Des clés dans le DNS, pour remplacer X.509 ?

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

JRES, 23 novembre 2011

X.509, c'est quoi ?

- X.509 est une norme de certificats (certificat = clé + méta-données + signature) numériques.

X.509, c'est quoi ?

- X.509 est une norme de certificats (certificat = clé + méta-données + signature) numériques.
- Son modèle de sécurité est qu'une AC (Autorité de Certification) signe le certificat après vérification. Les utilisateurs font ensuite confiance aux AC (compétence, honnêteté, sécurité). Le modèle est donc multi-racines.

X.509, c'est quoi ?

- X.509 est une norme de certificats (certificat = clé + méta-données + signature) numériques.
- Son modèle de sécurité est qu'une AC (Autorité de Certification) signe le certificat après vérification. Les utilisateurs font ensuite confiance aux AC (compétence, honnêteté, sécurité). Le modèle est donc multi-racines.
- Qui décide de qui est une AC ? Mozilla ? Microsoft ? L'ANSSI (cf. RGS) ? Le CNRS ? L'utilisateur ?

Utilisation de X.509 dans l'Internet

- L'utilisation la plus courante dans l'Internet est pour TLS, surtout HTTPS.

Utilisation de X.509 dans l'Internet

- L'utilisation la plus courante dans l'Internet est pour TLS, surtout HTTPS.
- Le serveur présente un certificat, le client peut vérifier que ce certificat a été signé par une AC de son magasin. Et cela permet d'afficher un joli cadenas.

Utilisation de X.509 dans l'Internet

- L'utilisation la plus courante dans l'Internet est pour TLS, surtout HTTPS.
- Le serveur présente un certificat, le client peut vérifier que ce certificat a été signé par une AC de son magasin. Et cela permet d'afficher un joli cadenas.
- Cela protège contre le terrible Homme au Milieu.

Les problèmes et limites de X.509

Le principal problème de X.509

Il est multi-racines, avec un `OR` entre les racines. Un certificat signé par **n'importe quelle AC du magasin** convient. Il ne sert donc à rien de choisir soigneusement son AC.

2011, année terrible pour X.509

1. Mars, Comodo est détourné via un revendeur (le mot de passe était dans la DLL) et émet des vrais-faux certificats pour `gmail.com`.

2011, année terrible pour X.509

1. Mars, Comodo est détourné via un revendeur (le mot de passe était dans la DLL) et émet des vrais-faux certificats pour `gmail.com`.
2. Août, Opération « Tulipe Noire », DigiNotar est piraté (même plus de traçabilité) et émet plein de vrais-faux certificats. La société se met en faillite, pour éviter d'assumer ses responsabilités.

2011, année terrible pour X.509

1. Mars, Comodo est détourné via un revendeur (le mot de passe était dans la DLL) et émet des vrais-faux certificats pour `gmail.com`.
2. Août, Opération « Tulipe Noire », DigiNotar est piraté (même plus de traçabilité) et émet plein de vrais-faux certificats. La société se met en faillite, pour éviter d'assumer ses responsabilités.
3. Octobre, l'EFF révèle, en analysant les révocations, que quatre autres AC avaient été compromises sans que cela soit révélé publiquement.

Autres modèles de sécurité

- Le modèle TOFU (SSH ou bien extensions au navigateur HTTPS, comme par exemple CERT Patrol). On fait confiance au certificat la première fois et on ne s'inquiète que s'il change ensuite. Mais il est difficile de savoir si un changement est légitime ou pas (cas de Facebook en octobre).

Autres modèles de sécurité

- Le modèle TOFU (SSH ou bien extensions au navigateur HTTPS, comme par exemple CERT Patrol). On fait confiance au certificat la première fois et on ne s'inquiète que s'il change ensuite. Mais il est difficile de savoir si un changement est légitime ou pas (cas de Facebook en octobre).
- Les modèles à réseau de pairs, qu'on interroge pour savoir ce qu'ils pensent (Perspectives ou Convergence). Intéressant car purement pair à pair. Mais peu de réalisations concrètes encore.

Mettre les clés dans le DNS

Troisième approche : réutiliser l'infrastructure et les réseaux de confiance existants, en mettant les clés/certificats dans le DNS.

- C'est le projet DANE (*DNS-based Authentication of Named Entities*) de l'IETF. Cahier des charges dans le RFC 6394.

Mettre les clés dans le DNS

Troisième approche : réutiliser l'infrastructure et les réseaux de confiance existants, en mettant les clés/certificats dans le DNS.

- C'est le projet DANE (*DNS-based Authentication of Named Entities*) de l'IETF. Cahier des charges dans le RFC 6394.
- DANE a trois modes d'opération, selon qu'on veut plus ou moins couper les ponts avec X.509.

Les trois modes de DANE

- Type 0 : on ajoute dans le DNS le certificat de son AC, évitant ainsi les attaques de type DigiNotar. On continue à valider avec X.509.

Les trois modes de DANE

- Type 0 : on ajoute dans le DNS le certificat de son AC, évitant ainsi les attaques de type DigiNotar. On continue à valider avec X.509.
- Type 1 : très proche du type 0, on ajoute dans le DNS son certificat, ce qui protège même contre sa propre AC.

Les trois modes de DANE

- Type 0 : on ajoute dans le DNS le certificat de son AC, évitant ainsi les attaques de type DigiNotar. On continue à valider avec X.509.
- Type 1 : très proche du type 0, on ajoute dans le DNS son certificat, ce qui protège même contre sa propre AC.
- Type 2 : on dit adieu à X.509, on publie son certificat dans le DNS et aucune validation X.509 n'est faite.

