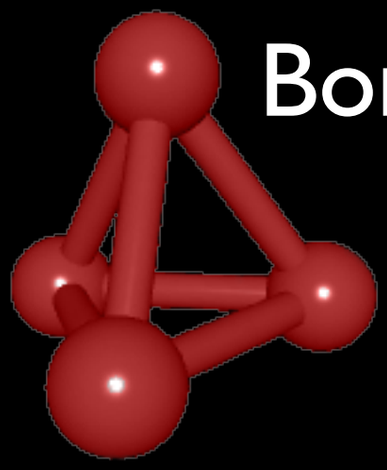

Bond Internet Systems

SSHFP: usando DNSSEC para beneficio propio

João Luis Silva Damas

Gestión de claves en SSH

- El servidor genera una clave nueva
- ¿Cómo se distribuye a todos los clientes?
  - *Are you sure you want to continue connecting (yes/no)?*
  - *¿Quién verifica realmente la clave?*

DNSSEC

- Hasta ahora, para nosotros ingenieros eso sólo ha tenido el aspecto de más trabajo...
- ...pero puede ser una oportunidad
  - mejorar la seguridad
  - practicar antes de que *“caiga el marrón”*

Oportunidad

- .org, .com, .net ya firmados.
- unos 50 ccTLDs ya firmados.

SSHFP

- RFC 4255 (Enero 2006)
- presente en openssh desde 20031015
- SSH Fingerprint
  - Fingerprint de la clave SSH

```
shuttle.c-l-i.net.      IN      SSHFP   2 1 575897C6164E07B920CE92416049AB33DFAF30E6

shuttle.c-l-i.net.      IN      SSHFP   1 1 A59E2131D3137174CB8FBF9556D79282FAECDA36
```

Cómo usarlo

1. Generar el registro de DNS y añadirlo a la zona
2. Configurar los clientes de SSH
3. Asegurar la zona con DNSSEC

Registro SSHFP

- A mano, o bajarse el software de Xcelerance
- http://www.xelerance.com/services/software/sshfp/

Configurar clientes (1)

Añadir la opción

VerifyHostKeyDNS yes|*ask*

en .ssh/config.

Configurar clientes (2)

Habilitar EDNS0 en /etc/resolv.conf o la shell:

options edns0

RES_OPTIONS=edns0

Todavía no están en todos los S.O. pero si en los *BSD/LINUX más recientes

Asegurar la zona DNSSEC

- Si la zona no está asegurada con DNSSEC el proceso no añade mucho
- Con DNSSEC habilitado
  - si la validación tiene éxito, OpenSSH utiliza la nueva clave automáticamente

Ejemplo