Electronic Mail Security

Lennart Franked

Department of Information and Communication Systems (ICS),
Mid Sweden University, Sundsvall.

20 april 2015

Litterature

The lecture covers chapter 8 “Electronic Mail Security” in [1] and the RFC document “Analysis of Threats Motivating DomainKeys Identified Mail **[rfc4686]**
When you have finished reading this chapter, you should solve problems 8.6 - 8.8 in [1].

Overview

1. PGP
   - Pretty Good Privacy
2. S/MIME
   - Multipurpose Internet Mail Extensions
   - S/MIME
3. DKIM
   - DKIM

- Provides Confidentiality, Authentication and Integrity services.
- Mainly used for e-mail and file storage.
- Combines symmetric and asymmetric encryption

- Provides Confidentiality, Authentication and Integrity services.
- Mainly used for e-mail and file storage.
- Combines symmetric and asymmetric encryption

- Provides Confidentiality, Authentication and Integrity services.
- Mainly used for e-mail and file storage.
- Combines symmetric and asymmetric encryption

- Authentication.
- Confidentiality.
- Compression.
- E-mail compatibility.

- Authentication.
- Confidentiality.
- Compression.
- E-mail compatibility.

- Authentication.
- Confidentiality.
- Compression.
- E-mail compatibility.

- Authentication.
- Confidentiality.
- Compression.
- E-mail compatibility.

- Combines an hash algorithm such as MD5 or SHA with an asymmetric encryption scheme such as RSA, DSS or El Gamal.
- RSA ensures that only the owner of an asymmetric key-pair is able to generate a signature.
- SHA ensures that no one could modify the data sent.
- Signature could either be sent together with the data or detached.

- Combines an hash algorithm such as MD5 or SHA with an asymmetric encryption scheme such as RSA, DSS or El Gamal.
- RSA ensures that only the owner of an asymmetric key-pair is able to generate a signature.
- SHA ensures that no one could modify the data sent.
- Signature could either be sent together with the data or detached.

- Combines an hash algorithm such as MD5 or SHA with an asymmetric encryption scheme such as RSA, DSS or El Gamal.
- RSA ensures that only the owner of an asymmetric key-pair is able to generate a signature.
- SHA ensures that no one could modify the data sent.
- Signature could either be sent together with the data or detached.

- Combines an hash algorithm such as MD5 or SHA with an asymmetric encryption scheme such as RSA, DSS or El Gamal.
- RSA ensures that only the owner of an asymmetric key-pair is able to generate a signature.
- SHA ensures that no one could modify the data sent.
- Signature could either be sent together with the data or detached.

Supports a variety of symmetric encryption algorithms

- IDEA, 3DES, CAST5, AES (128,192,256) et cetera.

Supports most cipher modes

- ECB, CFB, CBC, CTR et cetera.

`gpg -version` – Displays supported algorithms.

Supports a variety of symmetric encryption algorithms

- IDEA, 3DES, CAST5, AES (128,192,256) et cetera.

Supports most cipher modes

- ECB, CFB, CBC, CTR et cetera.

`gpg -version` – Displays supported algorithms.

- Generates a signature first and prepend it to the message.
- Plaintext and signature is then encrypted.

- Generates a signature first and prepend it to the message.
- Plaintext and signature is then encrypted.

- Most e-mail systems only permit ASCII-text.
- PGP/GPG therefore converts 8 bit binary stream to ASCII using Radix-64 conversion.
    - 3 bytes binary data are mapped to 4 byte ascii-data.
    - Increase message size by 33%
    - Converts the message regardless of content (Even if content already is in ASCII).

- Most e-mail systems only permit ASCII-text.
- PGP/GPG therefore converts 8 bit binary stream to ASCII using Radix-64 conversion.
    - 3 bytes binary data are mapped to 4 byte ascii-data.
    - Increase message size by 33%
    - Converts the message regardless of content (Even if content already is in ASCII).

- Most e-mail systems only permit ASCII-text.
- PGP/GPG therefore converts 8 bit binary stream to ASCII using Radix-64 conversion.
  - 3 bytes binary data are mapped to 4 byte ascii-data.
  - Increase message size by 33%
  - Converts the message regardless of content (Even if content already is in ASCII).