Exemple d'enregistrement DANE - type 1

Avertissement : le protocole n'est pas fini, la syntaxe peut changer.

Cet enregistrement dit « voici ma clé publique, fais les deux vérifications, X.509 et cette clé » (type 1, le premier champ après "DANE")

```
_443._tcp.www.example.com. IN DANE (
   1 1 2 92003ba34942dc74152e2f2c408d29ec
         a5a520e7f2e06bb944f4dca346baf63c
         1b177615d466f6c4b71c216a50292bd5
         8c9ebdd2f74e38fe51ffd48c43326cbc )
```

Exemple d'enregistrement DANE - type 1

Avertissement : le protocole n'est pas fini, la syntaxe peut changer.

Cet enregistrement dit « voici ma clé publique, fais les deux vérifications, X.509 et cette clé » (type 1, le premier champ après "DANE")

```
_443._tcp.www.example.com. IN DANE (
   1 1 2 92003ba34942dc74152e2f2c408d29ec
         a5a520e7f2e06bb944f4dca346baf63c
         1b177615d466f6c4b71c216a50292bd5
         8c9ebdd2f74e38fe51ffd48c43326cbc )
```

(Deuxième champ après "DANE" : 1 pour "clé", troisième champ, 2 pour "condensat SHA-512")

Exemple d'enregistrement DANE - type 2

Cet enregistrement dit « voici mon certificat, oublie X.509, cette affirmation suffit »

```
_443._tcp.www.example.com. IN DANE (
   2 0 0 3082030730820 1efa003020102020... )
```

Exemple d'enregistrement DANE - type 2

Cet enregistrement dit « voici mon certificat, oublie X.509, cette affirmation suffit »

```
_443._tcp.www.example.com. IN DANE (
   2 0 0 3082307308201efa003020102020... )
```

(Deuxième champ après "DANE" : 0 pour "certificat complet", troisième champ, 0 pour "valeur effective, pas condensat")

L'importance de DNSSEC

- Évidemment, tout ceci suppose que le client récupère le bon enregistrement DANE, malgré l'Homme au Milieu

L'importance de DNSSEC

- Évidemment, tout ceci suppose que le client récupère le bon enregistrement DANE, malgré l'Homme au Milieu
- Le DNS est trop vulnérable pour cela (faille Kaminsky)

L'importance de DNSSEC

- Évidemment, tout ceci suppose que le client récupère le bon enregistrement DANE, malgré l'Homme au Milieu
- Le DNS est trop vulnérable pour cela (faille Kaminsky)
- DNSSEC est donc indispensable (quasi-indispensable ?) à DANE

L'importance de DNSSEC

- Évidemment, tout ceci suppose que le client récupère le bon enregistrement DANE, malgré l'Homme au Milieu
- Le DNS est trop vulnérable pour cela (faille Kaminsky)
- DNSSEC est donc indispensable (quasi-indispensable ?) à DANE
- C'est pourquoi, malgré les vulnérabilités connues de X.509, l'idée de sérieusement le remplacer par des clés dans le DNS est récente. (Elle date du déploiement effectif de DNSSEC, en 2010.)

DNS+DNSSEC est-il un progrès ?

Pour ne pas remplacer une technique percée par une autre analysons la sécurité de DNS + DNSSEC.

- DNSSEC n'est pas encore déployé partout : la racine et tous les gros TLD, mais pas beaucoup de domaines en dessous (20 % en Tchéquie, beaucoup moins en France).

DNS+DNSSEC est-il un progrès ?

Pour ne pas remplacer une technique percée par une autre analysons la sécurité de DNS + DNSSEC.

- DNSSEC n'est pas encore déployé partout : la racine et tous les gros TLD, mais pas beaucoup de domaines en dessous (20 % en Tchéquie, beaucoup moins en France).
- Peu de résolveurs valident (coucou aux gens de Lothaire, qui le font).

DNS+DNSSEC est-il un progrès ?

Pour ne pas remplacer une technique percée par une autre analysons la sécurité de DNS + DNSSEC.

- DNSSEC n'est pas encore déployé partout : la racine et tous les gros TLD, mais pas beaucoup de domaines en dessous (20 % en Tchéquie, beaucoup moins en France).
- Peu de résolveurs valident (coucou aux gens de Lothaire, qui le font).
- DNSSEC ne protège pas contre le contenu qui était incorrect au départ. Si le registre est piraté (cas de l'affaire `www.google.bd`), DNSSEC ne pourra rien faire.

DNS+DNSSEC est-il un progrès ?

Pour ne pas remplacer une technique percée par une autre analysons la sécurité de DNS + DNSSEC.

- DNSSEC n'est pas encore déployé partout : la racine et tous les gros TLD, mais pas beaucoup de domaines en dessous (20 % en Tchéquie, beaucoup moins en France).
- Peu de résolveurs valident (coucou aux gens de Lothaire, qui le font).
- DNSSEC ne protège pas contre le contenu qui était incorrect au départ. Si le registre est piraté (cas de l'affaire `www.google.bd`), DNSSEC ne pourra rien faire.
- Les acteurs des noms de domaine sont-ils meilleurs que les AC X.509 ? Pas forcément.

DNS+DNSSEC est-il un progrès ?

Pour ne pas remplacer une technique percée par une autre analysons la sécurité de DNS + DNSSEC.

- DNSSEC ne protège pas contre le contenu qui était incorrect au départ. Si le registre est piraté (cas de l'affaire `www.google.bd`), DNSSEC ne pourra rien faire.
- Les acteurs des noms de domaine sont-ils meilleurs que les AC X.509 ? Pas forcément.
- Mais, au moins, leur pouvoir est borné. Le registre de `.BD` peut être incompétent, cela n'affectera pas `www.google.fr`.