Chiffrement intégral des disques

sauf l'initramfs !

Vous avez sans doute chacun dans vos organisations des ordinateurs ou serveurs complètement chiffrés. J'utilise par exemple de mon côté régulièrement LUKS pour chiffrer des partitions LVM.

Problème lorsqu'on redémarre...

Une difficulté se présente lorsque l'on doit redémarrer ces serveurs, ce qui impose une présence physique ou via une console distante pour accéder à la machine que vous souhaitez redémarrer.

Accès ssh pour redémarrer. . .

Un accès console ou une présence physique n'étant pas toujours envisageable, des solutions comme dropbear-initramfs ont vu le jour. Lorsqu'il s'agit d'une ou de quelques machines cette solution peut être envisagée.

Mais en automatique ?

Lorsque vous gérez des parcs informatiques plus larges, cette intervention humaine à chaque démarrage n'est plus adaptée.

C'est là qu'arrive la "Network-Bound Disk Encryption"

Clevis et Tang

Dernière debconf online

Il est maintenant possible de faire un démarrage automatique depuis un réseau de confiance.

Présentation de Christophe BIEDL 30/05/2020.

Clevis

Clevis is a plugable framework for automated decryption. It can be used to provide automated decryption of data or even automated unlocking of LUKS volumes.

```
$ clevis encrypt PIN CONFIG < PLAINTEXT > CIPHERTEXT.jwe
$ clevis decrypt < CIPHERTEXT.jwe > PLAINTEXT
```

Clevis sur github

Tang

Tang is a server implementation which provides cryptographic binding services without the need for an escrow. Clevis has full support for Tang.

- Tang is a server for binding data to network presence.
- Tang Versus Key Escrow: Ease of Use and Simple Security

```
$ echo hi | clevis encrypt tang '{"url": "http://tang.local
The advertisement is signed with the following keys:
        kWwirxc5PhkFIH0yE28nc-EvjDY

Do you wish to trust the advertisement? [yN] y
```

Tang sur github

Autres usages ?

Si le mécanisme est solide, pourquoi pas l'implémenter pour stocker d'autres secrets (pour remplacer le mot de passe sur des réseaux de confiance?)

Jusqu'où s'arrête le réseau?

Echange

- Avez-vous déja mis en oeuvre ces outils ?
- Avez-vous une critique à formuler sur la mise en oeuvre de ces outils (crypto, processus, . . .).
- Quel niveau de confiance peut-on accorder selon vous à ce mécanisme de PIN selon vous? . . .