Forging Digital Signatures

Albert Levi
Sabanci University
Istanbul, TURKEY
levi@sabanciuniv.edu

ACSAC 2002
Outline

• What’s a digital signature?
• How S/MIME handles digital signatures?
• How to obtain a certificate (a.k.a. digital ID)
• Tricks that you can do to get a bogus certificate
  - Sending a signed message using other’s name
• Scope of a S/MIME signature and related problems
  - How to interpret a digital signature?
What is Digital Signature?

• Cryptographic processing over the message
• Uses public-key cryptography
In More Cryptographic Terms (e.g. RSA)

- **Message**
- **Cryptosystem**
- **Hash Algorithm**
- **Hash**
- **Signature**
- **Private Key**
- **Public Key**
- **Hash**
- **Hash Algorithm**

Sender

Receiver

=?
S/MIME

- Secure/Multipurpose Internet Mail Extensions
- A standard way for email encryption and signing
- IETF effort (RFCs 2632, 2633, 2634)
- Industry support
- Not a standalone software, a system that is to be supported by email clients
- Previous slide shows how S/MIME handles digital signatures
- Also provides encryption
Quick E-mail History

- SMTP and RFC 822
  - only ASCII messages
- MIME (Multipurpose Internet Mail Extensions)
  - content type
    - Almost any of information can appear in an email message
- S/MIME: Secure MIME
  - new content types, like signature, encrypted data
Certificates

• Finding out correct public key of a user
  - Endorsed binding between the public key and the owner
  - Endorsed by a trusted Certification Authority (CA)
    • via CA’s signature over the certificate

• How to determine user
  - by name?
  - by e-mail address?
Certificate Management in S/MIME

• CA-centered
• CA certificates come with the client software
• An ordinary user is not aware of the CAs that he/she trusts
• Certificates are sent along with the signed messages
Certificate Management in S/MIME

- One should get a certificate from a CA in order to send signed messages
- Certificates classes (common practice by most CAs)
  - Class 1
  - Class 2
  - Class 3
- CA certification policies (Certificate Practice Statement)
  - ID-control practices
    - Class 1: only email address
    - Class 2: against third party database
    - Class 3: apply in person and submit picture IDs and/or hard documentation
Attack 1: Class 1 Certificate Attack

- No identity check during registration
- Binding between public key and e-mail address
- It is possible to enroll under a different name
  - Name spoofing is possible in signed messages
- E-mail clients do not make this fact explicit to average users
Attack 1: Class 1 Certificate Attack

- Step 1: Get an e-mail address that implies the person you want to imitate
- Step 2: Register for a certificate with that bogus name and e-mail address
- Step 3: Step up an outgoing e-mail account at your favorite e-mail client software with that bogus name
- Step 4: Send bogus signed messages
Step 2: Registration

Personal Digital ID Enrollment

You are about to begin the enrollment process for a Class 1 Digital ID. Enrollment can be completed online within a few minutes. Your Class 1 Digital ID is bound to your validated e-mail address and can be used to digitally sign your e-mail and receive encrypted e-mail. It can also be used by your Web browser as the equivalent of an electronic membership card or passport to identify yourself to participating Web sites that wish to restrict access, eliminating the need to remember usernames and passwords.

INTERNATIONAL CUSTOMERS: You should enroll for your Class 1 individual certificate through your LOCAL AFFILIATE.

If you want a Digital ID to send secure e-mail from an e-mail package other than Microsoft Outlook Express, Microsoft Outlook, or Netscape Messenger please click here.

Class 1 Digital ID:

- Authenticates your e-mail address
- Automatic listing in our public directory and easy lookup of anyone else's Digital ID
- US $1,000 of NetSure™ protection against economic loss caused by corruption, loss, or misuse of your Digital ID
- Free revocation and replacement if your Digital ID is lost or corrupted

US $14.95 per year, or free 60 day trial edition
Payable by Visa, MasterCard, American Express and Discover
Step 2: Registration

Step 1 of 4: Complete Enrollment Form

Contents of Your Digital ID
Fill in all fields. Use only the English alphabet with no accented characters. This information is included in your Digital ID and is available to the public.

First Name:
Nickname or middle initial allowed (example – Jack B.)
Jay

Last Name:
(example – Doe)
Leno

Your E-mail Address:
(example – jaboer@xerox.com)
jayerno_show@yahoo.com

Challenge Phrase
This unique phrase protects you against unauthorized action on your Digital ID and should not be shared with anyone. Do not lose it! It is required to revoke, replace, renew or set preferences for your Digital ID.

