Les packages signés sous OpenBSD

Marc Espie <espie@openbsd.org>

July 18, 2014

Les packages sous OpenBSD

Spécifiques à OpenBSD

Ça n'est *pas* le `pkg_add` de NetBSD
Ni le `pkgng` de FreeBSD

Les packages sous OpenBSD

Spécifiques à OpenBSD

Ça n'est *pas* le `pkg_add` de NetBSD
Ni le `pkgng` de FreeBSD

- Tout est en perl
- Mises à jour depuis 2006

Les packages sous OpenBSD (2)

Outils standardisés

```
#! /usr/bin/perl
use OpenBSD::PackingList;

package OpenBSD::PackingElement;
sub walk
{
# do nothing
}

package OpenBSD::PackingElement::Sample;
sub walk
{
my $self = shift;
print $self->fullname, "\n";
}

package main;

my $p = OpenBSD::PackingList->from_installation("pkgname");

$p->walk;
```

Les packages sous OpenBSD (3)

Pas de cache

- L'installation se fait au vol
- Les noms de packages sont standardisés
- On télécharge "juste ce qu'il faut" (e.g., la packing-list)

Les packages sous OpenBSD (3)

Pas de cache

- L'installation se fait au vol
- Les noms de packages sont standardisés
- On télécharge "juste ce qu'il faut" (e.g., la packing-list)

Vérif d'abord

- On vérifie tout sur la plist et le fs
- ...Puis on installe/update
- Pas de système transactionnel

Signatures antiques

Gzip

On peut mettre des choses dans l'entête de Gzip

- comme une signature X509
- ... conduit à gzsig

Signatures antiques

Gzip

On peut mettre des choses dans l'entête de Gzip

- comme une signature X509
- ... conduit à gzsig

Défauts

- Il faut télécharger tout le package
- ... surface d'attaque énorme

Signature moderne 1

Cahier des charges

- Il y a 3 ans, demande de 3rd party
- Mécanisme générique $\rightarrow$ plus simple
- Certificats X509

Signature moderne 1

Cahier des charges

- Il y a 3 ans, demande de 3rd party
- Mécanisme générique → plus simple
- Certificats X509

Just-In-Time

- On signe juste la packing-list
- Celle-ci contient les sha256 de tout
- Signature validée en même temps que les infos de mise-à-jour
- Chaque fichier vérifié à l'extraction

Signature moderne 2

Et les méta info

- Entête de tar
- Tout ce qui est important est dans la PLIST

Signature moderne 2

Et les méta info

- Entête de tar
- Tout ce qui est important est dans la PLIST

X509

- Bizarrerie d'openssl (mime-encoding)
- Compliqué
- Opaque (PKI)

Enter Signify

Une signature moderne

- écrit par Ted Unangst
- crypto elliptique
- signe du sha512
- pas de PKI!

Enter Signify

Exemple

```
untrusted comment: signature from openbsd 5.6 packages private key
RWR0EANmo9nqhtL3waUA0Buq/b2QHW06S0rufjAwgztCOU5P6+7kh+YnyetC6jiaV57WURH9n0EvoiMbzPmbR+qxIeUf6jWfBgg=
SHA256 (INSTALL.amd64) = 84b7e7cb7e5bc44a85dd60c1f6c1730900cc833f66a209e32b3d21132f637308
SHA256 (base56.tgz) = 0db2b0336007cac50f289a5d4f71cb4cbed085cf8656e27deef390b758138a0d
SHA256 (bsd) = 03b95b2e4f00421aab0c74ae3d6a2ef90992c765022a14af989e4d74b6d360ac
SHA256 (bsd.mp) = fae0d3b4a7ef6dc0d840996a3c0820682f63d516af70dfea3d28b0d7788eff0b
SHA256 (bsd.rd) = fc440856dcb0c0f09f363ddf7db6b93e7555eb0630b1136d732d2100108e38bb
SHA256 (cd56.iso) = d203cd7774d6f09f4555f7f23b74ce969e96162c23baeed2fafc5fcd35575a75
SHA256 (cdboot) = fd65d49a4765bb9c83ccbb77e9a99385aa7c4cd0cc7636db9327ca102d8106b3
SHA256 (cdbr) = c5244fd55f85263035feb411f6e7fc17614b160116c878e850d84b17f67f2951
SHA256 (comp56.tgz) = e30dacce8a067ead6cedb0dff63f0a605e9f2065d404cc78608a584e99190009
SHA256 (etc56.tgz) = 22b9cc137df79a7ec0c910d80f1b98b561adf33ff589ab4625f48090b76fef74
SHA256 (floppy56.fs) = 8c0a5cc9836d09c5d0a357294b61f58f076ea632afebd319aa143de56244732d
SHA256 (game56.tgz) = 4694c173836a095cc7bbea751995934cbff301aff64ea2a075d1ff7f2b8f1abf
SHA256 (install56.fs) = 9407ba385a5fc19587f77e1e4debbd0a54538c6ea86d3861ac6d8c78ccd67917
SHA256 (install56.iso) = 4fc8acfbb27315a96ad030270a0500342dc8a3f54866ea97c088ae8ac987ce9f
SHA256 (man56.tgz) = 46492a6b6751e1e400f064a8fdadfa68fa5090f54962acade2e4537d7494f8e7
SHA256 (miniroot56.fs) = 0bf0b54018cb1f96fe21f20e5f761c4051512627c77cc650af17d3600e0c945d
```

Question de process

Transparence

- Une clé, un usage
- Signé après coup, en mode déconnecté
- Pas de révocation

Et les packages

Caractéristiques

- Pas de sha256 global
- Signature après coup, sur une machine séparée

Et les packages

Caractéristiques

- Pas de sha256 global
- Signature après coup, sur une machine séparée

Problèmes

- Signature = gunzip/sign/repack
- trop lent
- chunked gzip

Propriétés

Perl

- `$plist->write_no_sig($fh);`
- Tout est signé (date aussi)
- Pas de recalcul des sha256

Propriétés

Perl

- `$plist->write_no_sig($fh);`
- Tout est signé (date aussi)
- Pas de recalcul des sha256

Cohérence

- Un package toujours updaté (quirks)
- Date de signature
- Liste de packages à risque

Bonus!

Reordered packages

- Fichiers qui changent en tête de package
- LRU
- Tout petit! (histoire des sha256)

Bonus!

Reordered packages

- Fichiers qui changent en tête de package
- LRU
- Tout petit! (histoire des sha256)

Fan-out

- 40–50 Go
- Rsyncable gzip $\rightarrow$ fragile
- low-tech solution
- timestamp à zero
- chunked gzip "from end"
- .gmo sans ts

Questions !!!