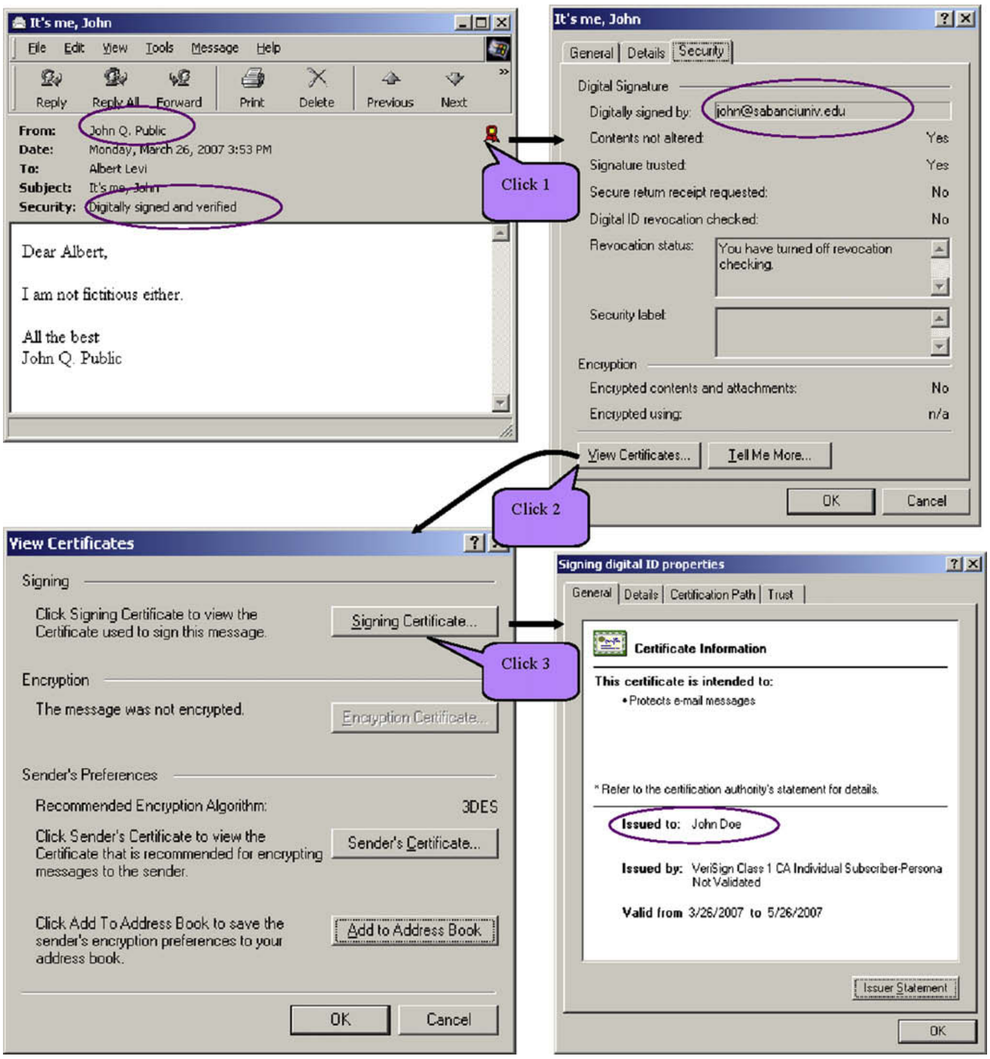
```
Dear Albert,

Just to inform you that I am not a fictitious person any more.
I sign, therefore I am.

Best
John
```

Fig. 2 – A digitally signed message with a bogus name. (a) as shown by MS Outlook Express, (b) as shown by Mozilla Thunderbird.

Therefore, it is possible to use any name while sending signed messages, even if the certificate contains no name in it.

Since the S/MIME clients perform a match between the e-mail address in the certificate and the e-mail address in the e-mail header, the sender must use the e-mail address within the certificate. This address would definitely be different than the actual address of the person whose identity is being stolen. This may lead the recipient to figure out that there is something wrong, if the recipient identifies e-mail senders by their e-mail addresses rather than their names. However, people generally use real names for identification.

The policy identifiers that point to the CPS (Certificate Practice Statement) of the CA may be another hint for the recipient to understand the limitations of class-1 certificates. However, such a CPS control may require a long reading, and sometimes expertise in security technology for comprehension. Another action that the recipient may take is to check the certificate details by clicking on some buttons. CAs mostly put a remark in the certificate to mention that the person is not validated. However, a user with average technical information about security cannot easily comprehend the details of a certificate, especially when his/her popular e-mail client program says "the message has been signed and verified", and shows the sender's name in the message header. Indeed, there are some studies in the literature that put forward the problems of understanding and using the security functionality that exists in end-user programs. Whitten and Tygar (1999) analyzed PGP and found a number of user interface design flaws that may contribute to security failures. Furnell et al. (2006) has recently carried out a survey study and concluded that more than half of the MS Outlook Express users show important deficiencies in comprehending sufficient information about e-mail encryption and digital signatures. Another recent work by Furnell (2005) highlights problems of users in terms of finding, understanding, and ultimately using the security features that are meant to be at their disposal. As these studies showed, the user interface with which the security features are presented to the users is very important for an average user to protect himself/herself. Users should be educated to be more conscious about the limitations of class-1 certificates in order not to make the e-mail service more insecure in the name of security. Thus, in order to protect the users from the bogus names in class-1 certificates, the e-mail clients may take an automated action



From: John Q. Public
Date: Monday, March 26, 2007 3:53 PM
To: Albert Levi
Subject: It's me, John
Security: Digitally signed and verified

Dear Albert,

I am not fictitious either.

All the best
John Q. Public

Digital Signature
Digitally signed by: john@sabanciuniv.edu
Contents not altered: Yes
Signature trusted: Yes
Secure return receipt requested: No
Digital ID revocation checked: No
Revocation status: You have turned off revocation checking.
Security label:
Encryption
Encrypted contents and attachments: No
Encrypted using: n/a

Signing
Click Signing Certificate to view the Certificate used to sign this message.
Encryption
The message was not encrypted.
Sender's Preferences
Recommended Encryption Algorithm: 3DES
Click Sender's Certificate to view the Certificate that is recommended for encrypting messages to the sender.
Click Add To Address Book to save the sender's encryption preferences to your address book.

Certificate Information
This certificate is intended to:
• Protects e-mail messages
* Refer to the certification authority's statement for details.
Issued to: John Doe
Issued by: VeriSign Class 1 CA Individual Subscriber-Persona Not Validated
Valid from 3/26/2007 to 5/26/2007

Fig. 3 – A digitally signed message that uses a name different than the one in the certificate.

