Cryptography and Network Security

EMAIL SECURITY

Session Meta Data

Author	**Dr T Sree Sharmila**
Reviewer	
Version Number	1.0
Release Date	10 August 2018

Revision History

Revision Date	Details	Version no.
		1.0

Agenda

- Email Security
  - Enhancements
- Pretty Good Privacy (PGP)
  - Operation
  - Session keys
  - Key rings
  - Key management
- S/MIME
  - Function
  - Cryptography algorithm
  - Certificate process
  - Certificate authorities
- Summary
- Test your understanding
- References

Email Security

- email is one of the most widely used and regarded network services
- currently message contents are not secure
  - may be inspected either in transit
  - or by suitably privileged users on destination system

Agenda

- Email Security
  - Enhancements
- Pretty Good Privacy (PGP)
  - Operation
  - Session keys
  - Key rings
  - Key management
- S/MIME
  - Function
  - Cryptography algorithm
  - Certificate process
  - Certificate authorities
- Summary
- Test your understanding
- References

Email Security Enhancements

- confidentiality
  - protection from disclosure
- authentication
  - of sender of message
- message integrity
  - protection from modification
- non-repudiation of origin
  - protection from denial by sender

Agenda

- Email Security
  - Enhancements
- Pretty Good Privacy (PGP)
  - Operation
  - Session keys
  - Key rings
  - Key management
- S/MIME
  - Function
  - Cryptography algorithm
  - Certificate process
  - Certificate authorities
- Summary
- Test your understanding
- References

Pretty Good Privacy (PGP)

- widely used de facto secure email
- developed by Phil Zimmermann
- selected best available crypto algs to use
- integrated into a single program
- available on Unix, PC, Macintosh and Amiga systems
- originally free, now have commercial versions available also

Agenda

- Email Security
  - Enhancements
- Pretty Good Privacy (PGP)
  - Operation
  - Session keys
  - Key rings
  - Key management
- S/MIME
  - Function
  - Cryptography algorithm
  - Certificate process
  - Certificate authorities
- Summary
- Test your understanding
- References

PGP Operation – Authentication

1. sender creates a message
2. SHA-1 used to generate 160-bit hash code of message
3. hash code is encrypted with RSA using the sender's private key, and result is attached to message
4. receiver uses RSA or DSS with sender's public key to decrypt and recover hash code
5. receiver generates new hash code for message and compares with decrypted hash code, if match, message is accepted as authentic

PGP Operation – Confidentiality

1. sender generates message and random 128-bit number to be used as session key for this message only
2. message is encrypted, using CAST-128 / IDEA/3DES with session key
3. session key is encrypted using RSA with recipient's public key, then attached to message
4. receiver uses RSA with its private key to decrypt and recover session key
5. session key is used to decrypt message

PGP Operation – Confidentiality & Authentication

- uses both services on same message
  - create signature & attach to message
  - encrypt both message & signature
  - attach RSA encrypted session key

