

S/MIME

Mathias Jeschke

Humboldt-Universität zu Berlin

Seminar: Interoperabilität und Sicherheit

23.11.2005

Einleitung

□ Motivation:

- ECHOLON (Stichwort: Betriebsspionage)
- Mailzustellung über SMTP geschieht evtl. über mehrere Server mit ungeklärter Vertrauensstatus
- Gleiches gilt für das Routing bei TCP/IP

□ Ziele von E-Mail-Verschlüsselung:

- Integrität
- Vertraulichkeit
- Authentizität

Einleitung – Begriffe

□ MUA – Mail User Agent (Mail-Client)

□ Mailheader 

```
From:Bob <bob@berlin.de>  
To: Alice <alice@berlin.de>  
Subject: Hallo Alice  
Date: Wed, 23 Nov 2005 00:00:00 +0100  
...
```

□ Mailbody 

```
Hallo Alice,  
Dies ist eine Mail  
nach RFC 822
```

Ziele des Vortrags

- ❑ X.509-Zertifikate (kurze Einleitung)
- ❑ MIME
- ❑ Format von S/MIME-basierten E-Mails:
 - Verschlüsselung
 - Signatur
 - Verschlüsselung, Signatur und Kompression
- ❑ Nicht Thema: Transport-Sicherung

Überblick

- S/MIME ist nicht auf E-Mail beschränkt
- kann überall eingesetzt werden, wo MIME eingesetzt wird (z.B. HTTP, Instant Messaging)

X.509-Zertifikate

- ❑ Grundlage von S/MIME
- ❑ Verknüpfen Pubkey mit Identität (beglaubigt durch den Aussteller)
- ❑ Benötigen vertrauenswürdige Instanz (CA) - zu Testzwecken kann solche mit OpenSSL erstellt werden

X.509-Zertifikate

- ❑ E-Mail-Zertifikate sollten Adresse in der subjectAltName-Erweiterung tragen, nicht im subjectDN!
- ❑ Zertifikate OHNE E-Mail-Adresse sind erlaubt, die Zuordnung muss dann der MUA treffen (Adressbuch)

X.509-Zertifikate

- Erweiterungen sollten – bis auf wenige Ausnahmen – keine kritischen Einträge enthalten
 - Ausnahmen:
 - Key Usage Certificate Extension (digitalSignature oder nonRepudation)
- Benutzte Hash-Algorithmen:
 - MD2 (Kompatibilität), MD5, SHA1

Zertifikat-Verteilung

- Zertifikate können:
 - In E-Mails eingebettet sein (Anhang)
 - Über ein gemeinsames Verzeichnis bezogen werden (z.B. LDAP)
 - Im MUA des Empfängers bereits installiert sein

CRLs - Rückruflisten

- ❑ Certificate Revocation Lists
- ❑ Sind von CA unterschrieben und haben Gültigkeitszeitraum
- ❑ Nach Möglichkeit sollte der MUA *immer* die aktuellste CRL von der CA holen
- ❑ CRLs können auch in der E-Mail eingebettet sein

Typische Probleme bei der Verifikation von Zertifikaten

- ❑ Absender(-adresse) passt nicht zum Zertifikat (z.B. bei PGP unkritisch?)
- ❑ Zertifikat-Kette führt zu keiner bekannten (vertrauenswürdigen) CA
- ❑ CRL ist abgelaufen
- ❑ Zertifikat ist abgelaufen
- ❑ Zertifikat wurde zurückgerufen

S/MIME – Exkurs: MIME

- Mail nach RFC 822:
 - Alphabet: 7-Bit-ASCII
 - Daher:
 - Keine Binärdateien (Programme, Bilder, ...)
 - Keine nationalen Zeichensätze (Umlaute, €)
 - Evtl. Probleme beim Übersetzen von SMTP (RFC 821) - Tabulatoren, Zeilenlängen, ...
- Lösung: Einheitliches Datenformat

S/MIME – Exkurs: MIME

- ❑ MIME = Multipurpose Internet Mail Extensions, beschrieben in RFC 2045-2049
- ❑ Neue Header-Felder:
 - MIME-Version: 1.0
 - Content-Type (z.B. text/plain, text/html)
 - Content-Transfer-Encoding, z.B.:
 - ❑ 7bit
 - ❑ base64
 - ❑ quoted-printable

