# Living in a monkeysphere

bjoernb

KBS

26. Januar 2012

# What is a monkeysphere?

- Sorry it is not about animals like you might think
- It is about us, living in a monkeysphere
- It is about identifying someone as person
- It is about your peers living in a monkeysphere
- It is about authentication, as we need it for authorization and confidentiality

# Trust relationships

Whom should we trust?

- Should we trust some certificate authorities?
- We do not know how they certificate some service
- We even do not know them, do we?
- Why not trust the people we already know and have relationship to?

# adding services to the web of trust

What we have is the Web of trust, that reflects trust relationships transitively.

- People we know sign services like ssh, https
- We use a service:
    - monkeysphere gets the keys
    - monkeysphere checks trust relations
    - monkeysphere grants us access to a service, if we do trust
    - if we do not trust monkeysphere provides us with the old way

How does this work then?

- create pgp-key with service-protocol and fqdn as uid
- sign the pgp-key
- export the pgp-key to the web of trust
- let others sign the key

What do we get out of this?

- trusting people we know to authenticate a service to us
- getting around calling server administrators asking for fingerprints

This is how we create a key:

```
monkeysphere-host import-key /etc/ssh/ssh_host_rsa_key ssh://bjoern.example.org
```

That is what a key looks like:

```
bjoern:/etc/ssh# monkeysphere-host show-key
pub   2048R/EF569B13 2012-01-22
uid                  ssh://bjoern.example.org
OpenPGP fingerprint: 2B41525D52E6188BA836B2B77DC7EF21EF569B13
ssh fingerprint: 2048 67:cf:a1:73:89:d2:52:a8:77:90:98:1f:f6:6b:f0:dc (RSA)
```

# Sources and documentation

- **Definition of the name**
  `http://www.cracked.com/article_14990_what-monkeysphere.html`
- **monkeysphere project**
  `http://web.monkeysphere.info/`
- **talk at debconf10**
  `http://meetings-archive.debian.net/pub/debian-meetings/2010/debconf10/high/1382_1382_Monkeysphere.ogv`
- **talk at debconf11**
  `http://meetings-archive.debian.net/pub/debian-meetings/2011/debconf11/high/775_Debian_as_though_cryptographic_authentication_mattered.ogv`