Very Brief Introduction to PGP

IP Systems Workshop
Kathmandu, Nepal – July 2004

PGP Software

PGP Software

- PGP 8 (for Windows, Mac, etc.)
- Earlier versions of PGP were free
- GnuPG is a GPL-licenced alternative
  - http://www.gnupg.org/
  - gpg

PGP Keys

PGP Keys

- What is a PGP key?
  - public key cryptography
  - key pair: a public key and a private key
    - the private key is never shared with anybody else
    - the public key can be distributed far and wide

Making a PGP Key

- gpg --gen-key
  - Real Name
  - Comment
  - E-mail address
  - Passphrase

Signing Data

Signing Data

- You have some data you want to send to someone else
- You want that person to be able to tell that it really came from you, and not from someone pretending to be you
- You sign the data

Checking a Signature

- Secret key is required to generate a signature
  - so only the person who has access to the secret key can make one
- Public key is required to verify a signature
  - anybody who has the public key can verify a signature
  - it's important to have confidence that the public key you have is authentic

Encryption

Encrypting Data

- You need a public key to encrypt data
- You can encrypt towards multiple keys simultaneously
  - authenticity of the public key is important if you want to control the readership of the plain text

Decrypting Data

- You need a corresponding secret key to decrypt the data
- The fact that data is encrypted doesn't tell you anything about the identity of the originator
  - messages can be both signed and encrypted (and frequently are)

Trusting Keys

Key Authenticity

- Having confidence in public keys is important
  - verifying signed data is authentic
  - encrypting data
- Manually verifying that public keys are authentic for all possible people you want to talk to would be tedious

Key Signing

- Alice sign's Bob's public key
  - this means that Alice trusted a particular public key to belong to the person whose name is on it (Bob)
  - Alice's PGP software can use that key signature in future when verifying signatures and encrypting data

Web of Trust

- Charlie has never met Bob, but Charlie has a trusted copy of Alice's key
- Charlie can see Alice's signature on Bob's key
- Charlie can verify that the signature was created by a key he is confident belongs to Alice
- Charlie can choose to trust Bob's key based on confidence he has in Alice's signature

Key Signing Party

SANOG IV Key Signing

- 28 July
  - in the evening some time, I think
- Check http://www.sanog.org/
- Ask Gaurab
- Read updates on the SANOG mailing list

Verifying Fingerprints

- People will read out fingerprints at the front of the room
- The person whose fingerprint is being read out will verify that it is accurate
- Other people can thus verify that the fingerprint on the hand-out is correct

Verifying Identity

- After the fingerprint shenanigans, you know that the public keys are valid, according to the person who claimed to be able to know
- If you don't know those people, you should check that they are who they claim to be

Later

- Retrieve the keyring from BigLumber
- Based on the information you recorded on the sheet, you are able to check that the keys you just downloaded are accurate
- Sign the keys that you are able to trust
- Disseminate the keys with your new signature (send to key servers, send to key owners)

The End