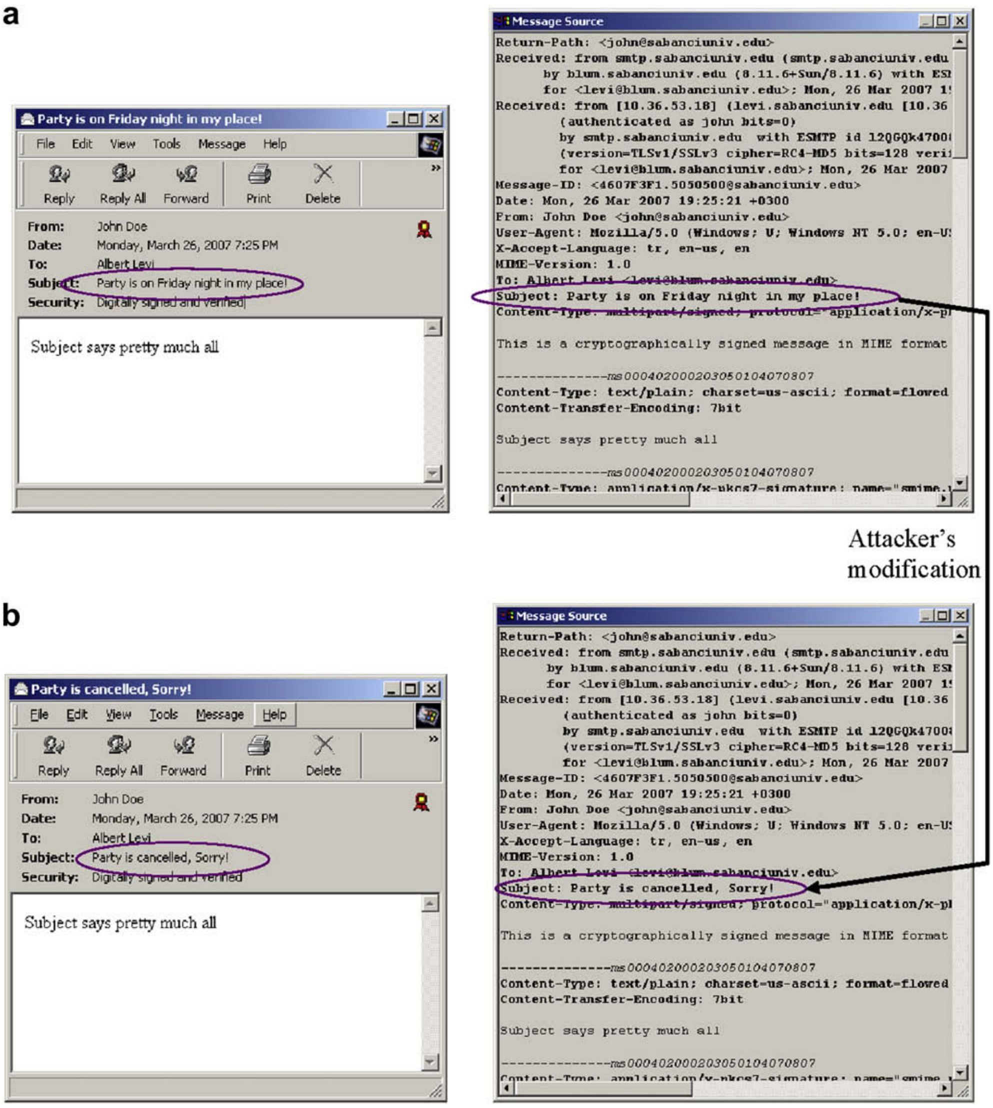
to identify class-1 certificates and warn the recipient with a proper GUI message, although it is not mandated by the S/MIME standards. Such a GUI based solution is proposed and implemented in Sections 4.3 and 4.4.

More radical solutions could be (a) discontinuation of class-1 certificate issuances by CAs and/or (b) stopping class-1 root-CA certificate distribution with e-mail client programs, so that the recipients are enforced to make a trust decision on those certificates. We frankly do not believe that these solutions are applicable in the market conditions, mainly due to two reasons: 1) it is contrary to the win-win deal between the CAs and the e-mail client developers, 2) such an action would make the certificate penetration among the Internet users worse.

3.2. *Using a name different than the one in the certificate*

The only connection between a certificate and an e-mail message is the e-mail address. S/MIME Version 3.0 verification process mandates having the same e-mail address both in the sender certificate and in the e-mail message header. However, S/MIME Version 3.0 does not mandate a comparison between the name in the certificate and the name in the e-mail according to RFC 2632, Section 3 (Ramsdell, 1999a). S/MIME Version 3.1 (RFC 3850) has the same verification process as well. This verification process enables the sender to be able to send a signed e-mail message using an e-mail address that exists in a certificate, but with a different name. Of course the certificate fields will not change, but the e-mail is verified as if it is from another person. An example is shown in Fig. 3, upper left snapshot. The certificate used in this example is the same as the one used for the example given in Fig. 2. As can be seen from the "from" field, the sender name is different and this is not the name that appears in the certificate; but the signature is still verified.

Moreover, this particular problem is not a problem of only class-1 certificates, but also of class-2 and class-3 certificates as well. The problem is in e-mail signature verification process. This process is independent of the certificate classes and the level of identity assurance in certificates. As long as the names are not compared during verification, no matter how strong identity assurance is provided in certificate



From: John Doe
Date: Monday, March 26, 2007 7:25 PM
To: Albert Levi
Subject: Party is on Friday night in my place!
Security: Digitally signed and verified

Subject says pretty much all

```
Return-Path: <john@sabanciuniv.edu>
Received: from smtp.sabanciuniv.edu (smtp.sabanciuniv.edu
      by blum.sabanciuniv.edu (8.11.6+Sun/8.11.6) with ESI
      for <levi@blum.sabanciuniv.edu>; Mon, 26 Mar 2007 1!
Received: from [10.36.53.18] (levi.sabanciuniv.edu [10.36
        (authenticated as john bits=0)
        by smtp.sabanciuniv.edu  with ESMTP id 12QGQk4700(
        (version=TLSv1/SSLv3 cipher=RC4-MD5 bits=128 veri:
        for <levi@blum.sabanciuniv.edu>; Mon, 26 Mar 2007
Message-ID: <4607F3F1.5050500@sabanciuniv.edu>
Date: Mon, 26 Mar 2007 19:25:21 +0300
From: John Doe <john@sabanciuniv.edu>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-U:
X-Accept-Language: tr, en-us, en
MIME-Version: 1.0
To: Albert Levi <levi@blum.sabanciuniv.edu>
Subject: Party is on Friday night in my place!
Content-Type: multipart/signed; protocol="application/x-pl

This is a cryptographically signed message in MIME format

--------------ms000402000203050104070807
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit

Subject says pretty much all

--------------ms000402000203050104070807
Content-Type: application/x-pkcs7-signature; name="smime.
```

From: John Doe
Date: Monday, March 26, 2007 7:25 PM
To: Albert Levi
Subject: Party is cancelled, Sorry!
Security: Digitally signed and verified

Subject says pretty much all

```
Return-Path: <john@sabanciuniv.edu>
Received: from smtp.sabanciuniv.edu (smtp.sabanciuniv.edu
      by blum.sabanciuniv.edu (8.11.6+Sun/8.11.6) with ESI
      for <levi@blum.sabanciuniv.edu>; Mon, 26 Mar 2007 1!
Received: from [10.36.53.18] (levi.sabanciuniv.edu [10.36
        (authenticated as john bits=0)
        by smtp.sabanciuniv.edu  with ESMTP id 12QGQk4700(
        (version=TLSv1/SSLv3 cipher=RC4-MD5 bits=128 veri:
        for <levi@blum.sabanciuniv.edu>; Mon, 26 Mar 2007
Message-ID: <4607F3F1.5050500@sabanciuniv.edu>
Date: Mon, 26 Mar 2007 19:25:21 +0300
From: John Doe <john@sabanciuniv.edu>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-U:
X-Accept-Language: tr, en-us, en
MIME-Version: 1.0
To: Albert Levi <levi@blum.sabanciuniv.edu>
Subject: Party is cancelled, Sorry!
Content-Type: multipart/signed; protocol="application/x-pl

This is a cryptographically signed message in MIME format

--------------ms000402000203050104070807
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit

Subject says pretty much all

--------------ms000402000203050104070807
Content-Type: application/x-pkcs7-signature; name="smime.
```

Fig. 4 – a. Original signed message and its source. b. Altered message.

issuance, this assurance will not be able to be relayed to signature verification.

The recipient can understand the existence of the problem by checking the sender's e-mail address, which is the original certificate holder's e-mail address (Fig. 3, upper right snapshot), or by examining the certificate details, which show the name and information of the original certificate holder. Fortunately, S/MIME Version 3.1 (RFC 3850) (Ramsdell, 2004a) recommends to display the name and other certificate details when displaying an indication of successful or unsuccessful signature verification. We have tested some S/MIME compliant e-mail client programs to assess how they relay name and other certificate details to the end users. The details of this analysis will be given in Section 4.2 and 4.3, but here we give a brief overview and an example. These tests show that the e-mail clients relay the name information either on some late windows that appear after clicking on three or four buttons, or in a confusing way. An example case is depicted in Fig. 3 for MS Outlook Express 6. As shown in this figure, the name in the certificate is shown after three clicks. Similar user interface considerations for other e-mail client systems will be detailed later in Section 4.

Actually, as discussed in the previous section, it is not a good idea to rely on recipient's off-line checks on the names or any other certificate field to assure about the validity of a signature. Users' expectation from a secure e-mail client software is automated detection of an anomaly. However, none of the e-mail clients perform the name consistency check since it is not part of the S/MIME standard.

3.3. *E-mail header alteration*

Basically speaking, an e-mail message consists of two parts: "header" and "content" (content is named as the "MIME entities" in S/MIME documentations). Header contains the envelope information, like *from*, *to*, *cc*, *date*, *subject*, etc. Content does not contain the header. RFC 2633, Section 3.1 (Ramsdell, 1999b) clearly states that S/MIME Version 3 is to be used to secure the content, not the header. This fact causes any malicious alterations on the e-mail header to go undetected. A practical attack could be the alteration of the *subject* field of a message by the recipient. For example, consider an investor *A* sends a signed message to his broker *B* to buy X Inc. stocks in the subject field and leaves the message body blank. *B* mistakenly buys Y stocks instead of X. In order to compensate this mistake, *B* can update the message source such that the subject of the message from *A* now orders Y Inc. stocks. The altered message is still digitally signed and verified.

