E-Mail and File Security With GnuPG

Matt Brodeur
mbrodeur@nexttime.com

GnuPG

Introduction – What is GnuPG?

- Pretty Good Privacy (PGP)
  - Created by Philip Zimmerman in 1991
  - Now sold by PGP Corporation

- GNU Privacy Guard
  - "GnuPG is a complete and free replacement for PGP."
    (FSF)
  - GnuPG implements the OpenPGP (RFC2440) standard

Introduction – What is OpenPGP?

- OpenPGP is part of a protocol that provides cryptographic security for electronic communication

- OpenPGP provides the four essential components of secure communication
  - Authentication
  - Integrity
  - Nonrepudiation
  - Confidentiality

Why use PGP?

- OpenPGP can protect
  - Financial information
  - Business plans
  - Sensitive data
  - Software distribution
  - Public announcements

How? - Install Software

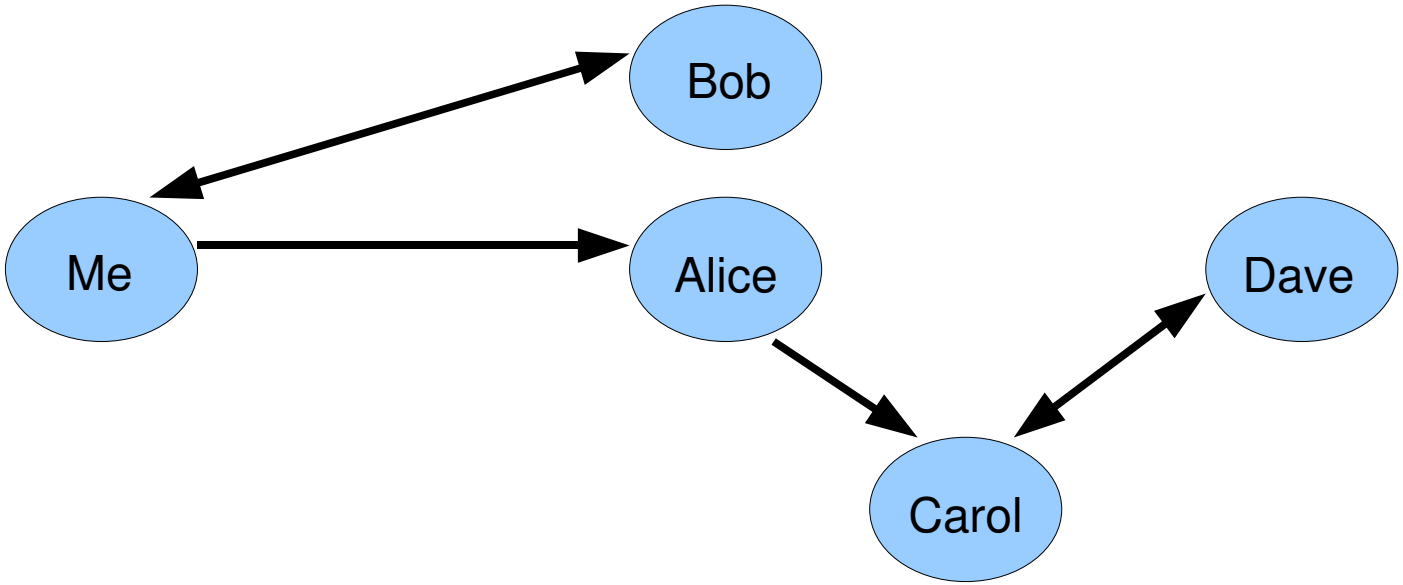
- http://www.gnupg.org/download.html
- Latest versions are 1.4.6 and 2.0.2
- Available precompiled for most systems, source for others.
  - Windows - http://www.gpg4win.org
- Check your distribution, you might already have it.

Public Key Cryptography

- Symmetric Encryption
- Split Key Encryption
  - Public Key
  - Private Key
- Digital Signatures / Hybrid Encryption

Web of Trust

- How can you trust someone you've never met?



- Verify the *Validity* of the keys for people you know, and *Trust* them to verify others.

How? - Create Keys

- gpg –gen-key
- Key Length
  - DSA (Signing Key) will be 1024 bits
  - ElGamal (Encryption Key) can be between 1024 and 4096 bits
  - "The longer the key the more secure it is against brute-force attacks, but for almost all purposes the default keysize is adequate since it would be cheaper to circumvent the encryption than try to break it."
    (GPH)
- **USE A GOOD PASSPHRASE**

Keys – Expiration and Revocation

- Suggested method (GPH)
  - No expiration on main (signing) key
  - Expire encryption keys regularly
- **USE A GOOD PASSPHRASE**
- Generate a revocation certificate (--gen-revoke) immediately
  - Store in a safe place
  - AWAY from secret key

Keys – Multiple Identities

- You may have multiple IDs on one certificate
  - --edit-key, adduid
- IDs may be added but never removed
  - One can revoke a UID's self-signature
- Multiple keys can be used instead

Keys - Verification

- Key ID vs Fingerprint
  - Key IDs are not globally unique
- One must check owner's identity, Key ID, and fingerprint
- User ID and E-Mail tests
- Take note of how certain you are of someone's identity

  ...and how well others are checking, too.

Keys - Signing

- gpg --edit-key
  - "sign" command
- gpg --sign-key
- Indicate how closely you have verified the owner's identity (Validity)
  - Validity is stored with the signed key and shared with the world
- Indicate how much you trust the owner to verify the identity of others (Ownertrust)
  - Ownertrust is a personal assessment and is stored locally
- Local signatures (lsign)

Useful Commands / Options

- --keyserver [keyserver name]
- --send-keys [UID/KeyID/etc]
- --recv-keys [KeyID only]
- --search-keys [string]
  - Searches server for matching keys
- --refresh-keys
  - Retrieves latest version of all keys on your public ring

- Keyserver name and options can be set in ~/.gnupg/gpg.conf

Useful Commands / Options

- --policy-url
  - Link a signing policy page to a signature
- addphoto, showphoto (--edit-key commands)
  --photo-viewer option
  - Attach a photograph to a key
- Common Problem: "WARNING: using insecure memory!"
  - GPG needs to lock memory to prevent paging sensitive data

Advanced Topics / Issues

- E-Mail headers are unencrypted
  - Including Subject
- PGP/GPG interoperability
  - http://www.gnupg.org/(en)/documentation/faqs.html#q5
- PGP-MIME vs Traditional PGP
  - Capability vs Compatibility
  - Good mailers should support both

Conclusion - Links

- This Presentation
  - http://www.nexttime.com/mbrodeur/GPG2007/
- GnuPG Home Page (Downloads, Frontends, FAQ, GPH)
  - http://www.gnupg.org
- RFC 2440 (OpenPGP Message Format)
  - ftp://ftp.rfc-editor.org/in-notes/rfc2440.txt
- OpenPGP vs S/MIME
  - http://www.imc.org/smime-pgpmime.html