- Most e-mail systems only permit ASCII-text.
- PGP/GPG therefore converts 8 bit binary stream to ASCII using Radix-64 conversion.
  - 3 bytes binary data are mapped to 4 byte ascii-data.
  - Increase message size by 33%
  - Converts the message regardless of content (Even if content already is in ASCII).

- Most e-mail systems only permit ASCII-text.
- PGP/GPG therefore converts 8 bit binary stream to ASCII using Radix-64 conversion.
  - 3 bytes binary data are mapped to 4 byte ascii-data.
  - Increase message size by 33%
  - Converts the message regardless of content (Even if content already is in ASCII).

- Compensates for the ASCII to Radix-64 conversion.
- Message is usually compressed after signing.
  - No need to store compressed version of the email.
  - Compression algorithms aren't deterministic.
  - Different results between versions of the compression algorithm.
- Strengthens security.
- ZIP, ZLIB or BZIP2 are the most commonly used compression algorithms.

- Compensates for the ASCII to Radix-64 conversion.
- Message is usually compressed after signing.
  - No need to store compressed version of the email.
  - Compression algorithms aren't deterministic.
  - Different results between versions of the compression algorithm.
- Strengthens security.
- ZIP, ZLIB or BZIP2 are the most commonly used compression algorithms.

- Compensates for the ASCII to Radix-64 conversion.
- Message is usually compressed after signing.
  - No need to store compressed version of the email.
  - Compression algorithms aren't deterministic.
  - Different results between versions of the compression algorithm.
- Strengthens security.
- ZIP, ZLIB or BZIP2 are the most commonly used compression algorithms.

- Compensates for the ASCII to Radix-64 conversion.
- Message is usually compressed after signing.
  - No need to store compressed version of the email.
  - Compression algorithms aren't deterministic.
  - Different results between versions of the compression algorithm.
- Strengthens security.
- ZIP, ZLIB or BZIP2 are the most commonly used compression algorithms.

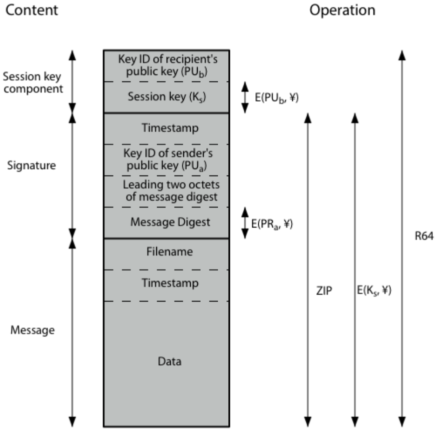
- Compensates for the ASCII to Radix-64 conversion.
- Message is usually compressed after signing.
  - No need to store compressed version of the email.
  - Compression algorithms aren't deterministic.
  - Different results between versions of the compression algorithm.
- Strengthens security.
- ZIP, ZLIB or BZIP2 are the most commonly used compression algorithms.

- Compensates for the ASCII to Radix-64 conversion.
- Message is usually compressed after signing.
  - No need to store compressed version of the email.
  - Compression algorithms aren't deterministic.
  - Different results between versions of the compression algorithm.
- Strengthens security.
- ZIP, ZLIB or BZIP2 are the most commonly used compression algorithms.

- Compensates for the ASCII to Radix-64 conversion.
- Message is usually compressed after signing.
  - No need to store compressed version of the email.
  - Compression algorithms aren't deterministic.
  - Different results between versions of the compression algorithm.
- Strengthens security.
- ZIP, ZLIB or BZIP2 are the most commonly used compression algorithms.

