Foundations of Computer Security

Lecture 70: PGP Key Management II

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Key Management

In PGP, session keys and passphrase-based keys are generated on the fly, used once and discarded.

Public and private keys are persistent and need to be preserved and managed. Recall that a user can have multiple public/private key pairs.

Managing Key Pairs

Given that a user may have multiple public/private key pairs, how do we know which public key was used to encrypt a message.

- Send the public key along with the message. *Inefficient, since the key might be thousands of bits.*
- Associate a unique ID with each key pair and send that with the message. *Would require that all senders know that mapping of keys to ID's for all recipients.*
- Generate an ID *likely* to be unique for a given user. *This is PGP's solution. Use the least significant 64-bits of the key as the ID.*

This is used by the receiver to verify that he has such a key on his "key ring." The associated private key is used for the decryption.

Key Rings: Private Key Ring

Each user maintains two key ring data structures: a **private-key ring** for his own public/private key pairs, and a **public-key ring** for the public keys of correspondents.

The private key ring is a table of rows containing:

Timestamp: when the key pair was generated.

Key ID: 64 least significant digits of the public key.

Public key: the public portion of the key.

Private key: the private portion, encrypted using a passphrase.

User ID: usually the user's email address. May be different for different key pairs.

Public Key Ring

Public keys of other users are stored on a user's public-key ring. This is a table of rows containing (among other fields):

Timestamp: when the entry was generated.

Key ID: 64 least significant digits of this entry.

Public key: the public key for the entry.

User ID: Identifier for the owner of this key. Multiple IDs may be associated with a single public key.

The public key can be indexed by either User ID or Key ID.

Retrieving a Private Key

Whenever PGP must use a private key, it must decrypt it. For example, suppose R receives a message encrypted with K_R.

1. PGP retrieves receiver's encrypted private key from the private-key ring, using the Key ID field in the session key component of the message as an index.
2. PGP prompts the user for the passphrase to recover the unencrypted private key.
3. PGP recovers the session key and decrypts the message.

Validity of Public Key

Associated with each public key in the user's public key ring is a **key legitimacy field** that indicates the extent to which PGP trusts that this is a valid public key for this user.

Legitimacy is determined from certificates and chains of certificates, the user's assessment of the trust to be assigned to the key, and various heuristics for computing trust.

Revoking Public Keys

A user may wish to revoke a public key because:

- compromise is suspected, or
- to limit the period of use of the key.

The owner issues a signed key revocation certificate. Recipients are expected to update their public-key rings.

Lessons

- Each PGP user must manage his own private keys and the public keys of others.
- These are stored on separate keys rings.
- Private keys are protected by encryption; public keys are stored with certificates attesting to their trustworthiness.
- Keys can be revoked.

Next lecture: Availability