Beginning System Administration DeCal

Week 11

May 4, 2009

Parts of this lecture adapted from Phil Dibowitz's presentation *PGP: What, Why, When, Which, How, and More...*, UUASC 02/02/2006.

Cryptography and Encryption

Terms, Concepts, Methods

Cryptography is hard.

cryptography : the procedures, processes, methods, etc., of making and using secret writing, as codes or ciphers. [1]

encryption : To alter (a file, for example) using a secret code so as to be unintelligible to unauthorized parties. [2]

---

[1] http://dictionary.reference.com/browse/cryptography

[2] http://dictionary.reference.com/browse/encryption

Cryptography
Two General Forms

symmetric-key : shared secret key, block and stream ciphers, cryptographic hash functions

public-key : private and public keys, digital signatures

PGP
Pretty Good Privacy

- Developed in 1991. GnuPG (GPG), the open source equivalent, developed in 1999.
- Decentralized
- Encrypt data/email to intended recipients (or yourself)
  - `gpg --encrypt secrets.txt`
  - `gpg --decrypt secrets.txt.gpg`
  - Mail client support (e.g., Enigmail and Thunderbird)
- Digital verification

- Available for Windows, GNU/Linux, Mac OS X
- Key generation
  - `gpg --gen-key`
  - Two keys: one for encryption, one for signing
  - Size, expiration, name, **passphrase**
- Usage
  - Command-line utilities
  - Mail client support

- Key fingerprint (hash)
- *Public* Key Distribution
  - Key servers
  - Other methods
- Key signing: level of trust, verification of identity

Web of Trust

- Signatures and verification of identity
  - Why? Vouching for identity
  - When? Key signing parties, individual meet ups
  - How? Government issued identification, fingerprint, signature
  - Drawbacks?
- Trust
  - Various trust options
  - Calculated trust

Summary

- Email/plaintext communications (e.g., IM) can be secured with various forms of public-key cryptography.
- Cryptography is pretty hard.
- Simple overview.
- Unfortunately, not as widely used as it could be. (Why?)

More Information

- GPG: `http://www.gnupg.org/gph/en/manual.html`
- RFC 3156: MIME Security with OpenPGP
- RFC 2015: MIME Security with Pretty Good Privacy (PGP)
- RFC 2046: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types