PGP Message

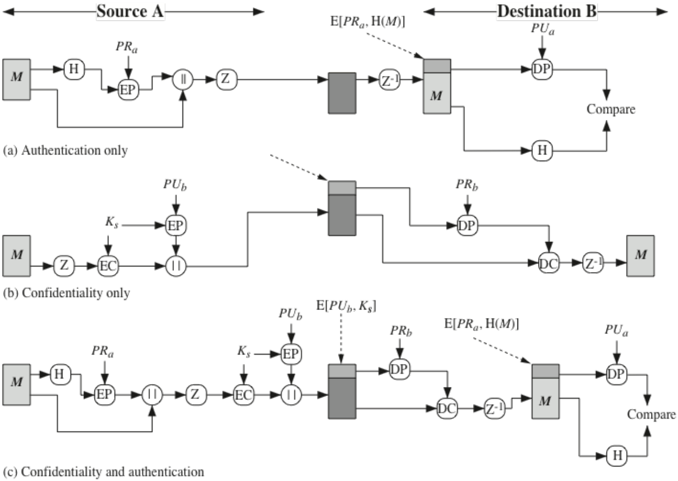
Pretty Good Privacy



Notation:
E(PU_b, ¥) = encryption with user b's public key
E(PR_a, ¥) = encryption with user a's private key
E(K_s, ¥) = encryption with session key
ZIP = Zip compression function
R64 = Radix-64 conversion function

PGP processing

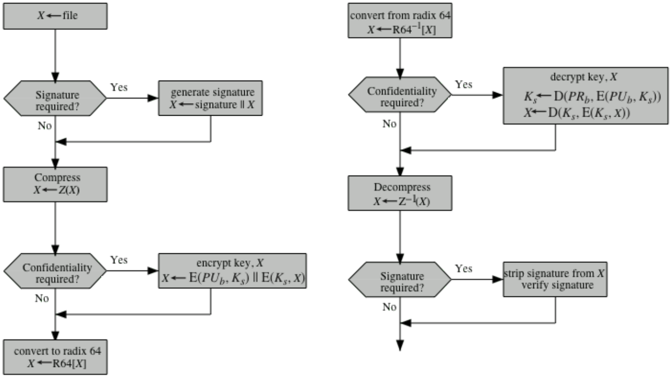
Pretty Good Privacy



Figur 2: [1]

Transmission and reception diagram

Pretty Good Privacy



(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

Figur 3: [1]

Secure Multipurpose Internet Mail Extensions

- E-mail consist of an envelope and a content.
- Envelope contains information needed for the content to be delivered.
- Content contains the message along with header fields.
- Header format `Keyword: Argument`
- Message only meant to contain text.

- E-mail consist of an envelope and a content.
- Envelope contains information needed for the content to be delivered.
- Content contains the message along with header fields.
- Header format *Keyword*: `Argument`
- Message only meant to contain text.

- E-mail consist of an envelope and a content.
- Envelope contains information needed for the content to be delivered.
- Content contains the message along with header fields.
- Header format *Keyword*: `Argument`
- Message only meant to contain text.

- E-mail consist of an envelope and a content.
- Envelope contains information needed for the content to be delivered.
- Content contains the message along with header fields.
- Header format *Keyword*: `Argument`
- Message only meant to contain text.

- E-mail consist of an envelope and a content.
- Envelope contains information needed for the content to be delivered.
- Content contains the message along with header fields.
- Header format *Keyword*: `Argument`
- Message only meant to contain text.

Purpose of MIME

Multipurpose Internet Mail Extensions

- SMTP were only intended to transfer 7-bit ASCII.
- Some SMTP implementations do not always follow the SMTP-standard in regards to for example text formatting.

- SMTP were only intended to transfer 7-bit ASCII.
- Some SMTP implementations do not always follow the SMTP-standard in regards to for example text formatting.

- MIME was developed to overcome some of these limitations.
- Adds five new message headers fields that contains information about the message contents.
  - MIME-Version
  - Content-Type – What type of data is sent in the content.
  - Content-Transfer Encoding – What kind of transfer encoding that have been used to represent the data.
  - Content-ID – Identify every MIME-message
  - Content-descriptor

- MIME was developed to overcome some of these limitations.
- Adds five new message headers fields that contains information about the message contents.
  - MIME-Version
  - Content-Type – What type of data is sent in the content.
  - Content-Transfer Encoding – What kind of transfer encoding that have been used to represent the data.
  - Content-ID – Identify every MIME-message
  - Content-descriptor