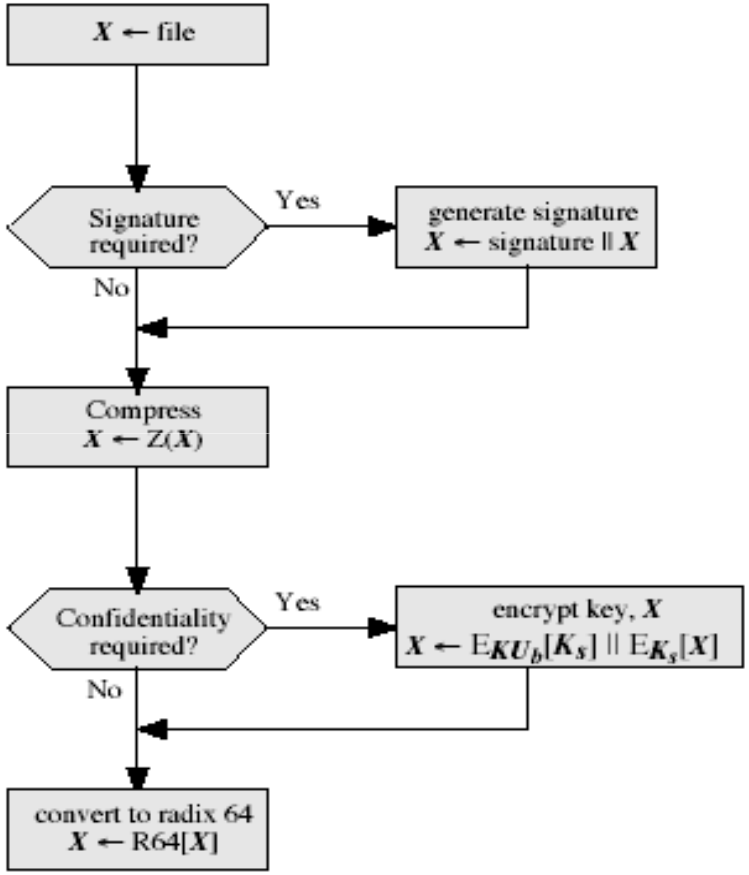
PGP Operation – Compression

- by default PGP compresses message after signing but before encrypting
  - so can store uncompressed message & signature for later verification
  - & because compression is non deterministic
- uses ZIP compression algorithm

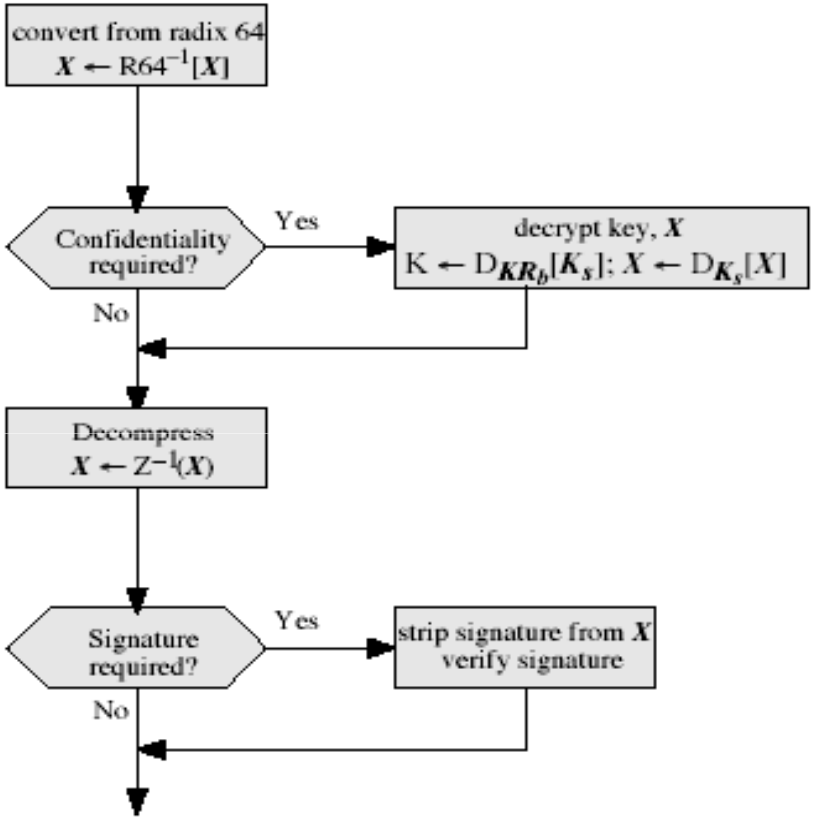
PGP Operation – Email Compatibility

- when using PGP will have binary data to send (encrypted message etc)
- however email was designed only for text
- hence PGP must encode raw binary data into printable ASCII characters
- uses radix-64 algorithm
  - maps 3 bytes to 4 printable chars
  - also appends a CRC
- PGP also segments messages if too big

PGP Operation – Summary



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

Agenda

- Email Security
  - Enhancements
- Pretty Good Privacy (PGP)
  - Operation
  - Session keys
  - Key rings
  - Key management
- S/MIME
  - Function
  - Cryptography algorithm
  - Certificate process
  - Certificate authorities
- Summary
- Test your understanding
- References

PGP Session Keys

- need a session key for each message
  - of varying sizes: 56-bit DES, 128-bit CAST or IDEA, 168-bit Triple-DES
- generated using ANSI X12.17 mode
- uses random inputs taken from previous uses and from keystroke timing of user

PGP Public & Private Keys

- since many public/private keys may be in use, need to identify which is actually used to encrypt session key in a message
  - could send full public-key with every message
  - but this is inefficient
- rather use a key identifier based on key
  - is least significant 64-bits of the key
  - will very likely be unique
- also use key ID in signatures

