Sécurité de DANE

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 9 décembre 2013

https://www.bortzmeyer.org/securite-dane.html

Le système DANE ("*DNS-Based Authentication of Named Entities*") permet d'augmenter la sécurité des échanges chiffrés avec TLS en permettant au gérant du serveur de publier lui-même le certificat qu'il utilise, et en permettant au client de vérifier, par une deuxième voie, le DNS, que le certificat est le bon. L'expérience d'autres technologies de sécurité est que DANE, s'il est effectivement déployé dans le futur, sera attaqué par des méchants compétents et que ses faiblesses seront exploitées. C'est donc une bonne idée, avant ce déploiement massif, de se demander quelle est la sécurité de DANE et quelles attaques sont possibles. Plaçons-nous donc dans la peau de l'attaquant. Alice se connecte au serveur de Bob en TLS (par exemple en HTTPS), et Bob utilise DANE. Que peut faire Mallory pour se faire passer pour Bob sans qu'Alice s'en aperçoive ?

Si vous ne connaissez pas DANE, vous pouvez l'apprendre dans l'excellent dossier thématique de l'AFNIC <http://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/7450/show/securiser-les-communications-sur-internet-de-bout-en-bout-avec-le-protocole-dan
html> ou (plus anciens) dans mon article à JRES <https://www.bortzmeyer.org/jres-dane-2011.
html> ou encore dans mon article sur le RFC 6698 [1], qui normalise DANE. Avant DANE, les communications en TLS (RFC 5246) étaient sécurisées par X.509 uniquement. Une grosse faiblesse de X.509 est que n'importe quelle autorité de certification peut émettre un certificat pour n'importe quel nom, même s'il n'est pas son client. On voit ainsi régulièrement des faux certificats émis par des AC malhonnêtes, maladroites ou piratées, par exemple pour intercepter le trafic des services de Google.

Donc, plaçons-nous quelques années dans le futur. DANE est largement déployé, des sites Web accessibles en HTTPS publient les enregistrements DANE (nommés TLSA) dans leurs zones DNS signées avec DNSSEC, Alice veut se connecter au serveur de Bob et Mallory, qui peut détourner le trafic, veut être Homme au Milieu sans que le navigateur Web d'Alice ne donne l'alarme.

D'abord, Mallory, en vrai professionnel, étudie les mises en œuvre de DANE dans les navigateurs. Il y a deux façons très différentes d'utiliser DANE, les utilisations 0 et 1 d'un côté, et les 2 et 3 de l'autre.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6698.txt

Lorsque l'enregistrement TLSA contient 0 ou 1 dans le champ « Utilisation du certificat » ("*Certificate usage*"), l'authentification DANE se fait **en plus** de l'authentification X.509 classique (plus exactement PKIX, un profil de X.509 décrit dans le RFC 5280). Avec ces utilisations 0 et 1, Mallory doit casser DNSSEC et X.509. Lorsque l'enregistrement TLSA contient 2 ou 3, l'authentification DNSSEC se fait à la place de l'authentification X.509 classique.

Quelles utilisations seront adoptées ? Les plus prudents, soucieux de ne pas lâcher la proie pour l'ombre, adopteront sans doute 0 et 1, **renforçant** la sécurité X.509 par celle de DNSSEC (stratégie « ceinture et bretelles »). Les autres, ou simplement ceux qui ne veulent pas passer par les procédures et coûts des AC X.509, adopteront les utilisations 2 et 3 (stratégie « remplacer les bretelles par des ceintures »). Mais il ne faut pas oublier que les choix de sécurité, dans le cas de HTTPS, sont faits essentiellement par les auteurs de navigateurs, pas par les utilisateurs (que ce soit Alice ou Bob). Il est donc possible que certains navigateurs ne mettent en œuvre DANE que pour les usages 0 et 1, jugeant 2 et 3 trop dangereux.

Donc, Mallory regarde l'enregistrement TLSA de Bob (ici, avec le site Web <https://dane.rd.nic.fr/>) :

```
% dig TLSA _443._tcp.dane.rd.nic.fr

; <<>> DiG 9.9.3-rpz2+rl.13214.22-P2-Ubuntu-1:9.9.3.dfsg.P2-4ubuntu1 <<>> TLSA _443._tcp.dane.rd.nic.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40804
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;_443._tcp.dane.rd.nic.fr. IN TLSA

;; ANSWER SECTION:
_443._tcp.dane.rd.nic.fr. 1 IN TLSA 3 0 1 (
C68EBCC998FDA83222CABF2C0228ECC413566E709E5D
C5CF25396A8BF4342DD3 )
...
;; Query time: 117 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Dec 09 10:39:48 CET 2013
;; MSG SIZE  rcvd: 876
```

OK, il est bien signé (le bit `AD` pour "*Authentic Data*"). Rappelons en effet que DANE **dépend** de DNSSEC. Le RFC 6698 est très clair là-dessus (après de longs débats à l'IETF) : les enregistrements TLSA non signés sont ignorés. Une conséquence est que la sécurité de DANE dépend d'une bonne politique DNSSEC. Par exemple, pour être vraiment sûre, la validation DNSSEC devrait se faire sur le poste local d'Alice <https://www.bortzmeyer.org/son-propre-resolveur-dns.html>.