In another scenario, an attacker could modify the subject field while the message is en route. Such a scenario is shown in Fig. 4a and b. Fig. 4a shows the original message and its source. Fig. 4b shows the altered message and source.

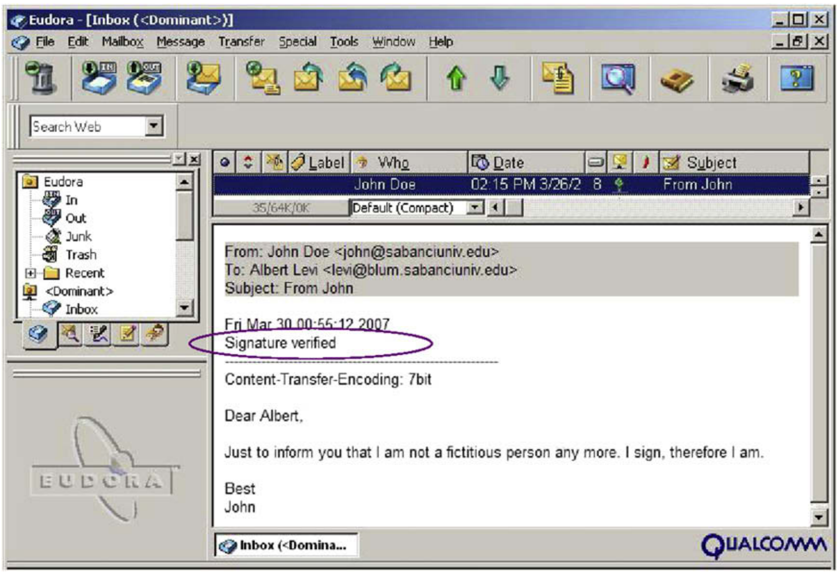
Besides the *subject* field, other header fields, such as *to*, *from*, *cc*, *date*, can all be altered without affecting the verifiability of the existing signature over the message content. The only exception is the e-mail address (but not the name) of the *from* field. If this address is altered, the signature becomes non-verifiable because of S/MIME's e-mail address crosscheck.

A precaution against header alteration is not to rely on the e-mail header information, which is nothing but an envelope that can be altered. The sender should put all sensitive information, including his/her name, affiliation, address, and the recipients' information, subject, date, etc., into the message body.

S/MIME Version 3.1 (RFC 3851 (Ramsdell, 2004b)) provides an optional header protection to some extent, but this protection has some practical problems as discussed below. The method proposed by RFC 3851 (Ramsdell, 2004b) is to encapsulate the actual message into a single MIME object of message/rfc822 type as an attachment and to apply the S/MIME signature to this object. This signed message/rfc822 MIME object is to be attached to another e-mail message that will be sent to the recipient. In this method, the header fields of the actual message would be in the scope of the digital signature. However, the header of the outer message that carries the actual message in its attachment is not in the scope of S/MIME protection. Thus, in order the protection of the actual (encapsulated) message to be conveyed to the verifying e-mail recipient, the encapsulated message should be shown as the only message. Although, RFC 3851 recommends the e-mail clients to show the encapsulated message as the outer (and therefore only) message to the recipient, this does not comply with current e-mail related IETF standards and e-mail client implementations. Existing standard message/rfc822 processing at the recipient side is to show the encapsulated message as an attachment and show the header of the outer

Table 1 – Analysis of GUI criteria for the scope of signature.

	Clear statement about the signature scope (verification)	Clear statement about the signature scope (signing)	No verification message/icon at the header display	No verification icon at the preview pane
Ideal GUI	*Exists on the e-mail display window*	*Exists*	*No icon/No message*	*No icon*
Netscape Messenger 7.2	Does not exist	Does not exist	Icon exists/No message	*No icon*
Mozilla Thunderbird 1.5.0.10	Does not exist	Does not exist	Icon exists/No message	*No icon*
MS Outlook Express 6	Does not exist	Does not exist	Icon exists/Message exists	Icon exists
MS Outlook XP	Does not exist	Does not exist	*No icon/No message*	Icon exists
MS Outlook 2007	Does not exist	Does not exist	Icon exists/Message exists	Icon exists
Eudora 7.1 (with S/MIME plugin)	Does not exist	Does not exist	*No icon/No message*	*No icon*



From: John Doe <john@sabanciuniv.edu>
To: Albert Levi <levi@blum.sabanciuniv.edu>
Subject: From John

Fri Mar 30 00:55:12 2007
Signature verified

Content-Transfer-Encoding: 7bit

Dear Albert,

Just to inform you that I am not a fictitious person any more. I sign, therefore I am.

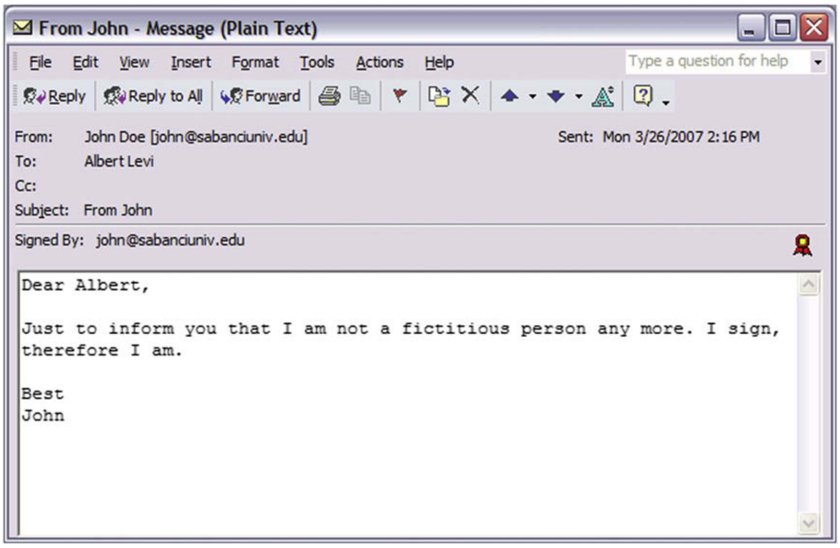
Best
John

Fig. 5 – E-mail window of Eudora; signature verification message is at the beginning of body.

message as the main header. Furthermore, the headers of the outer and the encapsulated messages of message/RFC822 type may be different from each other. This difference is natural since the aim of message/rfc822 attachment is to forward an e-mail message; forwarded message may have different envelope information and subject. Moreover, header protection of S/MIME Version 3.1 is not a mandatory feature and actions to be taken in case of an inconsistency between the protected header fields and ordinary outer header fields are up to the e-mail client system at the recipient. Thus, for the sake of compatibility with S/MIME Version 3.0 and regular MIME conventions, e-mail client developers would prefer to show the message/rfc822 attachments just as a regular attachment and would not issue an error for header inconsistencies, if they implement such a header protection. In this way, the outer header and the subject that are shown in the e-mail window would still suffer the abovementioned header alteration attack. Actually, probably due to these practical problems mentioned here, none of the e-mail clients that we examined (including recently released MS Outlook 2007 and recent version of Mozilla Thunderbird) support header protection of S/MIME Version 3.1 in both sending and verifying S/MIME messages.