S/MIME – Exkurs: MIME

□ Content-Typen

- Text: einfacher Text
- Multipart: mehrere Mailbodies mit eigenem MIME-Header
- Message: Einbettung von Mails nach RFC 822 und Fragmentierung möglich
- Image
- Video
- Audio
- Application: Anwendungsdaten, Bytesequenzen

S/MIME – Exkurs: MIME

- Content-Typen: multipart/mixed
 - Einzelne MIME-Teile werden durch so genannte „boundaries“ getrennt
 - Diese dürfen sonst nicht in der Mail vorkommen

```
From: Alice <alice@berlin.de>  
To: Bob <bob@berlin.de>  
Subject: Hallo Bob  
MIME-Version: 1.0  
Content-type: multipart/mixed; boundary="meine boundary"
```

```
--meine boundary
```

```
Content-type: text/plain; charset=us-ascii
```

```
Hallo Bob.
```

```
--meine boundary
```

```
Content-type: text/plain; charset=iso-8859-1
```

```
Hallo Bob ein weiteres Mal.
```

```
--meine boundary--
```

S/MIME-Anforderungen

- Algorithmen im S/MIME-Client:
 - Hash
 - SHA1 (vorgeschrieben)
 - MD5 (empfohlen)

 - Signaturverfahren
 - id-dsa-with-sha1 (vorgeschrieben)
 - RSA (vorgeschrieben)

S/MIME-Anforderungen

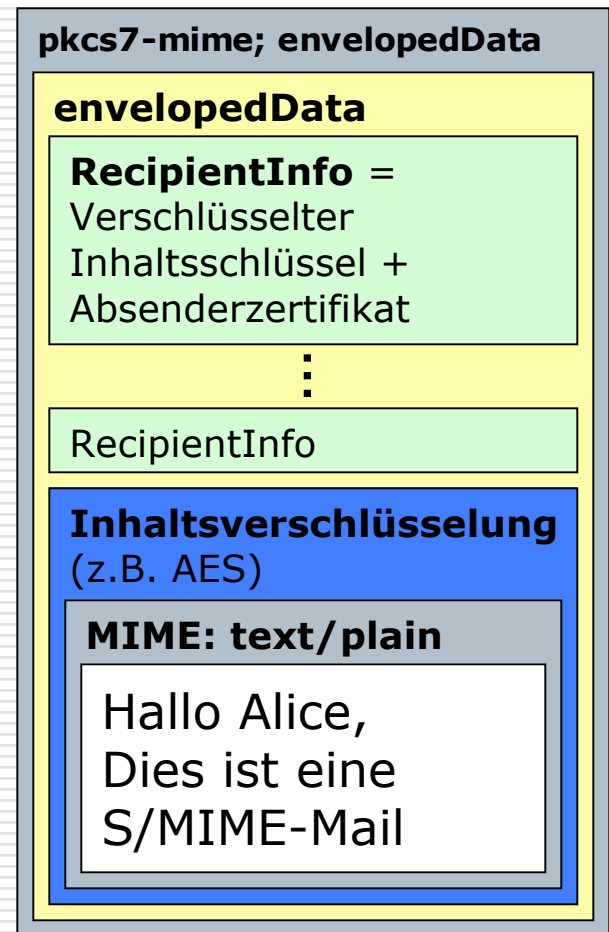
- Algorithmen im S/MIME-Client:
 - Verschlüsselung des symm. Schlüssels
 - RSA (vorgeschrieben)
 - Diffie-Hellman (empfohlen)

 - Symmetrische Inhalts-Verschlüsselung
 - 3DES (vorgeschrieben)
 - AES (128-256) (empfohlen)
 - RC2/40 (empfohlen)

S/MIME-Format

□ Verschlüsselung

1. Inhalts-(Sitzungs)-Schlüssel erzeugen
2. (MIME-)Inhalt verschlüsseln
3. Inhaltsschlüssel für **jeden** Empfänger mit seinem pubkey verschlüsseln und mit eigenem Zertifikat zusammen einpacken (**RecipientInfo**)
4. PKCS#7-Container erstellen
5. Versenden als **pkcs7-mime; smime-type=envelopedData**