- MIME was developed to overcome some of these limitations.
- Adds five new message headers fields that contains information about the message contents.
  - MIME-Version
  - Content-Type – What type of data is sent in the content.
  - Content-Transfer Encoding – What kind of transfer encoding that have been used to represent the data.
  - Content-ID – Identify every MIME-message
  - Content-descriptor

- MIME was developed to overcome some of these limitations.
- Adds five new message headers fields that contains information about the message contents.
  - MIME-Version
  - Content-Type – What type of data is sent in the content.
  - Content-Transfer Encoding – What kind of transfer encoding that have been used to represent the data.
  - Content-ID – Identify every MIME-message
  - Content-descriptor

- MIME was developed to overcome some of these limitations.
- Adds five new message headers fields that contains information about the message contents.
  - MIME-Version
  - Content-Type – What type of data is sent in the content.
  - Content-Transfer Encoding – What kind of transfer encoding that have been used to represent the data.
  - Content-ID – Identify every MIME-message
  - Content-descriptor

- MIME was developed to overcome some of these limitations.
- Adds five new message headers fields that contains information about the message contents.
  - MIME-Version
  - Content-Type – What type of data is sent in the content.
  - Content-Transfer Encoding – What kind of transfer encoding that have been used to represent the data.
  - Content-ID – Identify every MIME-message
  - Content-descriptor

- MIME was developed to overcome some of these limitations.
- Adds five new message headers fields that contains information about the message contents.
  - MIME-Version
  - Content-Type – What type of data is sent in the content.
  - Content-Transfer Encoding – What kind of transfer encoding that have been used to represent the data.
  - Content-ID – Identify every MIME-message
  - Content-descriptor

- Enveloped data – Encrypts any content type together with session key.
- Signed Data – Encrypt message digest over the content, both content and signature are encoded in base64.
- Clear-signed data – Encrypts message digest over the content, only signature is encoded in base64.
- Signed and enveloped data – Combines Enveloped data and Signed Data.

- Enveloped data – Encrypts any content type together with session key.
- Signed Data – Encrypt message digest over the content, both content and signature are encoded in base64.
- Clear-signed data – Encrypts message digest over the content, only signature is encoded in base64.
- Signed and enveloped data – Combines Enveloped data and Signed Data.

- Enveloped data – Encrypts any content type together with session key.
- Signed Data – Encrypt message digest over the content, both content and signature are encoded in base64.
- Clear-signed data – Encrypts message digest over the content, only signature is encoded in base64.
- Signed and enveloped data – Combines Enveloped data and Signed Data.

- Enveloped data – Encrypts any content type together with session key.
- Signed Data – Encrypt message digest over the content, both content and signature are encoded in base64.
- Clear-signed data – Encrypts message digest over the content, only signature is encoded in base64.
- Signed and enveloped data – Combines Enveloped data and Signed Data.

S/MIME functionality II

S/MIME

- S/MIME Similar to PGP
- Supports DSS, RSA and El Gamal asymmetric encryption algorithms.
- Supports MD5 and SHA hash algorithms for integrity and signing.
- 3DES is used as the symmetric encryption algorithm.
- Use X.509 public key certificates.

S/MIME functionality II

- S/MIME Similar to PGP
- Supports DSS, RSA and El Gamal asymmetric encryption algorithms.
- Supports MD5 and SHA hash algorithms for integrity and signing.
- 3DES is used as the symmetric encryption algorithm.
- Use X.509 public key certificates.

S/MIME functionality II

- S/MIME Similar to PGP
- Supports DSS, RSA and El Gamal asymmetric encryption algorithms.
- Supports MD5 and SHA hash algorithms for integrity and signing.
- 3DES is used as the symmetric encryption algorithm.
- Use X.509 public key certificates.

S/MIME functionality II

- S/MIME Similar to PGP
- Supports DSS, RSA and El Gamal asymmetric encryption algorithms.
- Supports MD5 and SHA hash algorithms for integrity and signing.
- 3DES is used as the symmetric encryption algorithm.
- Use X.509 public key certificates.

