Building a Web of Trust

ccTLD Workshop 2004, Amsterdam

Joe Abley <jabley@isc.org>

July 2003

- cisco issued the advisory “cisco-sa -20030717-blocked”, describing a vulnerability which had the potential to cause widespread network disruption
- operators of key infrastructure got a small amount of forewarning of the problem

August 2003

- A copy of openssh-3.4p1.tar.gz containing a trojan horse was loaded onto a compromised ftp server in Calgary, Alberta some time before August 1, 2003
- The FSF announced that ftp.gnu.org had been compromised some time in March 2003

Wouldn’t it be Nice if...

- ... it was possible to discuss sensitive issues with people and have some confidence that they were who they claimed to be?
- ... it was possible to download software from public repositories and be confident that the tarballs hadn’t been meddled with?

Imagine if...

- ... you could encrypt conversations with people to discuss ad-hoc operational issues?
- ... you could transfer customer lists, billing data, logs or packet captures to other people without having to send it in the clear?

Requirements Redux

- Ability to authenticate the origin of arbitrary data (”signing”)
- Ability to encrypt arbitrary data such that the plain text will be obscured from casual observers (”encryption”)
- Ability to do both without having to wave dead chickens in the air or perform unnecessary gynmastics

Motivations

- Not to install SSH/DNS/whatever servers with trojans in them
- To be able to send secure e-mail to people as simply as you can currently send insecure e-mail to people
  - even internal mail gets forwarded out to strange places, more or less all of the time

PGP

- Pretty Good Privacy
- Originally written by Phil Zimmerman in 1991
- Subsequently developed and distributed by MIT, ViaCrypt, PGP Inc, Network Associates
- The GNU Privacy Guard is a compatible and free alternative

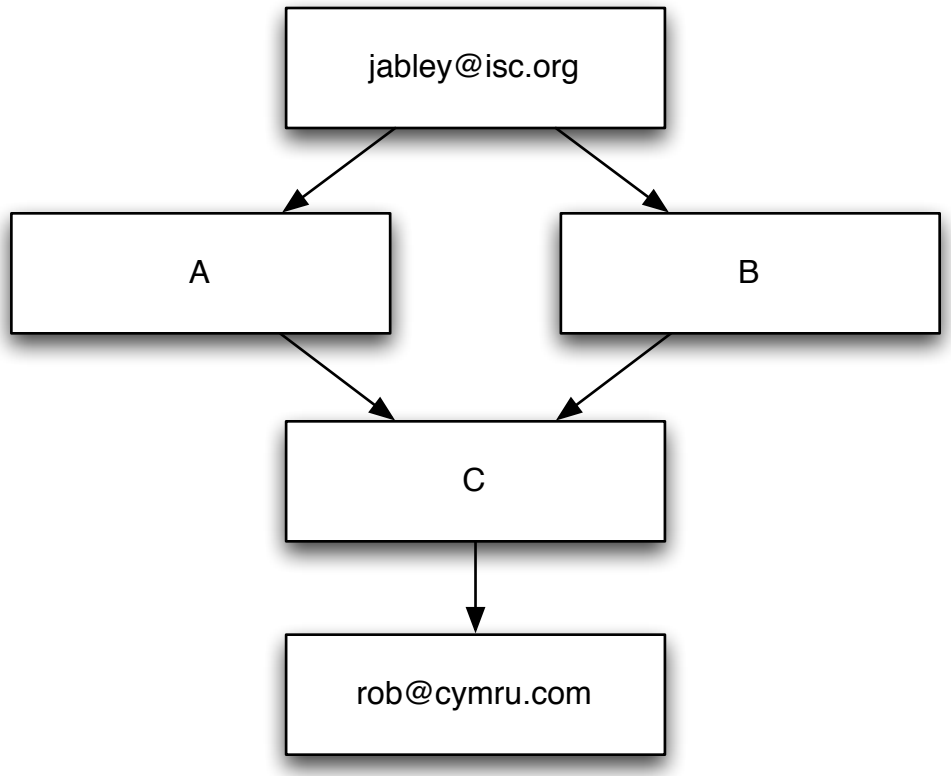
How about that PGP?

- PGP includes key management tools, as well as tools to sign and encrypt data
- Many modern mail clients have workable integration of sign/encrypt functions (some are even good)
- Public keyservers have existed for some time, and they seem to carry a lot of keys

Web of Trust

- PGP is designed to allow key distribution via public, non-secure means, whilst still providing a means to verify the integrity of keys by those that want to use them
- Public keys carry signatures
- A signs B implies "A has some level of trust in the authenticity of B"
- the "Web of Trust" is a directed graph of trust relationships

Web of Trust



- If there is a chain of trust from a key that I trust (my key) to a key that I don't know anything about, some sense of trust can be established
- Paths through the web of trust can be (and frequently are) asymmetric
- Path diversity is good

6 Degrees of Kevin Bacon

- The operator community worldwide is quite large
- There are many people who don't come to ccTLD meetings
- There is, however, a large number of people who know someone who comes to a ccTLD meeting, or knows someone who knows someone
- Building a Web of Trust which is dense and reliable enough for netops is not an unreasonable objective

Even if...

- ... we have PGP software installed
- ... we know how to use it
- ... we can find public keys to verify signatures
- ... we are communicating with someone who also has PGP software installed, and also knows how to use it, who can also find keys

... there is still work to do

- We rarely have a good way of verifying that the public keys we have found are in fact the right ones
- The public key servers are, well, public, and anybody can upload keys to them, so the fact that we find keys there is no indication of reliability
- Peoples' public keys expire
- People lose their secret keys
- The Web of Trust is soggy and has bits of mouldy old food hanging in it

Example

- ftp://ftp.isc.org/isc/bind9/9.2.3rc4/
  - bind-9.2.3rc4.tar.gz
  - bind-9.2.3rc4.tar.gz.asc
- Next, do the traditional stumble through manual pages and “gpg --help” output to work out what flavour of chicken to start waving

Example

```
[jabley@buffoon]% gpg --verify bind-9.2.3rc4.tar.gz.asc bind-9.2.3rc4.tar.gz
gpg: Signature made Sun Sep 21 23:47:32 2003 EDT using RSA key ID 51BAB2ED
gpg: Good signature from "Internet Software Consortium <pgpkey@isc.org>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 8F 10 6A 5E 72 25 3D DD  CE 66 E5 13 E6 8D 99 B7
[jabley@buffoon]%
```

- So, the signature we downloaded from ftp.isc.org corresponds to the tarball we downloaded from ftp.isc.org, and to key 0x51BA2ED which we found on a key server
- Do we know that the tarball is really what Mark, Kurt, Michael, David et all published? Really?

To Do

- Encourage people with whom you actually need to communicate securely to provide you with a mechanism for doing so
- Sign software so people can verify whether it has been tampered with
- Upload keys (and signatures) to keyservers
- Try not to let keys expire
- Strengthen and expand your personal Web of Trust

Keysigning Economics

- If your key has signed a lot of other keys, your key is a useful one for me to trust
- If I trust your key, I will sign it
- If lots of people sign your key, paths to your key will be short and diverse, and it will be easy to use

End