Track: ISP Security

TEAM CYMRU
WWW.CYMRU.COM

John Kristoff jtk@cymru.com

Agenda

- PGP Briefing – John Kristoff (Team Cymru)
- PROTECT IP – Chris Morrow (Google)
- BGP Security Demo – Oliver Borchert (NIST)
- Lightning Talks and PoC Personals – you
- PGP Key Signing - you

Add your key to the event keyring

- http://biglumber.com/x/web?keyring=6622
- You should have done this before you arrived
- Most of you didn't do this yet
- Which means the process will be suboptimal

Some PGP Software Options

- Linux or BSD
  - GnuPG package for your OS
- Mac OS X
  - GPGTools for a free GnuPG package
  - Symantec “trialware” PGP Desktop Email
- Windows
  - Symantec “trialware” PGP Desktop Email
- Android
  - Android Privacy Guard (APG)

Basic key pair setup

- Should use at least 2048-bit for new keys
- Create a long, strong password
  - http://dragonresearchgroup.org/tools/drgenpass
- Safeguard your private key
- Publish your key
  - On a key server, e.g.

```
gpg –keyserver pgp.mit.edu –send-keys foo@example.net
```

  - Put it on a web page
  - Add your fingerprint to your business card

Common gpg commands

- Export: `gpg –a –export foo@example.org`
- Sign: `gpg –edit-key foo@example.org`
- Decrypt: `gpg file.asc`
- Encrypt: `gpg –ear foo@example.org file`
- Fingerprint: `gpg –fingerprint foo@example.net`

How key signing should work

- Keys added to ring before arrival
- Bring two “good” forms of id with a picture
- Bring print-outs of your key address and fingerprint
- Coordinator distributes hard copy of key ring
  - Alternatively, hash published of hard copy you verify
- Each participant publicly accepts/denies their key
- Introduce, verify id's and note those you will sign
- Send encrypted signed keys to key owners

Key signing done imperfectly

- We exchange fingerprints with each other
- We verify each others ids
- We send the signed key to the key owner
- Some of you will probably upload the sig to a key server

Why?

- Who might see your plain text emails?
- Slight uptick in usage in the community
- Cool kids and their mean-shortest distance (MSD) rank