4. User interface considerations

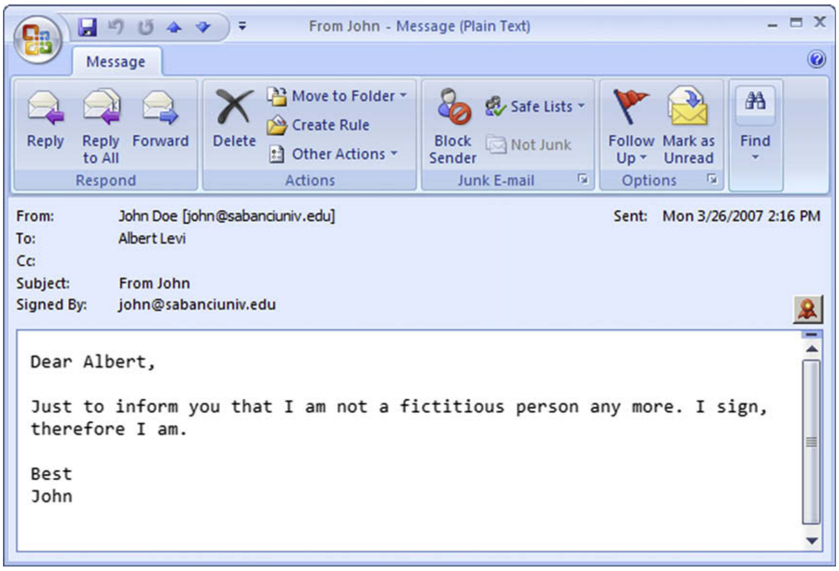
The precautions discussed for the problems given in Section 3 are partially human-computer interface (HCI) related. As discussed in (Johnston et al., 2003) the interface of a system is important and cannot be neglected, particularly in a security environment. Thus redesigning of the e-mail clients' user


From John - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Type a question for help
Reply
Reply to All
Forward

From: John Doe [john@sabanciuniv.edu] Sent: Mon 3/26/2007 2:16 PM
To: Albert Levi
Cc:
Subject: From John
Signed By: john@sabanciuniv.edu

```
Dear Albert,

Just to inform you that I am not a fictitious person any more. I sign,
therefore I am.

Best
John
```

Fig. 6 – E-mail window of MS Outlook XP; signature verification message and the icon are separated from header.



From: John Doe [john@sabanciuniv.edu] Sent: Mon 3/26/2007 2:16 PM
To: Albert Levi
Cc:
Subject: From John
Signed By: john@sabanciuniv.edu

Dear Albert,

Just to inform you that I am not a fictitious person any more. I sign, therefore I am.

Best
John

Fig. 7 – E-mail window of MS Outlook 2007; signature verification message and the icon are at the end of the header, but not separated from header.

interface to capture the attendance of the users in case of security problem would improve the overall security of the system. In this section, we first outline the GUI criteria that address the problems identified in Section 3. Then, we analyze how the current e-mail clients meet these criteria and define an ideal GUI. During our analyses, we considered six different e-mail client programs that support S/MIME. These are namely MS Outlook Express, MS Outlook XP, MS Outlook 2007, Netscape Messenger 7.2, Mozilla Thunderbird 1.5.0.10, and Eudora 7.1 with S/MIME plugin. The characteristics that meet the criteria are shown in italic in the analysis tables. The analysis tables also show the characteristics of an ideal GUI. Moreover, the ideal GUI is developed as an extension to Mozilla Thunderbird.

The criteria that we considered are grouped under three categories:

- The scope of S/MIME signature
- The e-mail address control at verification
- Relaying the certificate information to the verifier

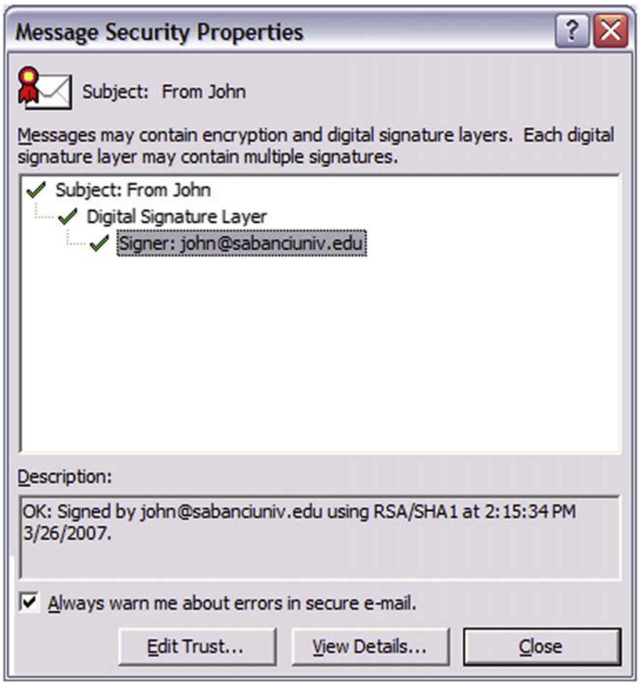
4.1. *GUI criteria for the scope of signature*

As mentioned in Section 3.3, the scope of an S/MIME signature is the body of the message, not the headers. The GUI should reflect this fact in both verification and signing.

Clear statement about the signature scope (verification): The basic way to convey the scope of S/MIME signature verification

Table 2 – Analysis of GUI criteria for the e-mail address control at verification (part 1).

	Message about e-mail address verification		Relaying name information stored in certificate	
	Place and reachability	Form of presentation	Place and reachability	Form of presentation
Ideal GUI	*0-click on the e-mail window; separated from header.*	*Bound to the signature or signer.*	*1-click in separate dialog box.*	*Not bound to the signature or signer*
Netscape Messenger 7.2	1-click in separate dialog box	*Bound to the signature/signer*	*1-click in separate dialog box.*	Bound to the signature/ signer
Mozilla Thunderbird 1.5.0.10	1-click in separate dialog box	*Bound to the signature/signer*	*1-click in separate dialog box.*	Bound to the signature/ signer
MS Outlook Express 6	0-click (part of the header) and 1-click in separate dialog box	0-click message does not have the e-mail address. *1-click message is bound to the signature/signer*	3-click in separate dialog box	*Not bound to the signature or signer*
MS Outlook XP	*0-click, separated from header (and also 1-click in separate dialog box)*	*Bound to the signature/signer*	3-click in separate dialog box	*Not bound to the signature or signer*
MS Outlook 2007	0-click, but at header; 1-click in separate dialog box	*Bound to the signature/signer*	4-click in separate dialog box	*Not bound to the signature or signer*
Eudora 7.1 (with S/MIME plugin)	Message on the e-mail window only says that the e-mail is signed but does not say who signed it.		Name information of certificate is not accessible	



Message Security Properties

Subject: From John

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

✓ Subject: From John
✓ Digital Signature Layer
✓ Signer: john@sabanciuniv.edu

Description:

OK: Signed by john@sabanciuniv.edu using RSA/SHA1 at 2:15:34 PM 3/26/2007.

☑ Always warn me about errors in secure e-mail.

Fig. 8 – 1-click window of Outlook XP that shows the signer's e-mail address.

is having a clear statement that specifies that the signature does not verify the header, but verifies only the body of the message. This message should appear in the window that e-mail is shown to the verifier.

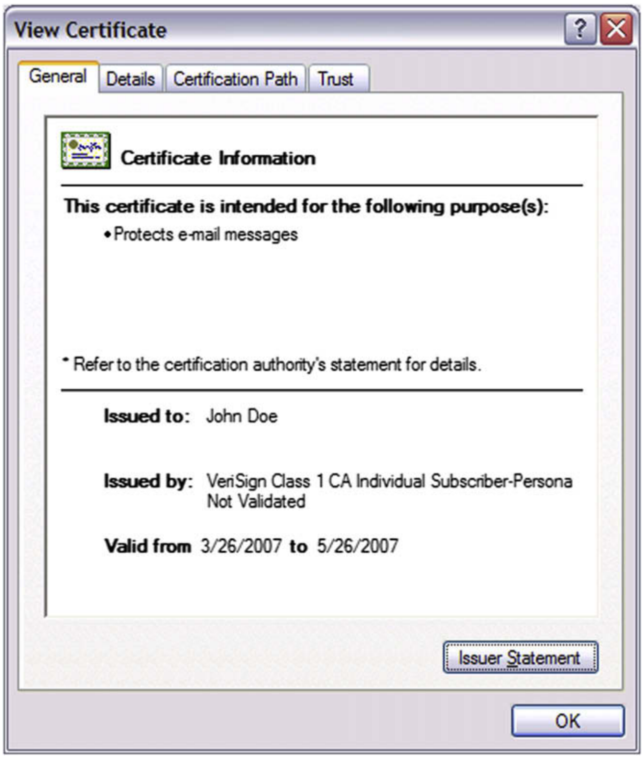
Clear statement about the signature scope (signing): Not only the verifier, but also the signer should be informed about the scope of S/MIME digital signature while signing. Thus, whenever the signer selects the option to digitally sign a message, there should be a clear message that mentions that the scope of the signature does not contain the header. Preferably, the signer should be advised to include its name and other information needed to be signed in the body of the message.

Other precautions at the verification phase that may reduce the possibility of misunderstanding that the header is protected are the followings:

No verification message/icon at the header display: The icon or the message of verification should not appear on the header part of the e-mail window, because having such a verification indication at the header part makes the users to think that verification starts from that point. The best part to put a signature verification message and/or an icon is the beginning of the message body or between message body and the header.

