

La NSA a t-elle une webcam dans votre salle de bains ?

Et autres questions sur l'espionnage high-tech

Stéphane Bortzmeyer
stephane+security@bortzmeyer.org

ESGI Security Day, 13 mars 2014

Introduction au problème

- 1 Jean-Kevin95 « Ouè, la NSA, on sait trop ky peuve lire dans les pensees, meme cryptees en RSA 65536 bits »
- 2 Edward Snowden « Faites confiance à la cryptographie »
- 3 Bruce Schneier « Faites confiance aux maths »

Peut-on avoir une idée des pouvoirs de la NSA ?

Avant Snowden

- 1 Beaucoup de spéculations
- 2 Des contre-mesures dont on ne savait pas si elles étaient efficaces (chiffrement, chapeau en alu)
- 3 Des discours rassurants « Ils sont gentils » « Ils n'ont pas les moyens de tout écouter, ne soyez pas paranos »
- 4 Des discours ironiques « Mais oui, c'est ça, la NSA lit vos courriers Gmail et des extra-terrestres reptiliens contrôlent secrètement le Vatican »

Après Snowden

- 1 Les paranos avaient raison. En fait, ils étaient même trop confiants.
- 2 Un très grand nombre de programmes d'espionnage portant des noms rigolos
<https://nsa-observer.laquadrature.net/>. Un énorme travail informatique.
- 3 Mais pas de percée fondamentale en physique ou en mathématiques.

Avertissement

- ① Une petite partie seulement des documents Snowden a été publiée. Plein de surprises à venir.
- ② Snowden n'était pas forcément au courant de tout. Des programmes très secrets peuvent ne pas être dans ses documents.
- ③ En crypto, on estime l'avance de la NSA à quelque part entre 10 et 30 ans (par rapport à la recherche publique),
- ④ De toute façon, nous savons tous que Snowden est un reptilien à figure humaine, membre des Illuminati, et qui essaie de nous tromper sur les vraies capacités du Gouvernement Mondial.

Tout cet exposé est donc assez spéculatif

Un exemple : PRISM

- ① Premier programme révélé par Snowden
- ② Google et Facebook permettent à la NSA d'accéder à leurs données
- ③ Purement passif
- ④ Basse technologie (et coût très faible)
- ⑤ Leçon : on sait depuis longtemps en sécurité que, si une des parties trahit, le chiffrement ne protège pas. Mais il y avait une \neq de point de vue : Alice et Bob croyaient parler entre eux, en fait chacun parlait à Google.

Autre exemple, QUANTUM et FOXACID

- 1 Le programme TAO est ciblé : les communications des cibles sont détournées par QUANTUM, puis envoyées à FOXACID qui tente de déposer un logiciel malveillant spécialisé dans la plate-forme de la victime.
- 2 QUANTUM est une attaque active (donc, par exemple, complètement illégale en France ; Hollande et Pellerin vont-ils porter plainte ?) par divers moyens (cela pourrait être le DNS mais les documents Snowden ne le disent pas)
- 3 Bien plus sophistiqué que PRISM
- 4 Mais faisable avec des moyens connus : c'est juste beaucoup de temps et de travail.

Monsieur Michu doit-il utiliser HTTPS ?

- 1 Monsieur Michu veut se connecter au site Web de l'EFF et ne veut pas qu'Obama le sache
- 2 `http://www.eff.org/` ou `https://www.eff.org/` ? Dans la presse, Monsieur Michu lit que « la NSA a cassé la crypto et peut lire les communications HTTPS »
- 3 Il demande aux plus grands experts en sécurité qui lui disent « euh, c'est compliqué »

Encore un nom de code rigolo

- ① En fait, la NSA ne casse pas la crypto, elle triche (programme BULLRUN),
- ② Machines infectées par FOXACID et qui trahissent,
- ③ Générateurs aléatoires trop prévisibles (petit coup de pouce de la NSA aux normes NIST), ← **le** problème de la crypto,
- ④ Vrais/faux certificats X.509 émis par les AC états-uniennes,
- ⑤ Logiciels *spyware* (Skype) ou avec portes dérobées (n'utilisez que du logiciel libre et, attention, c'est une condition nécessaire mais pas suffisante).

Normalisation

- ① Aujourd'hui, il n'y a guère de doute que la NSA avait affaibli délibérément le standard Dual_EC_DRBG.
- ② Le NIST, organisation gouvernementale fermée, était particulièrement vulnérable.
- ③ L'IETF ou le W3C, où tout se fait sous le regard de tous, sont-ils à l'abri de ces manipulations ?

Bogues ?

```
goto fail;  
goto fail;
```

- ① Deux cas fameux (Apple et GnuTLS) récents d'une bogue dans une bibliothèque TLS qui ignorait certaines vérifications
- ② Portes dérobées déguisées en bogues ?
- ③ Dans tous les cas, se rappeler que le logiciel contient des bogues. . .

Les progrès des maths

- ① La NSA peut casser RSA, vraiment ?
- ② En maths comme en informatique, il y a des progrès continus et prévisibles (qu'on peut accélérer en mettant des sous) et des percées imprévisibles (qui ne se pilotent pas).
- ③ RSA repose sur un problème difficile, la décomposition en facteurs premiers. D'autres algorithmes reposent sur le logarithme discret.
- ④ Malgré une recherche active, rien ne dit que le problème mathématique sous-jacent a été résolu. (Les vantardises des orateurs à Black Hat ou DEF CON ne comptent pas.)
- ⑤ Spécial parano : la NSA recommande officiellement les courbes elliptiques, plutôt que RSA. Avec la courbe P-256 normalisée par le NIST.

NSA contre chat de Schrödinger

- 1 Mais de toute façon, la NSA a des ordinateurs quantiques qui cassent une clé de 8 192 bits en vingt minutes, non ?
- 2 Les ordinateurs quantiques sont prometteurs depuis... quinze ans.
- 3 Les progrès sont très lents car la décohérence s'accélère vite avec le nombre de qubits
- 4 Avoir un ordinateur quantique qui puisse faire des calculs de taille réelle serait vraiment une percée ! Aujourd'hui, on se félicite d'avoir décomposé 143 en 11×13
<http://arxiv.org/abs/1111.3726v1>
- 5 Attention au bluff : l'ordinateur quantique est aussi un slogan commercial.
- 6 La NSA peut violer les lois des pays, pas les lois physiques.

En conclusion

- 1 Des pouvoirs énormes mais pas illimités, et pas connus en détail,
- 2 Et il y a d'autres attaquants, pas forcément aussi riches que la NSA,
- 3 Donc, il faut chiffrer ! Et appliquer les autres bonnes pratiques de sécurité (hygiène informatique, comme dit l'ANSSI) comme par exemple de ne pas utiliser Gmail et Google Drive
← **Vous, au fond, je vous ai vu !**