S/MIME-Format

□ Verschlüsselung: Beispiel

```
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;  
          name=smime.p7m
```

```
Content-Transfer-Encoding: base64
```

```
Content-Disposition: attachment; filename=smime.p7m
```

```
rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT6  
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H  
f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4  
0GhIGfHfQbnj756YT64V
```

S/MIME-Format

- Verschlüsselung: Auswahl des Inhaltsschlüssels
 - Sender liefert immer Präferenz-Liste der Algorithmen mit
 - Falls solche Liste für den Empfänger vorhanden (aus vergangener Kommunikation) benutze diese
 - Sonst benutze 3DES
 - Bei mehreren Empfängern nicht „starke“ und „schwache“ Algorithmen mischen

S/MIME-Format

- Signatur
(PKCS#7 - signedData)
 - Robust gegen Transformationen auf dem Transportweg
(eigener MIME-Typ)
 - Klartext nur von S/MIME-fähigen MUAs darstellbar



S/MIME-Format

□ Signatur (PKCS#7 - signedData) : Beispiel

```
Content-Type: application/pkcs7-mime; smime-type=signed-data;  
          name=smime.p7m
```

```
Content-Transfer-Encoding: base64
```

```
Content-Disposition: attachment; filename=smime.p7m
```

```
567GhIGfHfYT6ghyHhHUujpfyF4f8HHGTrfvhJhjH776tbB9HG4VQbnj7  
77n8HHGT9HG4VQpfyF467GhIGfHfYT6rfvbnj756tbBghyHhHUujhJhjH  
HUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H7n8HHGghyHh  
6YT64V0GhIGfHfQbnj75
```

S/MIME-Format

- Signatur mit „Clear Signing“ (multipart/signed)
 - Anfällig gegen Transformationen auf dem Transportweg (Leerzeichen, ...)
 - Abwärtskompatibel (alte MUAs können Klartext anzeigen aber Signatur nicht prüfen)



S/MIME-Format

□ Signatur mit „Clear Signing“ : Beispiel

```
Content-Type: multipart/signed;  
  protocol="application/pkcs7-signature";  
  micalg=sha1; boundary=boundary42
```

```
--boundary42
```

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

```
This is a clear-signed message.
```

```
--boundary42
```

```
Content-Type: application/pkcs7-signature; name=smime.p7s
```

```
Content-Transfer-Encoding: base64
```

```
Content-Disposition: attachment; filename=smime.p7s
```

```
ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6  
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj  
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4  
7GhIGfHfYT64VQbnj756
```

```
--boundary42--
```

S/MIME-Format

- Verschlüsselung und Signatur
 - envelopData und signedData sind wieder MIME-Bodies
 - V+S bzw. S+V wird durch Schachtelung ermöglicht

- Kompression als eigener MIME-Typ
 - Kompression und Verschlüsselung können daher kombiniert werden

S/MIME-Format

□ Andere PKCS-Typen:

- application/pkcs7-mime; smime-type="degenerated"
für Nachrichten mit ausschließlich CRLs oder Pubkey-Zertifikaten
- application/pkcs10-mime
für die Anforderung eines Pubkey-Zertifikates zur Registrierung

S/MIME vs. OpenPGP

- ❑ OpenPGP-Zertifikate werden von Nutzern untereinander „beglaubigt“ - S/MIME basiert auf CA-Zertifikaten
- ❑ S/MIME entwickelt sich mehr zum Industriestandard, PGP wird eher für private Kommunikation genutzt (Aufwand der Zertifikatverwaltung vs. Vertrauenswürdigkeit)

Zusammenfassung

- ❑ S/MIME baut auf dem MIME-Standard auf
- ❑ Neue MIME-Typen für Verschlüsselung, 2 x Signatur, Kompression und anderes
- ❑ Nicht zu unterschätzender Verwaltungsaufwand für Zertifikate
- ❑ Cryptographic Message Syntax (CMS) nächste Woche

Quellen

- ❑ RFC 2045-2049 - MIME
- ❑ RFC 3850 – S/MIME 3.1 Certificate Handling
- ❑ RFC 3851 – S/MIME 3.1 Msg. Spec.
- ❑ W. Stallings: „Sicherheit im Internet“, Addison-Wesley, ISBN: 3-8273-1697-9