No verification icon at the preview pane: There should not be an icon which shows that the message is signed in the message list part of the preview pane. The reason is that in this list only the header information is shown. Since the header is not protected, seeing a signature indication there may mislead the users.

As shown in Table 1, none of the-mail clients that we examined have a statement about the scope of S/MIME signature in both signing and verification. Regarding the



View Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Protects e-mail messages

* Refer to the certification authority's statement for details.

Issued to: John Doe

Issued by: VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

Valid from 3/26/2007 to 5/26/2007

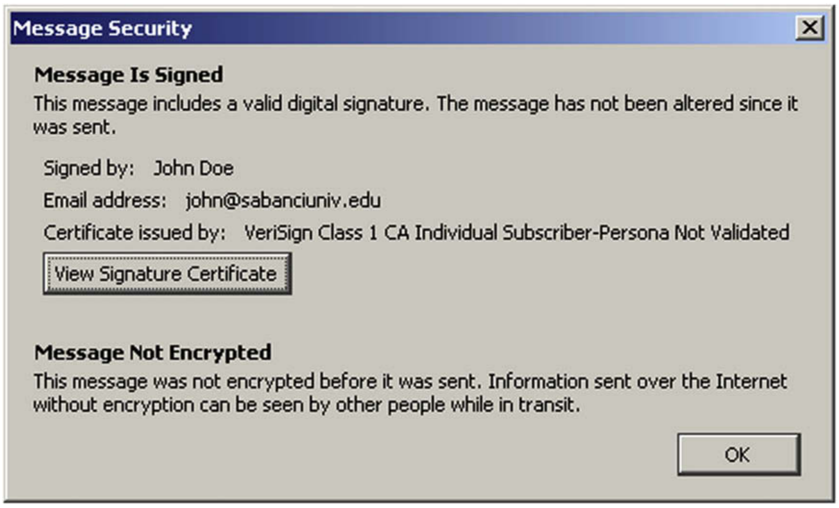
Fig. 9 – The window of Outlook XP that shows the name on the certificate.

precautions, Eudora has the best precaution since it does not have an icon or message at both header and the preview pane. As shown in Fig. 5, Eudora has a verification message in the message body, just before the actual message. In Outlook XP, the verification message and the icon are between the message and the header, and separated from the header with a line (Fig. 6). Outlook 2007 also has a similar icon and message at the end of the header part, but unlike Outlook XP, they look like parts of the header (Fig. 7). Netscape and Thunderbird, as shown in Fig. 2b, only have an icon of pen shape. Among these e-mail clients, the worst (i.e. the most misleading) header is the one of Outlook Express, since both icon and message mislead user as shown in Fig. 2a.

4.2. *GUI criteria for the e-mail address control at verification*

As mentioned in Section 2.2 and several parts of Section 3, S/MIME standards enforce the verifying software to cross-check the e-mail address on the certificate and the one in the e-mail headers. The GUI should contain several issues related with this control.

Message about e-mail address verification: The fact that the verification process only checks the e-mail address of the sender as the identity should be visualized by the verifier. The best way of doing this is to have a text message which says that the message was signed by the sender's e-mail address. In other words, this message should bind the signature or the signer to the e-mail address. This message should appear on the e-mail window so that the verifier should not click on



Message Security

Message Is Signed

This message includes a valid digital signature. The message has not been altered since it was sent.

Signed by: John Doe

Email address: john@sabanciuniv.edu

Certificate issued by: VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

Message Not Encrypted

This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.

Fig. 10 – 1-click window of Thunderbird that shows the signer's e-mail address and name.

something to view this information. We characterize this type of reachability as ''0-click'' (in general, we define ''*n*-click reachability'' where *n* is the number of clicks needed to get that window). Since conceptually the signature does not cover header, the GUI should also reflect this fact by separating this message from the header.

Relaying name information stored in certificate: In the message described in previous criterion, the sender's name must be deliberately hidden from the verifier since the standard S/MIME verification process does not verify the name. On the other hand, if the name information is included in the signer's certificate, this certificate field should be relayed to the user. This is because of the fact that some attacks are based on name spoofing as explained in Section 3.2 and visualization of this certificate field would warn the user about the attack. The ideal place to show the name field of certificate is on a separate window or dialog box that can be reachable at 1-click. However, the phrase should never bind the name to the signature; instead name should be cited as a certificate field only.

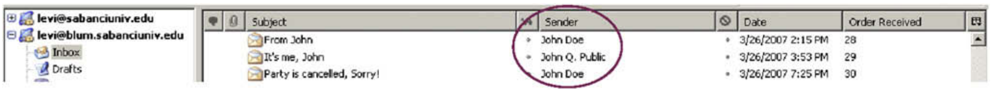
Warning about e-mail address inconsistency: In case of an inconsistency between the e-mail address in the signer certificate and the e-mail address at the message header (''from'' header), the verifying user must be warned. This warning may be a text message or an icon that reflects the situation.

Name information in the header: The ''from'' part of the e-mail headers may contain both name and e-mail address of the sender. Some e-mail clients may show both name and the address on the header part of the message window. However, some others may show only the name. Having only name information in the header part of the e-mail window may cause the verifier to wrongfully think that message is signed by that person independent of the e-mail address. As mentioned before, name control is not performed during the S/MIME signature verification. Therefore, showing only the name in the header is misleading; the e-mail clients should show only e-mail address or both address and the name together.

Name information in the preview pane: Due to the reasons explained in the previous paragraph, the name information should not be the only sender information to be shown on the preview pane as well. Instead the preview pane should display

Table 3 – Analysis of GUI criteria for the e-mail address control at verification (part 2).

	Warning about e-mail address inconsistency	Name information in the header	Name information in the preview pane
Ideal GUI	*Warning is issued as an icon and/or text*	*Only e-mail address OR name + e-mail address*	*Only e-mail address OR name + e-mail address*
Netscape Messenger 7.2	*Warning is issued as a special icon (a pen with a question mark). Detailed explanation is available upon click on the icon*	*Name + e-mail address*	Only name
Mozilla Thunderbird 1.5.0.10	*Warning is issued as a special icon. Detailed explanation is available upon click on the icon*	*Name + e-mail address*	Only name
MS Outlook Express 6	*Warning is issued as a special icon and an explanation. No click is needed to see the explanation.*	Only name	Only name
MS Outlook XP	No warning is issued	*Name + e-mail address*	Only name
MS Outlook 2007	No warning is issued	*Name + e-mail address*	Only name
Eudora 7.1 (with S/MIME plugin)	*Warning is issued as a message. No icon exists.*	*Name + e-mail address*	Only name



Subject	Sender	Date	Order Received
From John	John Doe	3/26/2007 2:15 PM	28
It's me, John	John Q. Public	3/26/2007 3:53 PM	29
Party is cancelled, Sorry!	John Doe	3/26/2007 7:25 PM	30

Fig. 11 – Partial preview pane of Thunderbird; only sender's name, not the e-mail address, is listed.

either the e-mail address of the sender or both address and name together.

S/MIME signature verification actually covers various controls, such as certificate validation, content alteration, etc., in addition to e-mail address crosscheck. The GUI requirements for all controls are not discussed in this paper for the sake of brevity and since these controls are not directly related to the attacks covered in Section 3.

