S/MIME protocol (Secure/Multipurpose Internet Mail Extension)

Morena Simatic
Universidade do Porto, Faculdade de Engenharia
Contents

• What is S/MIME?
• Characteristics of S/MIME
• Parts of S/MIME
  ▫ Message specification
  ▫ Certificate Handling
  ▫ PKCS#7- Cryptographic Message Syntax
• Deploying S/MIME in practice
• Example of using S/MIME
What is S/MIME?

- protocol for public key encryption and signing of e-mail encapsulated in MIME format
- protocol for adding cryptographic signature and encryption services to MIME data
- IETF standard
- developed by RSA Data Security
- end-to-end security
- “detached signatures”
Characteristics of S/MIME

- Provides cryptographic security:
  - Authentication
  - Message integrity
  - Non-repudiation (using digital signatures)
  - Privacy and data security (using encryption)
Characteristics of S/MIME

• Specifies the security application following the syntax given in PKCS #7
  ▫ PKCS#7-syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes
Characteristics of S/MIME

- It can be used in:
  - traditional mail user agents (MUAs)
  - automated message transfer agents
Parts of S/MIME - Message specification

- S/MIME message - combination of MIME bodies and PKCS objects
  - Data to be encrypted is a canonical MIME entity

Diagram:
- MIME entity
  - Other data
- Certificates and algorithm identifiers
- PKCS processing facilities
- PKCS object
  - Wrapped in MIME data
Parts of S/MIME - certification handling

• Obtain a key/certificate – use of separate keys for signature and for encryption
• In order to validate the keys of a message sent to it, an S/MIME agent needs to certify that the key is valid
• PKCS #7 message format supports X.509 format of certificates:
  ▫ Subject name
  ▫ Issuer name
Parts of S/MIME - PKCS#7- Cryptographic Message Syntax

• general syntax for data that may have cryptography applied to it:
  ▫ **digital signatures** - content first reduced to a message digest and then is encrypted with the RSA private key of the signer of the content
  ▫ **digital envelopes** – content is first encrypted under a content-encryption key and then the content-encryption key is encrypted with the RSA public keys of the recipients of the content
Deploying S/MIME in practice - problems

- Not all e-mail software handles S/MIME signatures: webmail clients
- Tailored for end-to-end security → encrypts also malware
- Stored encrypted messages can’t be decrypted if certificate/private key is not available
Example of using S/MIME

- Getting a certificate from certifying authority (Comodo) and importing it in the web browser
- Using firefox add-on Gmail S/MIME 0.4.3
Example of using S/MIME

- Sending a encrypted and signed message in Gmail using S/MIME
- Message is signed → attached smime.p7m document
Conclusion

• S/MIME defines how a digital certificate and encryption information can be provided as part of the message body
• S/MIME and digital certificates offer clients a low-cost way to improve their email security
Obrigada pela vossa atenção!