NSI Terminale - Architecture

Sécurisation : Diffie-Hellman

Frédéric Bayart

2020/04/27

Le protocole d'échange de clés de Diffie et Hellman, inventé en 1976, est utilisé lors de l'appariement des appareils Bluetooth.

Protocole d'échange de clés de Diffie et Hellman

Parallèlement à leur découverte du principe de la cryptographie à clé publique, Diffie et Hellman ont proposé en 1976 un protocole d'échange de clés totalement sécurisé.

Le problème est le suivant : Alice et Bob veulent s'échanger un message crypté en utilisant un algorithme nécessitant une clé K.

Ils veulent s'échanger cette clé K, mais ils ne disposent pas de canal sécurisé pour cela. Le protocole d'échange de clés de Diffie et Hellman répond à ce problème lorsque K est un nombre entier. Il repose sur l'arithmétique modulaire, et sur le postulat suivant :

Étant donnés des entiers p, a, x, avec p premier et $1 \leq a \leq p-1$:

- **il est facile** de calculer l'entier $y = a^x \pmod p$.
- si on connait $y = a^x \pmod p$, a et p, il est **très difficile** de retrouver x, pourvu que p soit assez grand.

Retrouver x connaissant $a^x \pmod p$, a et p s'appelle résoudre le problème du *logarithme discret*.

Comme pour la factorisation d'entiers, c'est un problème pour lequel on ne dispose pas d'algorithme efficace.

Principe de l'échange de clé

Expliquons maintenant comment Alice et Bob peuvent s'échanger une clé secrète par le protocole de Diffie-Hellman.

Ils font des actions en parallèle, que l'on décrit dans le tableau suivant :

Étape	Alice	Bob
1	Alice et Bob choisissent ensemble un grand nombre premier p et un entier $1 \leq a \leq p-1$. Cet échange n'a pas besoin d'être sécurisé.	
2	Alice choisit secrètement x_1.	Bob choisit secrètement x_2.
3	Alice calcule $y_1 = a^{x_1} \pmod p$.	Bob calcule $y_2 = a^{x_2} \pmod p$.
4	Alice et Bob s'échangent les valeurs de y_1 et y_2. Cet échange n'a pas besoin d'être sécurisé.	
5	Alice calcule $y_2^{x_1} = (a^{x_2})^{x_1} = a^{x_1 x_2} \pmod p$ et appelle ce nombre K, la clé secrète à partager avec Bob.	Bob calcule $y_1^{x_2} = (a^{x_1})^{x_2} = a^{x_1 x_2} \pmod p$ et appelle ce nombre K, la clé secrète à partager avec Alice.

À la fin du protocole, Alice et Bob sont donc en possession d'une même clé secrète K, qu'ils ne se sont pas échangés directement.

Man in the middle

Que se passe-t-il si quelqu'un a espionné leurs conversations ?

Un espion connait p, a, y_1 et y_2.

- Il ne peut pas retrouver K comme le font Alice ou Bob, car il lui manque toujours l'une des informations nécessaires, à savoir x_1 ou x_2.
- Il ne peut pas retrouver x_1 connaissant $y = a^{x_1} \pmod p$, a et p, puisque la résolution du logarithme discret est un problème difficile.

Conclusion

Cette découverte de Diffie et Hellman est une vraie révolution dans l'histoire de la cryptographie.

Le problème de l'échange des clés est en effet résolu.

Ce protocole a cependant un défaut : il exige la simultanéité des actions d'Alice et de Bob.

Si Alice veut envoyer un e-mail à Bob alors que celui dort ou n'est simplement pas connecté, elle ne pourra pas le faire immédiatement.

C'est pourquoi ce protocole fut en réalité très vite supplanté par les méthodes de chiffrement à clé publique de type RSA, pour lesquels on met à la disposition de tout le monde une clé publique. Toutefois, il est utilisé pour les problèmes d'appariement de deux objets dans la technologie Bluetooth.