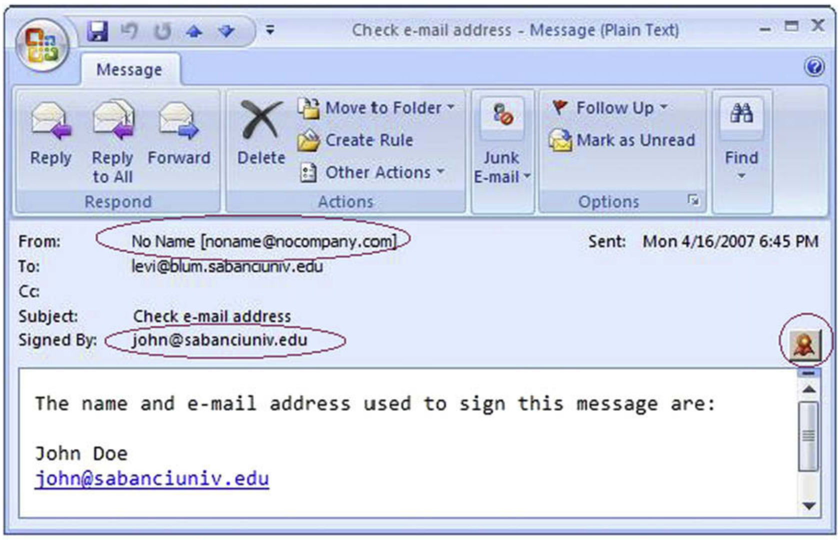
The analysis for the first two criteria is given in Table 2. As can be seen there, none of the e-mail clients that we analyzed meet all the criteria. However, except Eudora that fails in all aspects, other clients can be improved easily. All clients, except Outlook XP, either display the e-mail verification message at 1-click or at 0-click but at header. This message should be displayed at 0-click separated from header; this is doable. As a good example, the e-mail window of MS Outlook XP is showed in Fig. 6. Outlook 2007 e-mail window is similar to Outlook XP (Fig. 7), but the message looks like part of the header. Moreover, Outlook products are successful in showing the e-mail address properly (i.e. bound to the signature and/or signer) in 1-click windows. For example, 1-click window of Outlook XP is shown in Fig. 8. All Outlook products show the name information with a proper GUI (e.g. for MS Outlook XP, see Fig. 9) and message but they are displayed a bit late; they should move the window at which they show the name to 1-click. Finally, Netscape and Thunderbird should improve their GUIs by unbinding the name information from the signature and signer. The 1-click window of Thunderbird is given in Fig. 10. As can be seen from this figure, the e-mail address message meets the criteria, but the name message does not since it is bound to the signer/signature.

The analysis for the last three criteria is given in Table 3. Although most clients (except Outlook Express) contain e-mail addresses in the header, none of the clients do so in the preview pane. The preview pane of Thunderbird is given in Fig. 11 as an example.

Except the Outlook family (XP and 2007), all clients perform e-mail address crosscheck and relay this control to the verifiers as icons and/or messages. No crosscheck is performed and signature is considered as verified in MS Outlook 2007 and XP even if the e-mail address in the message header and the e-mail address in the certificate are different. Although this seems against S/MIME standard requirements, the verification message and the e-mail header show the e-mail address differences as shown in Fig. 12 (for Outlook 2007). However, the verifying user must examine the GUI and realize this problem on his/her own; this may not be easy for an average user.

4.3. GUI criteria about relaying the certificate information to the verifier

The S/MIME verifying software should first verify the signer certificate as mentioned in Section 2.2. However, the only verified binding between certificate and the message is the e-mail address of the sender. The criteria related with relaying this fact to the verifier has been detailed in the previous section. Moreover, the criteria related with relaying the name field of the certificate to the verifier are also discussed there. On the other hand, without properly showing the content of the signer's certificate to the verifier, the verification process cannot be fully comprehended by the verifier, but the



From: No Name [noname@nocompany.com]
Sent: Mon 4/16/2007 6:45 PM
To: levi@blum.sabanciuniv.edu
Cc:
Subject: Check e-mail address
Signed By: john@sabanciuniv.edu

```
The name and e-mail address used to sign this message are:

John Doe
john@sabanciuniv.edu
```

Fig. 12 – Outlook 2007 GUI shows differences in e-mail addresses even if the signature is shown as verified.

Table 4 – Analysis of GUI criteria about relaying the certificate information to the verifier.

	CA certification practice	Link to CPS	Full certificate details
Ideal GUI	*Brief summary*	*Accessible in 1–3 clicks*	*Accessible in 2–3 clicks*
Netscape Messenger 7.2	Does not exist	No link	2-click
Mozilla Thunderbird 1.5.0.10	Does not exist	No link	2-click
MS Outlook Express 6	Does not exist	4-click	4-click
MS Outlook XP	Does not exist	4-click	3-click
MS Outlook 2007	Does not exist	5-click	4-click
Eudora 7.1 (with S/MIME plugin)	Does not exist	No link	Does not exist

visualization of information in the certificate and the visualization of the verification results should be separated. The reason is that by verifying the signer's certificate during the verification process, the verifying system verifies only the CA signature on the certificate; the reliability of the information contained in the certificate depends on the CPS of the CA that must be assessed by the verifying user. The GUI considerations about relaying the certificate information to the verifier are discussed below.

CA certification practice: Displaying a brief summary of the CA certification practice would be a good idea to inform average users about the ID verification mechanism employed by the CA. In this way, the limitations of the class-1 certificates could be explained to the verifiers.

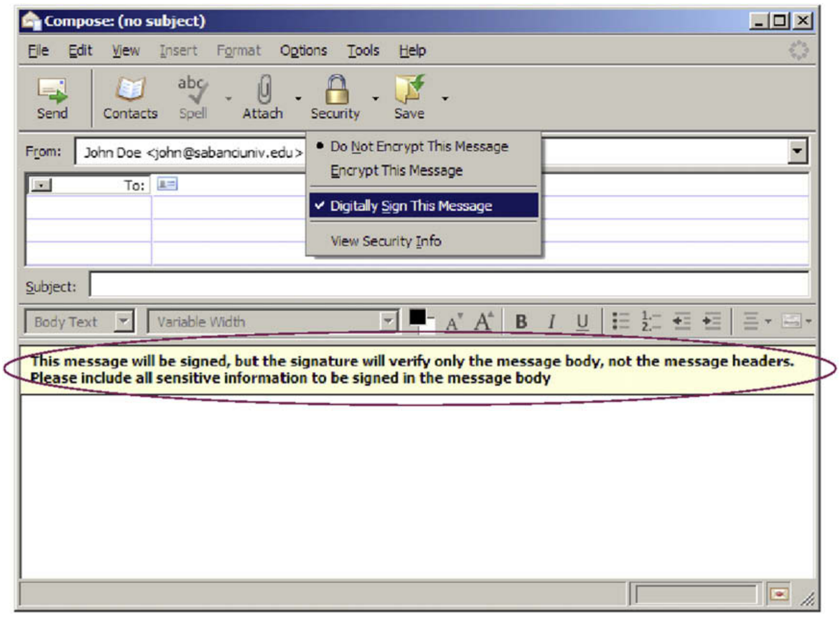
Link to CPS: Advanced and interested verifiers may need to read the CPS of the CA in order to learn more about the CA's certification practice. Such a link should be accessible via a few links from the message window.

Full certificate details: Again for interested and advanced users, all fields of the signer's certificate could be shown. However, in order not to confuse the average users, such a detailed visualization should not be directly reachable from the message window; instead 2 or 3 clicks should have been done to reach the full certificate details.

As shown in Table 4, Eudora does not display any certificate information. Thus it directly fails these criteria. Moreover, none of the clients that we tested display a brief summary of CA's certification practice. Netscape and Thunderbird do not contain a link to CPS. Outlook family products display necessary certificate information and have a link to CPS; however, they mostly are displayed a bit late so that the user should make several clicks to reach this information.

4.4. *Ideal GUI*

We develop an add-on to Mozilla Thunderbird for the ideal GUI described in the previous sections. As shown in Fig. 13, a clear statement about the scope of signature is added to the signing operation. Moreover, another message about the scope of digital signature verification is added to 0-click message window. As shown in Fig. 14, this message binds the signature and the signer to the e-mail address, which is a requirement from ideal GUI as mentioned in Section 4.2. Furthermore, this message and the corresponding icon have been separated from the header as mentioned in Section 4.1 as another ideal GUI requirement. This add-on can be downloaded from http://people.sabanciuniv.edu/levi/SMIME-GUI-addon/.

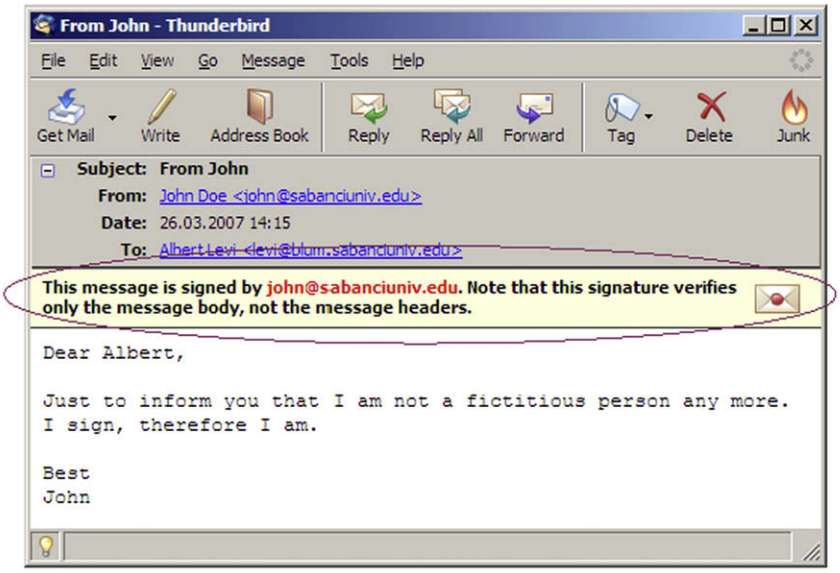


From: John Doe <john@sabanciuniv.edu>

Subject:

This message will be signed, but the signature will verify only the message body, not the message headers. Please include all sensitive information to be signed in the message body

Fig. 13 – Ideal GUI: Message about the scope of the digital signature while signing.



