Foundations of Computer Security

Lecture 69: PGP Key Management

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

Key Management

PGP makes use of four types of keys: one-time session symmetric keys, public keys, private keys, passphrase-based symmetric keys.

Session keys: used once and generated for each new message

Public keys: used in asymmetric encryption

Private keys: also used in asymmetric encryption

Passphrase-based keys: used to protect private keys

A single user can have multiple public/private key pairs.

Session Key Generation

Each session key is associated with a single message and used only once. Key size depends on the chosen encryption algorithm E; e.g. CAST-128: 128 bits, 3DES: 168-bits, etc.

The encryption algorithm E is used to generate a new n-bit key from a previous session key and two $n/2$-bit blocks generated based on user keystrokes, including keystroke timing. The two blocks are encrypted using E and the previous key, and combined to form the new key.

Public/Private Key Generation

For new RSA keys, an odd number n of sufficient size (usually > 200 bits) is generated and tested for primality. If it is not prime, then repeat with another randomly generated number, until a prime is found.

Primes appear in the neighborhood of n about every $ln(n) = lg_e(n)$ numbers. Since we can exclude even numbers, to find a prime of around 200 bits, it takes about $ln(2^{200})/2 = 70$ tries.

This is an expensive operation, but performed relatively infrequently.

Encrypting the Private Key

The private key is stored encrypted with a user-supplied passphrase:

1. The user selects a passphrase for encrypting private keys.
2. When a new public/private key pair is generated, the system asks for the passphrase. Using SHA-1, a 160-bit hash code is generated from the passphrase, which is discarded.
3. The private key is encrypted using CAST-128 with 128 bits of the hash code as key. The key is then discarded.

Whenever the user wants to access the private key, he must supply the passphrase.

Lessons

- PGP uses four kinds of keys: session keys, public and private keys, and passphrase generated keys.
- Public / private key pairs are the most expensive to generate.
- Since the security of the system depends on protecting private keys, these are encrypted using a passphrase system.

Next lecture: PGP Key Management II