Agenda

- Email Security
  - Enhancements
- Pretty Good Privacy (PGP)
  - Operation
  - Session keys
  - Key rings
  - Key management
- S/MIME
  - Function
  - Cryptography algorithm
  - Certificate process
  - Certificate authorities
- Summary
- Test your understanding
- References

PGP Key Rings

- each PGP user has a pair of keyrings:
  - public-key ring contains all the public-keys of other PGP users known to this user, indexed by key ID
  - private-key ring contains the public/private key pair(s) for this user, indexed by key ID & encrypted keyed from a hashed passphrase

Agenda

- Email Security
  - Enhancements
- Pretty Good Privacy (PGP)
  - Operation
  - Session keys
  - Key rings
  - Key management
- S/MIME
  - Function
  - Cryptography algorithm
  - Certificate process
  - Certificate authorities
- Summary
- Test your understanding
- References

PGP Key Management

- rather than relying on certificate authorities
- in PGP every user is own CA
  - can sign keys for users they know directly
- forms a “web of trust”
  - trust keys have signed
  - can trust keys others have signed if have a chain of signatures to them
- key ring includes trust indicators
- users can also revoke their keys

Agenda

- Email Security
  - Enhancements
- Pretty Good Privacy (PGP)
  - Operation
  - Session keys
  - Key rings
  - Key management
- S/MIME
  - Function
  - Cryptography algorithm
  - Certificate process
  - Certificate authorities
- Summary
- Test your understanding
- References

S/MIME (Secure/Multipurpose Internet Mail Extensions)

- security enhancement to MIME email
  - original Internet RFC822 email was text only
  - MIME provided support for varying content types and multi-part messages
  - with encoding of binary data to textual form
  - S/MIME added security enhancements
- have S/MIME support in various modern mail agents: MS Outlook, Netscape etc

Agenda

- Email Security
  - Enhancements
- Pretty Good Privacy (PGP)
  - Operation
  - Session keys
  - Key rings
  - Key management
- S/MIME
  - Function
  - Cryptography algorithm
  - Certificate process
  - Certificate authorities
- Summary
- Test your understanding
- References

S/MIME Functions

- enveloped data
  - encrypted content and associated keys
- signed data
  - encoded message + signed digest
- clear-signed data
  - cleartext message + encoded signed digest
- signed & enveloped data
  - nesting of signed & encrypted entities

Agenda

- Email Security
  - Enhancements
- Pretty Good Privacy (PGP)
  - Operation
  - Session keys
  - Key rings
  - Key management
- S/MIME
  - Function
  - Cryptography algorithm
  - Certificate process
  - Certificate authorities
- Summary
- Test your understanding
- References

S/MIME Cryptographic Algorithms

- hash functions: SHA-1 & MD5
- digital signatures: DSS & RSA
- session key encryption: ElGamal & RSA
- message encryption: Triple-DES, RC2/40 and others
- have a procedure to decide which algorithms to use

Agenda

- Email Security
  - Enhancements
- Pretty Good Privacy (PGP)
  - Operation
  - Session keys
  - Key rings
  - Key management
- S/MIME
  - Function
  - Cryptography algorithm
  - Certificate process
  - Certificate authorities
- Summary
- Test your understanding
- References

S/MIME Certificate Processing

- S/MIME uses X.509 v3 certificates
- managed using a hybrid of a strict X.509 CA hierarchy & PGP's web of trust
- each client has a list of trusted CA's certs
- and own public/private key pairs & certs
- certificates must be signed by trusted CA's

Agenda

- Email Security
  - Enhancements
- Pretty Good Privacy (PGP)
  - Operation
  - Session keys
  - Key rings
  - Key management
- S/MIME
  - Function
  - Cryptography algorithm
  - Certificate process
  - Certificate authorities
- Summary
- Test your understanding
- References

Certificate Authorities

- have several well-known CA's
- Verisign one of most widely used
- Verisign issues several types of Digital IDs
- with increasing levels of checks & hence trust

Class	Identity Checks	Usage
1	name/email check	web browsing/email
2+	enroll/addr check	email, subs, s/w validate
3+	ID documents	e-banking/service access

Agenda

- Email Security
  - Enhancements
- Pretty Good Privacy (PGP)
  - Operation
  - Session keys
  - Key rings
  - Key management
- S/MIME
  - Function
  - Cryptography algorithm
  - Certificate process
  - Certificate authorities
- Summary
- Test your understanding
- References

Summary

- have considered:
  - secure email
  - PGP
  - S/MIME

Test your understanding

1) Explain PGP in detail.
2) Explain S/MIME in detail.

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.