Subject: From John
From: John Doe <john@sabanciuniv.edu>
Date: 26.03.2007 14:15
To: Albert Levi <levi@blum.sabanciuniv.edu>

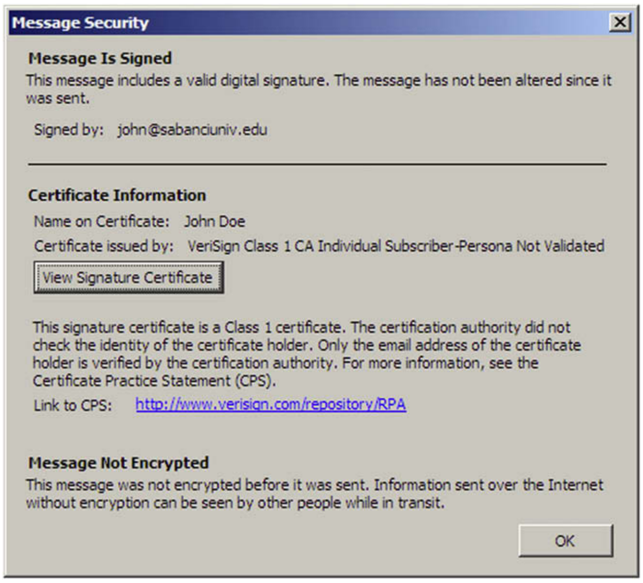
This message is signed by john@sabanciuniv.edu. Note that this signature verifies only the message body, not the message headers.

```
Dear Albert,

Just to inform you that I am not a fictitious person any more.
I sign, therefore I am.

Best
John
```

Fig. 14 – Ideal GUI: Message about the scope of the digital signature verification.

The 1-click window of the ideal GUI that appears upon pressing the verification icon is shown in Fig. 15. This window is, actually, the modified version of Fig. 10 according to the ideal GUI criteria given in Sections 4.2 and 4.3. In the messages of this window, signature is bound to the e-mail address, but the name on the certificate is relayed to the verifier without binding to the signature as mentioned in Section 4.2 as an ideal GUI requirement. Moreover, a brief summary for the CA certification practice and a link to CPS is added to this window in accordance with the ideal GUI requirements specified in Section 4.3.

As mentioned in Section 4.2, ideal GUI should include a warning in case of inconsistency between the e-mail address in the ‘‘from’’ message header and the e-mail address in the certificate. Fig. 16 shows the warning of the 0-click message window. Fig. 17 shows 1-click window at which a detailed message and the inconsistent e-mail addresses are shown.



Message Is Signed

This message includes a valid digital signature. The message has not been altered since it was sent.

Signed by: john@sabanciuniv.edu

Certificate Information

Name on Certificate: John Doe

Certificate issued by: VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

This signature certificate is a Class 1 certificate. The certification authority did not check the identity of the certificate holder. Only the email address of the certificate holder is verified by the certification authority. For more information, see the Certificate Practice Statement (CPS).

Link to CPS: http://www.verisign.com/repository/RPA

Message Not Encrypted

This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.

Fig 15 – Ideal GUI: 1-click window of successful verification.

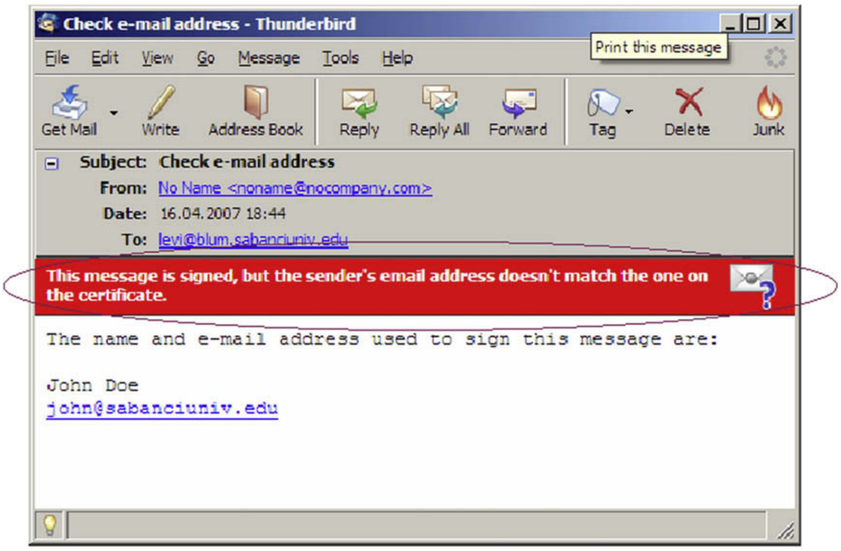
Another ideal GUI requirement is that the preview pane should display either the e-mail address of the sender or both address and name together. We have developed our Thunderbird add-on such that the user can optionally display only e-mail address (Fig. 18a) or e-mail address and name together (Fig. 18b) in the preview pane.

In order to evaluate the effectiveness of the GUI that was proposed in this section, we conduct a survey among 115 sophomore year university students who are ordinary computer users. In this survey, we used two screenshots similar to Fig. 14 and Fig. 16 and evaluate the user perception about (a) the entity who signed the message for class 1 certificate case, (b) the scope of signature, and (c) the interpretation of the error message shown in Fig. 16. We reach the following results by this survey. 68% of the respondents are aware that a signed message is signed and sent by the user that holds the account of the email address shown in header, but the identity is not guaranteed by the signature. 81% of the respondents are aware that the scope of signature does not include subject and date, but includes message body. 66% of the respondents correctly comprehend the erroneous case shown in Fig. 16 such that it implies the message is signed, but the signer is not known.

5. Discussions and conclusions

In this paper, we identified some problems of the S/MIME standard for digital signatures in e-mails. We proposed some solutions and an ideal GUI for the best comprehension of S/MIME signatures. We also comparatively analyzed some existing e-mail clients to evaluate their GUIs.

S/MIME effort is to add cryptographic security in e-mails using PKIX public key certificates. S/MIME uses e-mail addresses for identification, while certificates use both names

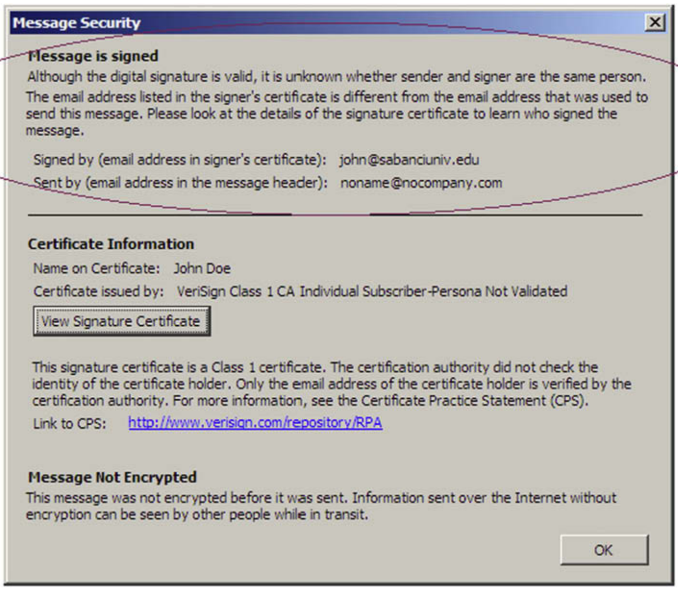


Subject: Check e-mail address
From: No Name <noname@nocompany.com>
Date: 16.04.2007 18:44
To: levi@blum.sabanciuniv.edu

This message is signed, but the sender's email address doesn't match the one on the certificate.

```
The name and e-mail address used to sign this message are:

John Doe
john@sabanciuniv.edu
```

Fig. 16 – Ideal GUI: Message displayed in case of e-mail address inconsistency during verification.