- S/MIME Similar to PGP
- Supports DSS, RSA and El Gamal asymmetric encryption algorithms.
- Supports MD5 and SHA hash algorithms for integrity and signing.
- 3DES is used as the symmetric encryption algorithm.
- Use X.509 public key certificates.

DKIM

DomainKeys Identified Mail

DomainKeys Identified Mail

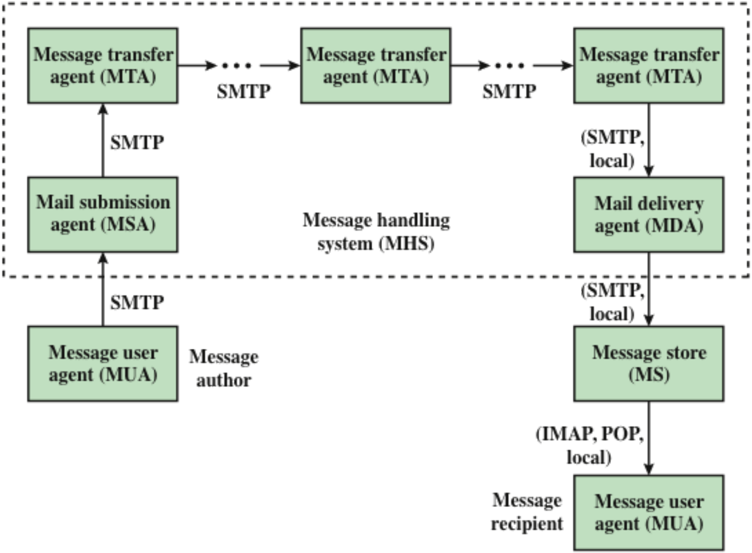
DKIM

- Developed by a range of e-mail provides.
- A system for verifying the origin of an e-mail.

- Developed by a range of e-mail provides.
- A system for verifying the origin of an e-mail.

Email Transmission

DKIM


Message transfer agent (MTA)
SMTP
Message transfer agent (MTA)
SMTP
Message transfer agent (MTA)
SMTP
(SMTP, local)
Mail submission agent (MSA)
Message handling system (MHS)
Mail delivery agent (MDA)
SMTP
(SMTP, local)
Message user agent (MUA)
Message author
Message store (MS)
(IMAP, POP, local)
Message recipient
Message user agent (MUA)

- Attackers that falsify sender address.
- Spammers that send on behalf of third parties. Often hijacks MTAs and computers as sending zombies.
- Attackers that have a financial motive. Attacks against the infrastructure, such as DNS Cache Poisoning or IP routing attacks.

- Attackers that falsify sender address.
- Spammers that send on behalf of third parties. Often hijacks MTAs and computers as sending zombies.
- Attackers that have a financial motive. Attacks against the infrastructure, such as DNS Cache Poisoning or IP routing attacks.

- Attackers that falsify sender address.
- Spammers that send on behalf of third parties. Often hijacks MTAs and computers as sending zombies.
- Attackers that have a financial motive. Attacks against the infrastructure, such as DNS Cache Poisoning or IP routing attacks.

Attacker resources

DKIM

- Inject messages to MTAs.
- Construct arbitrary headers.
- Sign messages on behalf of certain domains.
- Denial-of-Service using e-mail messages.
- Replay attacks.
- Modify e-mail envelope information.

- Inject messages to MTAs.
- Construct arbitrary headers.
- Sign messages on behalf of certain domains.
- Denial-of-Service using e-mail messages.
- Replay attacks.
- Modify e-mail envelope information.

- Inject messages to MTAs.
- Construct arbitrary headers.
- Sign messages on behalf of certain domains.
- Denial-of-Service using e-mail messages.
- Replay attacks.
- Modify e-mail envelope information.

Attacker resources

DKIM

- Inject messages to MTAs.
- Construct arbitrary headers.
- Sign messages on behalf of certain domains.
- Denial-of-Service using e-mail messages.
- Replay attacks.
- Modify e-mail envelope information.