Enter Challenge Phrase:
Do not use any punctuation

Choose a Full-service Class 1 Digital ID, or a 60-day Trial Class 1 Digital ID
Step 2: Registration

Digital ID Services

Step 2 of 4: Check E-mail

You should receive an e-mail from the Digital ID Center within the hour at the e-mail address you entered in the enrollment form. It will contain instructions for installing the Digital ID.
Step 2: Registration

To the recipient:

Date: Fri, 29 Nov 2002 06:51:08 -0800 (PST)
From: Digital ID Center <enrollee@company.com> | This is Spam | Add to Address Book

Subject: Trial Class 13 - Digital ID Pickup Instructions

**If you did not enroll for a Digital ID through [redacted] please do not follow the instructions below for picking up the ID.**

QUICK INSTALLATION INSTRUCTIONS

To ensure that someone else cannot obtain a Digital ID that contains your name and e-mail address, you must retrieve your Digital ID from secure web site using a unique Personal Identification Number (PIN).

Be sure to follow these steps using the same computer you used to begin the process.

Copy your Digital ID PIN
Your Digital ID PIN is: [redacted]

Go to [secure Digital ID Center](https://digitalid. company.com/enrollee/aspickup.htm)

Paste (or enter) your Digital ID PIN
Then select the SUMMIT button to install your Digital ID.

That's all there is to it!

INTERNATIONAL CUSTOMERS: International customers may be able to...
Step 2: Registration

Step 3 of 4: Pick up Digital ID

When picking up your ID, use the same machine and browser used for enrollment.

The Personal Identification Number (PIN) is needed to complete this step. It was contained in an e-mail message sent immediately after the enrollment form was submitted. This was sent from the Customer Support Department to the e-mail address entered in the enrollment form.

Copy the PIN number from the e-mail, paste (or enter) it into the box below, and click SUBMIT.

After the PIN is submitted, generating the Digital ID will take up to three minutes. Do not interrupt the browser until there is a response.

Enter the Digital ID Personal Identification Number (PIN): bbb8b104d4b4dc2e036b1b25a5b9c8c

Submit
Step 2: Registration

• Certificate is now installed
Step 3: Set up local account
Step 4: Send signed but bogus messages

Dear Albert,

I am writing to invite you to my show tomorrow.

Best,
Jay
What’s Wrong?

• Loose control for Class 1 certificates for commercial reasons
  - visibility
  - market share
• The system becomes less secure for the name of security
Attack 2: Use one’s certificate to send e-mails under another name

• Step 1: Set up another e-mail account at local client
  – Same e-mail address
  – But a different name

• Step 2: Send bogus signed messages
Step 1: Set up another account
Step 2: Send bogus signed message

Hi Albert,

Don't go the Jay's show, come to mine

Best

Larry
What’s Wrong?

• During verification, e-mail client does not match the name in certificate with the name in e-mail
  - Only e-mail addresses are matched (as mentioned in RFC 2632 (S/MIME Certificate Handling))
• Verifier’s manual check is needed
• Not a specific problem of class-1 certificates
  - Same attack is possible using class-2 and class-3 certificates
  - E-mail clients are not concerned with certificate classes
Attack 3: Forging the header

• The scope of a S/MIME signature does not include the e-mail header
  – from, to, cc, subject, date
• RFC 2633
  “S/MIME is used to secure MIME entities. A MIME entity may be a sub- part, sub-parts of a message, or the whole message with all its sub- parts. A MIME entity that is the whole message includes only the MIME headers and MIME body, and does not include the RFC-822 headers.”
• Indeed, the mail header is modified without changing the verification status
• Problem of all classes of certificates
Attack 3: Forging the header

- RFC 822 headers resemble envelopes
  - Signature of the letter does not cover the envelope
  - so the signature over the email “message” does not cover the RFC-822 header
  - But we do not write subject over the envelopes
What should be done?

• Class 1 certificates should be discontinued
  - All certificate must be issued with a personal presence requirement or by the approval of trusted registration authorities

• E-mail clients must be aware of certificate classes and issue appropriate warnings to the verifiers
What should be done?

• It is up to you whether to believe a digital signature is valid or not
  – Use your reasoning, not your e-mail client’s
• Try to identify people by their e-mail addresses
• Examine the details of certificate of the other party
• Do not trust Class 1 certificates
• Ask the sender to put all sensitive information within the message
  – Sender’s identity
  – Subject
  – Date
• Don’t let subject say all!