Chiffrement : faut-il mettre RSA en veilleuse ?

L'une des plus grandes caractéristiques d'Internet est qu'il évolue constamment à un rythme incroyable. Le temps ne se compte plus en décennies, voire en années, lorsqu'il s'agit du web. La voix amicale d'AOL qui nous accueillait en nous disant « vous avez du courrier » semble aujourd'hui être une relique ancienne. Personne n'a vu Jeeves depuis des années.

Alors pourquoi Internet continue-t-il à surcharger un système cryptographique qui a bientôt 45 ans ?

Au milieu des années 1970, alors que les informaticiens et les mathématiciens se précipitaient pour trouver un système de cryptographie à clé publique viable, deux systèmes sont apparus : Diffie-Hellman et RSA. Les équivalents Internet des Beatles et des Stones. Alors que Diffie-Hellman a tiré sa révérence comme les Beatles et a maintenant trouvé une nouvelle vie dans une nouvelle génération d'approches de courbes elliptiques qui s'en sont inspirées, RSA est comme les Stones, toujours en tournée bien au-delà de son apogée et pose la question suivante : « devrions-nous encore les laisser poursuivre ? ».

RSA n'est pas encore cassé, mais il est définitivement vulnérable. En fait, au cours des dernières années, un flux d'articles détaillant les moyens d'attaquer RSA a été publié à un rythme assez régulier. Pourtant, alors que nous discutons de concepts tels que la crypto-agilité et que nous nous lançons à pleine vitesse dans les cryptosystèmes post-quantiques, les entreprises et les organisations du monde entier continuent à surutiliser RSA dans leurs réseaux.

Il est temps de mettre RSA en veilleuse

RSA remplit actuellement deux fonctions très importantes sur Internet. Plus de 90% des connexions Internet commencent à utiliser RSA dans le cadre de la poignée de main (handshake) SSL. Il s'agit d'un point de contact critique où une attaque pourrait compromettre l'ensemble de la session, rendant toute communication entre le site web et le visiteur lisible et exploitable – pensez aux informations personnelles, aux données financières, aux dossiers médicaux, à la propriété intellectuelle, etc.

La deuxième fonction tout aussi importante est la création de signatures numériques cryptographiques. Nous utilisons ces signatures pour une multitude de choses, de l'authentification de courriels et de documents à la signature de mises à jour de logiciels et de micrologiciels. Lorsqu'un fichier ou un programme est signé numériquement, votre ordinateur et vos appareils mobiles sont conçus pour lui faire confiance. De toute évidence, il s'agirait là d'un autre point de contact potentiellement catastrophique où votre cryptosystème pourrait vous faire défaut.

Alors, quel est le problème avec RSA ? Il est double.

Commençons par la clé elle-même. Nous utilisons des clés plus longues et plus sûres pour des choses comme les signatures numériques et les « handshakes », car elles sont plus difficiles à

craquer. Une clé cryptographique, dans sa forme la plus basique, est juste une chaîne de 1 et de 0. La clé RSA moyenne est de 2048 bits, soit 2 048 1 et 0 dans une séquence. Craquer une clé signifie deviner sa valeur. Cela devient exponentiellement plus difficile à mesure que la clé s'allonge.

Les ordinateurs modernes et les techniques de chiffrement s'améliorant, les clés doivent nécessairement s'allonger pour maintenir leur sécurité. Un article technique publié en 2012, qui couvre une technique volontairement cachée appelée « triple factorisation logarithmique », a permis d'obtenir environ 6 millions de clés publiques et d'en craquer environ 13 000 en 13 heures de calcul. Cela représente moins de 99,8% de sécurité. Moquez-vous tant que vous voulez, mais ce n'est pas un chiffre acceptable.

Le problème avec RSA est qu'à mesure que ces clés s'allongent, l'augmentation de la sécurité n'est pas proportionnelle à l'augmentation de la puissance de calcul nécessaire pour les utiliser. Ce n'est tout simplement pas viable. Le CAB Forum vient de décréter que les clés utilisées pour la signature des logiciels doivent désormais avoir une longueur minimale de 3072 bits si vous utilisez RSA. Cette règle est valable pour le moment, mais nous atteindrons les limites dès que nous aurons atteint 4096.

Le deuxième problème avec RSA, au-delà des problèmes de mise à l'échelle, est la mise en œuvre passive. Afin de générer des clés, RSA utilise un générateur de nombres pseudo-aléatoires crypté et sécurisé (CSPRNG) pour créer des graines. Ces graines sont censées être aléatoires. Elles ne le sont pas. Elles utilisent des algorithmes, qui sont faillibles. En outre, de nombreuses organisations et entreprises utilisent les mêmes CSPRNG configurés de la même manière. Cela signifie que les clés RSA sont beaucoup moins aléatoires que ce que beaucoup d'entre nous aimeraient croire.

En fait, l'ensemencement RSA est l'un des endroits les plus faciles pour les forces de l'ordre ou un tiers malveillant pour insérer une porte dérobée. Si vous pouvez discerner les graines, le craquage des clés devient beaucoup plus facile. Maintenant, pensez au fait que des multinationales utilisent les mêmes CSPRNG, configurés de la même manière, utilisant les mêmes algorithmes et les mêmes gammes de nombres aléatoires, et la « bombe à retardement » commence à vous effleurer l'esprit.

RSA a été un incroyable système de cryptage, dont des éléments continueront à vivre dans des générations de futurs systèmes de chiffrement. Mais c'est aussi un dinosaure. Il est plus ancien que l'itération actuelle du World Wide Web lui-même. En tant que dirigeants d'entreprise dans le domaine de la sécurité, nous devons commencer à faire un effort concerté pour mettre fin à RSA et faire en sorte qu'il ne soit plus autant utilisé à mesure qu'Internet se rapproche de l'informatique quantique.

En fait, même si l'informatique quantique n'était pas juste à l'horizon, c'est déjà une discussion que nous aurions dû avoir il y a des années. Les systèmes à courbe elliptique et certains des autres systèmes de cryptographie qui sont mis au point en ce moment même offrent une plus grande sécurité tout en étant plus légers et plus agiles, ce qui signifie de meilleures performances en plus d'une meilleure sécurité.

Et cela signifie que le jour où l'informatique quantique sera enfin là, vous aurez déjà quelques longueurs d'avance sur la concurrence. RSA est déjà mort. Nous ne l'avons simplement pas encore accepté.

par Lila Kee, Chief Product Officer & GM Americas, GlobalSign.