Ici, l'utilisation est 3 (les données dans l'enregistrement TLSA sont un certificat auto-signé). Quelles sont les attaques possibles pour Mallory ? Sauf si Mallory connait un moyen de casser cryptographiquement DNSSEC, la seule solution est de s'attaquer à un des intermédiaires dans la chaîne DNSSEC, afin de supprimer ou de remplacer l'enregistrement TLSA. En effet, comme le DNS, DNSSEC fonctionne selon une logique arborescente : la validation de `www.example.nl` dépend de la racine du DNS <https://www.bortzmeyer.org/dnssec-racine-nsa.html> et du registre de `.nl`. On a déjà vu des registres ou des bureaux d'enregistrement être piratés <https://www.bortzmeyer.org/

attaques-sea.html>, donc cela n'a rien d'impossible (même si DNSSEC complique sérieusement la tâche de Mallory <https://www.bortzmeyer.org/piratage-registre-dnssec.html>). Avec l'utilisation 3, pas besoin d'attaquer une AC ou de trouver une faille dans le système X.509. Mais est-ce à dire qu'on a simplement remplacé la confiance dans son AC par la confiance dans son registre de noms de domaine ? Si c'était le cas, DANE ne changerait pas grand'chose. Mais il y a une grosse différence : avec X.509, vous devez faire confiance à **toutes** les AC, pas seulement celle que vous avez choisi et donc vous êtes clients, car toutes peuvent émettre un certificat pour le site Web de Bob. Avec DNS et DNSSEC, vous choisissez à qui vous faites confiance.

Et si l'enregistrement TLSA avait l'utilisation 2 ? Dans ce cas non plus, il n'y a pas de validation X.509 depuis le magasin de certificats du navigateur Web, et donc pas la peine de détourner une des AC reconnues des auteurs de navigateurs. Avec un enregistrement TLSA d'utilisation 2, le contenu de l'enregistrement TLSA est le certificat d'une AC (qui n'a pas besoin d'être dans le magasin des navigateurs). On a donc deux possibilités d'attaque : contre le système d'enregistrement de noms de domaine, comme dans le cas de l'utilisation 3 précédemment cité, ou bien une attaque contre cette AC particulière, par exemple en la piratant. Notons encore une fois que, contrairement au X.509 classique, Mallory n'a pas le choix de la cible, elle doit réussir à pirater une AC particulière. Conclusion : si l'AC désignée par l'enregistrement TLSA d'utilisation 2 est gérée par une organisation différente de celle de Bob, on a élargi les possibilités de Mallory.

Et si on a le navigateur paranoïaque hypothétique que je citais, celui qui refuse les utilisations 2 et 3 ? Ce cas n'est pas prévu par le RFC. Le plus logique serait qu'il ignore ces enregistrements (les faire correspondre d'autorité aux utilisations 0 et 1 serait une violation de la norme DANE, avec plein de résultats surprenants). On se trouverait donc ramené au cas d'un navigateur qui n'a pas DANE du tout, ce qui est le cas de la totalité de ceux d'aujourd'hui.

Et avec l'utilisation 1 ? Cette fois, les habitué(es) du X.509 classique se retrouveront en terrain connu. Une valeur 1 dans la champ « Utilisation du certificat » de l'enregistrement TLSA signifie que les données de l'enregistrement contiennent le certificat effectivement utilisé par le site **et** qu'il faut le valider par les mécanismes X.509 habituels. C'est la sécurité maximale : DNSSEC plus X.509. Mallory doit cette fois pirater une AC (pour faire un autre certificat) **et** modifier l'enregistrement TLSA. Pirater une AC, même celle utilisée par Bob, ne suffirait plus car le certificat est épinglé par Bob : celui-là et pas un autre.

Reste l'utilisation 0, nombre dont la présence dans le champ Utilisation signifie que l'enregistrement TLSA désigne une AC, celle de Bob. Mallory doit donc pirater le DNS pour le changer **ou bien** pirater cette AC particulière. Notez que, pour les utilisations 0 et 1, cette analyse dépend du fait que le piratage de l'AC et celui du DNS sont des opérations indépendantes. Si, en piratant l'un, Mallory peut pirater l'autre, la double sécurité ne sera en fait qu'une illusion. Or, certaines AC signent des certificats après juste un échange de courrier électronique, qui peut être détourné si on détourne le DNS.

En conclusion, DANE, comme toute technique de sécurité, n'est pas invulnérable. Un attaquant déterminé, patient et compétent peut en venir à bout. Il est donc nécessaire de faire une analyse de la sécurité et de voir ce qu'on risque.

Un autre article en français avec une analyse détaillée de la sécurité de DANE (avec notamment les risques des attaques par rejeu) est celui de Florian Maury <http://www.hsc.fr/ressources/articles/misc_dnssecpkix/index.html.fr>. En anglais, curieusement, je n'ai pas encore trouvé grand'chose, à part bien sûr la section 8 du RFC 6698.