STEVEN MEYER

Co-Fondateur & Co-CEO

Comment les Rainbow Tables accélérées par GPU ont changé la sécurité des mots de passe

Juin 2024, Microsoft vient d'annoncer le retrait progressif de NTLM, un protocole de sécurité pour l'authentification des utilisateurs de Windows. Cette retraite est attendue depuis longtemps, car ce protocole ne fonctionne plus depuis plus d'une décennie. Laissez-moi vous raconter comment je suis devenu célèbre en rendant obsolètes les mots de passe Windows à 8 caractères.

Casser un mot de passe est une science en soi. Vous pouvez l'obtenir de quelqu'un par ingénierie sociale grâce à des attaques de phishing et de faux sites web, vous pouvez le voler à l'aide d'un enregistreur de frappe et d'outils de récupération de mot de passe (comme Mimikatz), vous pouvez essayer de le deviner en utilisant des informations personnelles, ou vous pouvez le déchiffrer.
Le principe d'un mot de passe est assez simple : l'utilisateur et l'appareil partagent un secret commun (le mot de passe) et lorsque l'utilisateur veut s'authentifier, il le saisit sur l'appareil. L'appareil compare les deux, et ce n'est que si le mot de passe est identique que l'accès est accordé. Au lieu de stocker les mots de passe réels, qui peuvent être volés, l'industrie utilise une technique appelée "hachage". Celle-ci convertit le mot de passe original en un ensemble unique de caractères (le hachage), qui est facile à vérifier mais difficile à inverser et à révéler.

Mes recherches ont porté sur la manière d'inverser et de révéler les mots de passe d'une manière très optimisée. Une option consiste à précalculer les 6 quadrillions de mots de passe à 8 caractères et leurs hachages. Il serait alors très facile de les déchiffrer en effectuant une simple recherche, mais cela nécessiterait 133 Po de stockage. Une autre solution consisterait à déchiffrer le mot de passe en temps réel, mais cela prendrait un mois pour chaque opération de déchiffrement.
La solution a consisté à utiliser les Rainbow Tables, une solution ingénieuse à ce problème, qui permet un compromis temps-mémoire. Nous calculons à l'avance les hachages de mots de passe potentiels, mais nous les stockons de manière à réduire considérablement l'espace et le temps de recherche nécessaires. Le résultat de la recherche a été la création d'une Rainbow Table avec des GPU NVIDIA Cuda pouvant être placée dans un disque SSD de 1 To, utiliser 4 Go de RAM et casser 99 % des mots de passe NTLM de 8 caractères en 23 secondes en moyenne.
Ce projet a non seulement poussé l'industrie à utiliser des mots de passe de plus de 8 caractères, mais aussi à ajouter de la substances dans les mots de passe et à promouvoir des algorithmes coûteux en mémoire et en temps ,tels que Bcrypt, pour le stockage sécurisé des mots de passe.

> "Mes recherches ont porté sur la manière d'inverser et de révéler les mots de passe.
>
> Steven MEYER
> Co-CEO de ZENDATA

Always in movement to protect

notre équipe.