Message is signed

Although the digital signature is valid, it is unknown whether sender and signer are the same person. The email address listed in the signer's certificate is different from the email address that was used to send this message. Please look at the details of the signature certificate to learn who signed the message.

Signed by (email address in signer's certificate): john@sabanciuniv.edu
Sent by (email address in the message header): noname@nocompany.com

Certificate Information

Name on Certificate: John Doe
Certificate issued by: VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

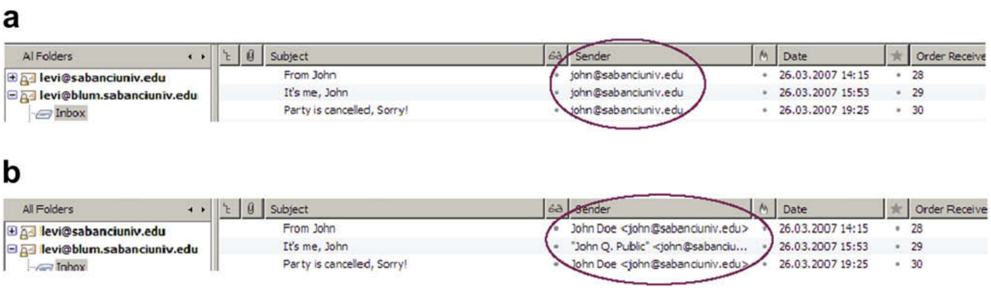
This signature certificate is a Class 1 certificate. The certification authority did not check the identity of the certificate holder. Only the email address of the certificate holder is verified by the certification authority. For more information, see the Certificate Practice Statement (CPS).

Link to CPS: http://www.verisign.com/repository/RPA

Message Not Encrypted

This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.

Fig. 17 – Ideal GUI: 1-click window in case of e-mail address inconsistency during verification.



Subject	Sender	Date	Order Receive
From John	john@sabanciuniv.edu	26.03.2007 14:15	28
It's me, John	john@sabanciuniv.edu	26.03.2007 15:53	29
Party is cancelled, Sorry!	john@sabanciuniv.edu	26.03.2007 19:25	30

Subject	Sender	Date	Order Receive
From John	John Doe <john@sabanciuniv.edu>	26.03.2007 14:15	28
It's me, John	"John Q. Public" <john@sabanciu...	26.03.2007 15:53	29
Party is cancelled, Sorry!	John Doe <john@sabanciuniv.edu>	26.03.2007 19:25	30

Fig. 18 – Preview pane of ideal GUI: (a) only e-mail address, (b) e-mail address and name.

and e-mail addresses. Several controls about the certificates are performed and PKIX rules are enforced in certificate validation, but not all of those controls directly affect the e-mail message that is the actual object to be verified. Regardless of strict identity check in certificate issuance, names in certificates are not tied to the e-mail messages in S/MIME. The only connection between a certificate and an e-mail message is the e-mail address. That fact enforces the recipients to know their parties by e-mail addresses, not by names. Moreover, certification practices of some CAs allow class-1 certificates to include invalidated names in it. Verifier should examine the certificate details thoroughly and use his/her judgment, not the e-mail client program's, in order not to be deceived in such cases.

S/MIME version 3.0 (Ramsdell, 1999b) does not ensure the integrity of the e-mail headers. S/MIME version 3.1 (Ramsdell, 2004b) proposes a nonstandard cryptographic header protection mechanism. However, this is not so easy to adapt in current e-mail client implementation. Therefore, as of this writing, none of the e-mail clients implemented header protection of S/MIME 3.1 in their products. Until header protection is successfully designed and implemented, it is preferable not to rely on the header information. Another way of saying is that the recipient should trust only what is written in the message body.

There is an important dilemma here. Limitations of S/MIME require the e-mail users to be more careful and perform off-line checks while accepting a digitally signed message. On the other hand, an ordinary user, who does not have enough information about security and cryptography, has a tendency to trust what his/her e-mail client says. He/she prefers automatic controls and easy-to-understand GUIs and warnings. Some discussions in S/MIME WG show that e-mail client systems will be able to provide more controls and easy-to-understand warnings in the future. However, one should not expect all of those controls as mandatory features in products with S/MIME support, at least until all potential interoperability problems among S/MIME, regular e-mail services, SMTP servers and certification services are identified and resolved. Indeed, none of the existing e-mail client GUIs are perfect in the sense that they provide all necessary controls and relay these controls to the users in a proper way.

REFERENCES

Freed N, Borenstein N. Multipurpose Internet Mail Extensions (MIME) part one: format of internet message bodies, RFC 2045; 1996.

Freed N, Borenstein N. Multipurpose Internet Mail Extensions (MIME) part two: media types, RFC 2046; 1996.

Freed N, Borenstein N. Multipurpose Internet Mail Extensions (MIME) part five: conformance criteria and examples, RFC 2049; 1996.

Freed N, Klensin J. Multipurpose Internet Mail Extensions (MIME) part four: registration procedures, RFC 4289; 2005.

Furnell S. Why users cannot use security. Computers & Security 2005;24(4):274–9. Elsevier.

Furnell S, Jusoh MA, Katsabas D. The challenges of understanding and using security: a survey of end-users. Computers & Security 2006;25(1):27–35. Elsevier.

ITU-T. Recommendation X.509, ISO/IEC 9594-8. Information Technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate Frameworks. 4th ed.; 2000.

Johnston J, Eloff JHP, Labuschagne L. Security and human computer interfaces. Computers & Security 2003;22(8):675–84. Elsevier.

Klensin J, editor. Simple mail transfer protocol, RFC 2821; 2001.

Levi A. Digital certificates. In: Bidgoli H, editor. The handbook of information security, vol. 1. Wiley; 2006. p. 823–35.

Moore K. MIME (Multipurpose Internet Mail Extensions) part three: message header extensions for non-ASCII text, RFC 2047; 1996.

PKIX Working Group. Public-Key Infrastructure (X.509) (pkix) Charter, http://www.ietf.org/html.charters/pkix-charter.html; 2008 [accessed 17.10.08].

Ramsdell B, editor. S/MIME Version 3 certificate handling, RFC 2632; 1999.

Ramsdell B, editor. S/MIME Version 3 message specification, RFC 2633; 1999.

Ramsdell B, editor. S/MIME Version 3.1 certificate handling, RFC 3850; 2004.

Ramsdell B, editor. S/MIME Version 3.1 message specification, RFC 3851; 2004.

Resnick P, editor. Internet message format, RFC 2822; 2001.

RSA Laboratories. Public-Key Cryptography Standards (PKCS), http://www.rsasecurity.com/rsalabs/pkcs/; 2008 [accessed 17.10.08].

S/MIME Working Group. S/MIME Mail Security (smime) Charter, http://www.ietf.org/html.charters/smime-charter.html; 2008 [accessed 17.10.08].

Stallings W. Cryptography and network security principles and practice. 4th ed. Prentice-Hall; 2006 [chapter 15].

Whitten A, Tygar JD. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: Proceedings of the 8th USENIX Security Symposium, Washington, D.C., USA, August; 1999.

Albert Levi received B.S., M.S. and Ph.D. degrees in computer engineering from Boğaziçi University, Istanbul, Turkey, in 1991, 1993 and 1999, respectively. He served as a visiting faculty member in the Department of Electrical and Computer Engineering, Oregon State University, USA, between 1999 and 2002. He was also a postdoctoral research associate in the Information Security Lab of the same department. Since 2002, he is a faculty member of Computer Science and Engineering in Sabanc? University, Faculty of Engineering and Natural Sciences, Istanbul, Turkey and co-director of Cryptography and Information Security Group (CISEC). He is promoted to associate professor level in January 2008. His research interests include computer and network security with emphasis on mobile and wireless system security, public key infrastructures (PKI), and application layer security protocols. He has served as the general chair of ISCIS 2006, SecureComm 2008 and as technical program committee member of various symposia and conferences. He is a member of IEEE, ACM, IEEE Computer Society, IEEE ComSoc, ACM SIGSAC and ACM SIGCOMM.

Can Berk Güder is an M.S. candidate in Computer Science and Engineering at Sabancı University. He acquired his B.S. degree in Computer Science and Engineering from Sabancı University in 2007. He served as webmaster co-chair of SecureComm 2008. His research interests include routing protocols for vehicular networks, e-mail security and natural language processing.