Pretty Good Privacy

Mahalingam Ramkumar
Mississippi State University, MS

November 15, 2004
1 Introduction
  - PGP Services

2 PGP Operation
  - PGP Components
  - PGP Message Generation and Reception

3 PGP Key Management
  - Structure of Key Rings
Services Provided by PGP

1. Digital Signature (DSS/SHA or RSA/SHA)
2. Message Encryption (CAST-128, IDEA, 3-DES in conjunction with RSA)
3. Compression (Lempel-Ziv)
4. E-mail compatibility (Radix-64 conversion)
5. Segmentation (to overcome maximum message length of 50,000 bytes for SMTP)
PGP Modes of Operation

1. Authentication (DSS/SHA or RSA/SHA)
2. Confidentiality (CAST-128, IDEA, 3-DES in conjunction with RSA)
3. Authentication and Confidentiality
PGP Modes

(a) Authentication only

(b) Confidentiality only

(c) Confidentiality and authentication
Transmission and Reception of PGP Messages

(a) Generic Transmission Diagram (from A)

1. $X \not\in \text{file}$
2. Signature required? Yes -> generate signature $X \not\in \text{signature} \parallel X$
3. No -> Compress $X \not\in Z(X)$
4. Confidentiality required? Yes -> encrypt key, $X \not\in E_{KUb}[K_s] \parallel E_{Kf}[X]$
5. No -> convert to radix 64 $X \not\in R_{64}[X]$

(b) Generic Reception Diagram (to B)

1. $X \not\in \text{file}$
2. Convert from radix 64 $X \not\in R_{64}^{-1}[X]$
3. Confidentiality required? Yes -> decrypt key, $X \not\in D_{KRb}[E_{KUb}[K_s]]$
4. No -> Decompress $X \not\in Z^{-1}(X)$
5. Signature required? Yes -> strip signature from $X$
6. No -> verify signature
Four types of keys - passphrase, one-time session keys, public keys, private keys

Two key rings - private and public

Private key ring is encrypted with passphrase

Every user has a public-private key pair

Can have multiple pairs.
PGP Message Components

1. Session key component
2. Signature
3. Message
Format of PGP Message

Content
- Session key component
- Signature
- Message

Operation
- E_{KU_b}
- E_{KR_a}
- ZIP
- R64
- E_{Ks}

Key ID of recipient's public key (KU_b)
Session key (K_s)
Timestamp
Key ID of sender's public key (KR_a)
Leading two octets of message digest
Message Digest
Filename
Timestamp
Data
PGP Message Generation

Figure 15.5   PGP Message Generation (from User A to User B; no compression or radix 64 conversion)
PGP Message Reception

1. Passphrase
2. Select private key
3. Decrypt private key
4. Select public key
5. Decrypt message
6. Compare digests

Public key ring
Private key ring
Encrypted session key
Message
Sender's Key ID
Encrypted digest
Recipient's Key ID

Private Key Ring

1. Timestamp
2. Key ID
3. Public key
4. Encrypted Private key (encrypted with passphrase)
5. User ID
Public Key Ring

1. Timestamp, Key ID, Public key, User ID,
2. Owner Trust (OT)
3. Key legitimacy (KL)
4. Signature(s)
5. Signature Trust(s) (ST)
Numerical Trust Assignment - for OT and ST

1. Undefined
2. Unknown
3. Usually not trusted
4. Usually trusted
5. Always trusted
6. Ultimate trust
Numerical Trust Assignment - KL

1. Undefined or Unknown
2. Not trusted
3. Marginally trusted
4. Complete trust
Relationship between KL, ST and OT

1. Consider public key of A signed by B and C
2. $r_A$, $r_B$ and $r_C$ - rows in the public key ring corresponding to A, B and C.
3. Legitimacy entry for A depends on the “signature trusts” of B and C in row $r_A$.
4. ST of B in $r_A$ - copy of the OT in row $r_B$
5. ST of C in $r_A$ - copy of the OT in row $r_C$
6. “Owner Trust” manually assigned by the PGP user.
7. KL is a function of “weighted” STs
8. If any ST is “ultimate” - KL is assigned “complete trust”
9. $X$ “usually trusted” signatures or $Y$ for “always trusted” signatures for A (or any combination) would result in “complete trust” of A’s public key
Trust Propagation

You

A B C D E F
G H I J K L M N O
P Q R
S

= X is signed by Y

= key's owner is trusted by you to sign keys

= key's owner is partly trusted by you to sign keys

= key is deemed legitimate by you

= unknown signatory

Figure 15.7   PGP Trust Model Example

Ramkumar PGP