LA CHAÎNE DE CONFIANCE DE DEBIAN

(Debian Web of trust)

DOMINIQUE DUMONT

QU'EST QUE LE PROJET DEBIAN

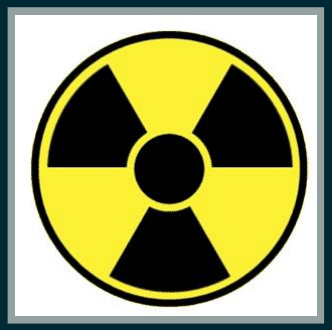
debian

- distribution Linux «universelle»
- pour serveurs, ordinateur de bureau, carte ARM
- logiciel libre (pas simplement gratuit)
- base de Ubuntu, Linux Mint, Raspbian et d'autres

EXAMPLES D'INSTALLATION DE LOGICIEL

- `sudo apt install un-logiciel`
- `npm install -g unLogiciel`
- `brew install unLogiciel`
- `choco install un-logiciel`
- `docker run acme/un-logiciel`
- `curl https://acme.com/un-logiciel.sh | sudo bash -`

UNE QUESTION DE CONFIANCE



Installer un logiciel implique une confiance absolue:

- envers l'auteur
- sur le serveur de stockage
- sur le moyen de transport

INSTALLATION D'UN PAQUET DEBIAN

```
sudo apt install cme
```

- trouve l'URL du paquet sur un serveur miroir
- télécharge le paquet
- installe le paquet

Mais:

- les serveurs miroirs ne sont pas sous le contrôle de Debian
- la connection n'est pas sûre (ftp, http)

SOLUTION / 1ÈRE PARTIE

Utiliser de la crypto (`gpg`) pour vérifier le contenu.
Dans l'exemple avec `cme`, `apt` et `gpg` vérifient:

- l'intégrité du logiciel
- que le logiciel a été signé par `dod@debian.org`
- que `dod@debian.org` est sur la liste des personnes autorisées

PROBLÈME

Qui se cache derrière `dod@debian.org` ?

Une personne, une compagnie ?

Comment lui faire confiance ?

SOLUTION / 2E PARTIE

A charge pour le projet Debian de vérifier:

- l'identité de dod
- que dod est membre de Debian

PROBLÈME

Les développeurs sont répartis dans le monde. Pas moyen pour les principaux responsables de Debian de rencontrer les nouveaux participants.

SOLUTION

Chaque développeur Debian peut:

- vérifier l'identité d'une personne (pièce d'identité requise)
- signer la clef publique gpg de cette personne avec sa clef privée
- et réciproquement
- étape indispensable pour qu'un contributeur devienne développeur Debian

ET LA CONFIANCE DANS TOUT ÇA ?

- le web of trust garantie l'identité réelle d'un développeur Debian
- mais pas ses intentions.
- elles sont vérifiées petit à petit quand une personne contribue puis devient développeur Debian

C'est pas parfait, mais ça fonctionne bien.

QU'EN EST-IL DE VOTRE GESTIONNAIRE DE PAQUET FAVORI ?

Quelle est chaîne de confiance de votre gestionnaire de paquet favori?

Y-a t'il des points faibles ?

APPLICATION PRATIQUE

Si vous voulez contribuer à Debian, je peux signer vos clefs à l'apéro.