RFC 6962 : Certificate Transparency

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 juin 2013

Date de publication du RFC : Juin 2013

https://www.bortzmeyer.org/6962.html

Plusieurs attaques spectaculaires, notamment celle contre DigiNotar, ont montré la fragilité de l'actuel système de gestion de certificats X.509. Comme n'importe quelle AC peut émettre un certificat pour n'importe quel nom de domaine, il ne suffit pas d'évaluer la sécurité de son AC, il faudrait idéalement évaluer **toutes** les AC. Ce RFC propose une approche différente : encourager/obliger les AC à **publier** « au grand jour » les certificats qu'elles émettent. Un titulaire d'un certificat qui craint qu'une AC n'émette un certificat à son nom sans son autorisation n'a alors qu'à surveiller ces publications. (Il peut aussi découvrir à cette occasion que sa propre AC s'est fait pirater ou bien est devenue méchante et émet des certificats qu'on ne lui a pas demandés.) À noter qu'une deuxième version du système décrit ici a été publiée en décembre 2021, dans le RFC 9162 [1] mais elle reste, fin 2021, peu déployée.

Ce n'est pas par hasard que les auteurs de ce RFC sont trois employés de Google. Dans l'affaire DigiNotar, comme dans d'autres affaires analogues, le premier vrai/faux certificat émis par celui qui a piraté une AC est souvent un certificat pour `gmail.com`, de façon à permettre d'espionner le trafic vers Gmail. La proposition de ce RFC (qui est encore expérimental) est d'empêcher l'émission « discrète » de vrais/faux certificats qui seraient ensuite utilisés uniquement à certains endroits (l'Iran dans le cas de DigiNotar mais cela peut aussi concerner des entreprises qui font des attaques de l'homme du milieu contre leurs propres employés).

Le principe est donc de créer un (ou plusieurs) journal des certificats émis. Le journal doit être public, pour que Google ou n'importe qui d'autre puisse l'auditer. Il doit être en mode « ajout seulement » pour éviter qu'on puisse réécrire l'histoire. Les certificats sont déjà signés mais le journal a ses propres signatures, pour prouver son intégrité. Conceptuellement, ce journal est une liste de certificats dans l'ordre de leur création. Toute AC peut y ajouter des certificats (la liste ne peut pas être ouverte en écriture à tous, de crainte qu'elle ne soit remplie rapidement de certificats bidons). En pratique, le RFC estime

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc9162.txt`

que la liste des AC autorisées à écrire dans le journal sera l'union des listes des AC acceptées dans les principaux navigateurs Web (voir aussi la section 4.7).

À chaque insertion, le journal renvoie à l'AC une estampille temporelle signée, permettant à l'AC de prouver qu'elle a bien enregistré le certificat. Si une AC peut présenter cette signature mais que le certificat est absent du journal, l'observateur aura la preuve que le journal ne marche pas correctement. Le format exact de cette estampille temporelle est décrit en section 3.2. Elle devra être envoyée au client par les serveurs TLS, comme preuve de la bonne foi de l'AC (cf. sections 3.3 et 5.2).

Les titulaires de certificats importants, comme Google, mais aussi des chercheurs, des agences de sécurité, etc, pourront alors suivre l'activité de ce(s) journal (journaux) public(s) (section 5.3 du RFC). Ce qu'ils feront en cas de détection d'un certificat anormal (portant sur leur nom de domaine, mais qu'ils n'ont pas demandé) n'est pas spécifié dans le RFC : cela dépend de la politique de l'organisation concernée. Ce RFC fournit un mécanisme, son usage n'est pas de son ressort. Ce journal n'empêchera donc pas l'émission de vrais/faux certificats, ni leur usage, mais il les rendra visibles plus facilement et sans doute plus vite.

Pour que cela fonctionne, il faudra que les clients TLS vérifient que le certificat présenté est bien dans le journal (autrement, le méchant n'aurait qu'à ne pas enregistrer son vrai/faux certificat, cf. section 5.4 du RFC).

En pratique, la réalisation de ce journal utilise un arbre de Merkle, une structure de données qui permet de mettre en œuvre un système où l'ajout de certificats est possible, mais pas leur retrait. La section 2 du RFC détaille l'utilisation de ces arbres et la cryptographie utilisée.

Le protocole utilisé entre les AC et le journal, comme celui utilisé entre les clients TLD et le journal, sera HTTP et le format des données sera JSON (section 4). Ainsi, pour ajouter un certificat nouvellement émis au journal géré sur `sunlight-log.example.net`, l'AC fera :

```
POST https://sunlight-log.example.net/ct/v1/add-chain
```

et le corps de la requête HTTP sera un tableau JSON de certificats encodés en Base64. La réponse contiendra notamment l'estampille temporelle (SCT pour "*Signed Certificate Timestamp*"). Pour récupérer des certificats, le programme de surveillance fera par exemple :

```
GET https://sunlight-log.example.net/ct/v1/get-entries
```

D'autres URL permettront de récupérer les condensats cryptographiques contenus dans l'arbre de Merkle, pour s'assurer qu'il est cohérent.

Notez que Google a produit une mise en œuvre <http://code.google.com/p/certificate-transparenc> de ce RFC, qui semble activement développée. Et il existe un pilote <https://www.imperialviolet.org/2013/08/01/ctpilot.html> écrit en Go. Il y a aussi une liste de diffusion <https://groups.google.com/group/certificate-transparency> sur ce projet et un site officiel du projet <http://www.certificate-transparency.org/> par Google. Sinon, si vous voulez en savoir plus sur cette idée de vérification publique, consultez « "*Efficient Data Structures for Tamper-Evident Logging*" <https://www.usenix.org/event/sec09/tech/full_papers/crosby.pdf> » de Scott A. Crosby et Dan S. Wallach. Autres lectures sur la "*certificate transparency*", un article de promotion <http://

queue.acm.org/detail.cfm?id=2668154> de Ben Laurie et un article violemment critique <http://blog.okturtles.com/2014/09/the-trouble-with-certificate-transparency/>.

Quelles sont les chances de succès de cette idée ? Tant que peu d'AC participent, ces journaux ne serviront pas à grand'chose (le méchant attaquera uniquement les AC non participantes). L'idée est qu'à moyen terme, la pression sur les AC (directement ou bien via les navigateurs Web qui ne feraient plus confiance aux AC non participantes) pourra faire que tous les certificats devront être dans le journal et que l'examen de celui-ci suffira à détecter les « vrais/faux certificats ».

Merci à Florian Maury pour sa relecture très détaillée.