Foundations of Computer Security

Lecture 67: PGP Services

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

PGP

Zimmermann developed PGP (Pretty Good Privacy) in the late 1980's and early 1990's. Some characteristics include:

1. Uses the best available cryptographic algorithms as building blocks.
2. Integrates these into a general-purpose algorithm that is processor-independent and easy to use.
3. Package and documentation, including source code, are freely available on-line.
4. PGP is now provided by Viacrypt in a compatible, low-cost commercial version.

PGP Services

PGP supplies five basic services:

1. Authentication
2. Confidentiality
3. Compression
4. Email compatibility
5. Segmentation

PGP Authentication

This is a digital signature function.

1. Sender creates a message M.
2. Sender generates a hash of M.
3. Sender signs the hash using his private key and prepends the result to the message.
4. Receiver uses the sender's public key to verify the signature and recover the hash code.
5. Receiver generates a new hash code for M and compares it with the decrypted hash code.

Abstractly:

$$S \longrightarrow R : \{h(M)\}_{K_S^{-1}}, M$$

PGP Confidentiality

PGP provides encryption for messages sent or stored as files.

1. Sender generates a message M and a random session key K.
2. M is encrypted using key K.
3. K is encrypted using the recipient's public key, and prepended to the message.
4. Receiver uses his private key to recover the session key.
5. The session key is used to decrypt the message.

Abstractly:

$$S \rightarrow R : \{K\}_{K_r}, \{M\}_K$$

Confidentiality and Authentication

Both authentication and confidentiality may be combined for a given message.

1. Apply the authentication step to the original message.
2. Apply the confidentiality step to the resulting message.

Why is it preferable to generate a signature for the plaintext message, rather than for the encrypted message?

Lessons

- PGP offers five basic services.
- Two of those are authentication and confidentiality; these can be combined.

Next lecture: PGP Services II