- Inject messages to MTAs.
- Construct arbitrary headers.
- Sign messages on behalf of certain domains.
- Denial-of-Service using e-mail messages.
- Replay attacks.
- Modify e-mail envelope information.

Attacker resources

DKIM

- Inject messages to MTAs.
- Construct arbitrary headers.
- Sign messages on behalf of certain domains.
- Denial-of-Service using e-mail messages.
- Replay attacks.
- Modify e-mail envelope information.

Attacker resources II

DKIM

- Send emails through a compromised computer.
- Manipulate IP-routing. (Fake/hide origin).
- DNS cache poisoning.
- Gain access to a significant amount of computing resources.
- Eavesdrop on traffic.

Attacker resources II

DKIM

- Send emails through a compromised computer.
- Manipulate IP-routing. (Fake/hide origin).
- DNS cache poisoning.
- Gain access to a significant amount of computing resources.
- Eavesdrop on traffic.

- Send emails through a compromised computer.
- Manipulate IP-routing. (Fake/hide origin).
- DNS cache poisoning.
- Gain access to a significant amount of computing resources.
- Eavesdrop on traffic.

Attacker resources II

DKIM

- Send emails through a compromised computer.
- Manipulate IP-routing. (Fake/hide origin).
- DNS cache poisoning.
- Gain access to a significant amount of computing resources.
- Eavesdrop on traffic.

Attacker resources II

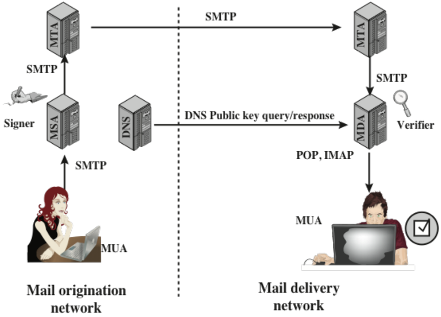
DKIM

- Send emails through a compromised computer.
- Manipulate IP-routing. (Fake/hide origin).
- DNS cache poisoning.
- Gain access to a significant amount of computing resources.
- Eavesdrop on traffic.

DKIM protection

DomainKeys Identified Mail ensures a certain protection against attackers located on a network outside of the recipient or senders network.

DKIM deployment
DKIM



DNS = domain name system
MDA = mail delivery agent
MSA = mail submission agent
MTA = message transfer agent
MUA = message user agent

Figur 5: [1]

- DKIM provides transparent e-mail authentication.
- Compared to PGP or S/MIME users do not need to have their own key-pair.
- PGP and S/MIME only signs the message content, DKIM signs content and part of header.
- DKIM signs all e-mails originating from a certain domain.

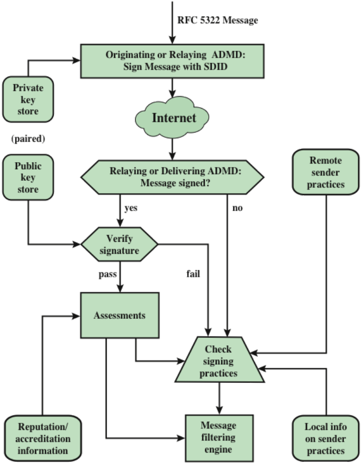
- DKIM provides transparent e-mail authentication.
- Compared to PGP or S/MIME users do not need to have their own key-pair.
- PGP and S/MIME only signs the message content, DKIM signs content and part of header.
- DKIM signs all e-mails originating from a certain domain.

- DKIM provides transparent e-mail authentication.
- Compared to PGP or S/MIME users do not need to have their own key-pair.
- PGP and S/MIME only signs the message content, DKIM signs content and part of header.
- DKIM signs all e-mails originating from a certain domain.

- DKIM provides transparent e-mail authentication.
- Compared to PGP or S/MIME users do not need to have their own key-pair.
- PGP and S/MIME only signs the message content, DKIM signs content and part of header.
- DKIM signs all e-mails originating from a certain domain.

DKIM functional flow

DKIM



Figur 6: [1]

Referenser

William Stallings. *Network security essentials : applications and standards*. 5. utg. International Edition. Pearson Education, 2013. ISBN: 978-0-273-79336-6.