PGP Key Management
Basic Principals

SANOG 9

January 14, 2007
Colombo, Sri Lanka

Hervey Allen

Core Concepts

- To encrypt data so that it can be read by one person, you need that person's public key.
- To decrypt data someone sent to you, you need your private key.
- To sign some data, you use your secret key.
- To check a signature on some data, you use the public key of the person who used it.

How do you do all This?

- Using gpg commands at the command line and manipulating text files with them.
- Using built-in tools in your operating system, or your email client.

Practical Aspects

As in what are the initial steps?

- Install GPG (as a port on FreeBSD).
- Create a public/private key pair. This is associated with your email address.
- Extract your public key. Maybe post it somewhere like http://pgp.mit.edu/
- Create your key fingerprint.
- Sign someone's public key.
- Check out http://www.gnupg.org/

A Few Notes

Install GPG

We'll install via ports. If your ports tree is not up-to-date you might install an older version of GnuPG.

You can always install like this:

```
pkg_add -r gnupg
```

Create Public/Private Key Pair

- Don't forget expiry date
- passphrase on private? What if none?
- What does this mean?
- How is this related to ssh?

Extract your Public Key to Text

- Why?
- What do you do with this?

Answers:

- Export to pgp key server
- Place in email
- Have people sign it – why?

Cool Effect – Still awake?

Create a Key Fingerprint

- Why?
- What does this do?
- Where might you use it?

Answers:

- Bottom of email?
- Pgp key server

Sign Someone's Public Key

What's the first step?

This is the “web of trust”

Where do the “signatures” go?

- pgp key server

What will you use this for?

??

- Passwords in email
- Financial information
- Contracts
- Other?

Let's go do it!