Foundations of Computer Security

Lecture 68: PGP Services II

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

PGP Services

Recall that PGP supplies five basic services:

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

Actually, only authentication and confidentiality are really "services." The others are engineering features designed to make PGP efficient and robust.

Compression

As a default, PGP compresses the message, using the ZIP compression algorithm, after applying the signature and before encryption.

It is done in this order because:

- It is preferable to sign an uncompressed message so that the signature does not depend on the compression algorithm.
- Versions of the compression algorithm behave slightly differently, though all version are interoperable.
- Encryption after compression strengthens the encryption, since compression reduces redundancy in the message.

Email Compatibility

PGP always involves encryption. Encrypted text contains arbitrary 8-bit octets. However, many email systems would choke on certain bit strings they'd interpret as control commands.

PGP uses radix-64 conversion to map groups of three octets into four ASCII characters. Also appends a CRC for data error checking. By default, even ASCII is converted.

Use of radix-64 expands the message by 33%. This is usually more than offset by the compression.

Segmentation and Reassembly

Email systems often restrict message length. Longer messages must be broken into segments, which are mailed separately.

PGP automatically segments messages that are too large. This is done after all of the other steps, including radix-64 conversion. Thus, signature and session key appear only once.

At the receiving end, PGP strips off mail headers and reassembles the message from its component pieces.

Lessons

- PGP provides the "services" of compression, email compatibility, and segmentation to make the system more robust and efficient.

Next lecture: PGP Key Management