Choisissez la meilleure authentification biométrique pour votre utilisation

La reconnaissance de la voix, du visage et des veines a chacune ses avantages et ses inconvénients.
Voici ce que les RSSI doivent savoir.

Evan Schuman ⋮

Grâce grandement à la consumérisation de la biométrie dans les cellulaires, la biométrie est devenue un moyen d'authentification peu coûteux et peu frictionnel.
Mais la biométrie varie considérablement en termes de précision et de commodité en fonction du type de biométrie et, surtout, des options de paramètres stricts ou indulgents.

Bon nombre des risques liés à la biométrie, tels que le stockage des données puis le vol des données lors d'une violation, ne sont pas un problème pour les entreprises, car elles utilisent massivement des fournisseurs tiers pour collecter et enregistrer les données. Néanmoins, si ce fournisseur biométrique tiers est violé et que les données d'authentification de l'entreprise se retrouvent sur le Dark Web, une partie du blâme finira par atterrir sur le bureau du RSSI.

Les enjeux sont également élevés pour les données biométriques.

« Écoutez, si mon mot de passe est volé, c'est une mauvaise journée, mais je peux en créer un nouveau et passer à autre chose », explique Rex Booth, RSSI de Sailpoint.
« Si mes données biométriques sont volées, c'est tout.
Je ne peux pas rafraîchir mes empreintes digitales ou développer une nouvelle rétine. Toute relation que j'ai avec un système dépendant de la biométrie à partir de ce jour est maintenant intrinsèquement précaire – fou la vie.

Pour sa part, Roger Grimes, évangéliste de la défense chez KnowBe4, soutient que la biométrie en général ne fonctionne pas bien.

« La plus grande idée fausse est que la biométrie est extrêmement précise », dit-il.
« Aucun des algorithmes ne se rapproche de ce qu'ils prétendent être.
Il y a énormément de faux matchs. »

Ainsi, il incombe à un RSSI d'examiner les avantages et les inconvénients de chaque mesure de sécurité, y compris la biométrie à mettre en œuvre et la manière de le faire efficacement.

La reconnaissance vocale a besoin d'une sauvegarde sérieuse

Le problème de cybersécurité le plus fondamental avec la biométrie est la précision par rapport à la facilité d'utilisation.
Malheureusement, les techniques biométriques les moins intrusives sont souvent les moins précises.

Une approche biométrique très populaire auprès du secteur financier est l'authentification vocale. Une équipe de chercheurs de l'Université de Waterloo a rapporté à la fin juin qu'elle avait « découvert une méthode d'attaque capable de contourner avec succès les systèmes de sécurité d'authentification vocale avec un taux de réussite allant jusqu'à 99% après seulement six essais ».
Le rapport de recherche complet a été présenté au symposium IEEE 2023 sur la sécurité et la confidentialité.

La méthode Waterloo « a identifié les marqueurs dans l'audio deepfake qui trahissent qu'elle est générée par ordinateur, et a écrit un programme qui supprime ces marqueurs, le rendant impossible à distinguer de l'audio authentique ».
Les chercheurs ont testé leur audio par rapport au système d'authentification vocale d'Amazon Connect, signalant un taux de réussite de 10 % en quatre secondes ; Le succès est passé à plus de 40% en 30 secondes.

« Avec certains des systèmes d'authentification vocale les moins sophistiqués ciblés, ils ont atteint un taux de réussite de 99% après six tentatives », indique le rapport.

La reconnaissance faciale dépasse les empreintes digitales

Mariona Campmany, directrice marketing de la société d'authentification Veridas, dit qu'elle préfère la reconnaissance faciale et la voix sur les empreintes digitales, pour plusieurs raisons.

« Premièrement, les lecteurs d'empreintes digitales sont plus facilement interopérables et susceptibles d'être extraites de données personnelles – ils n'offrent pas le niveau élevé de protection de la vie privée que la biométrie faciale et vocale offre », dit-elle.
« La capture d'empreintes digitales nécessite également des caméras à plus haute résolution ou un logiciel spécialisé par rapport aux appareils biométriques faciaux, ce qui les rend moins accessibles et universellement applicables. »

L'une des complexités d'une stratégie biométrique est qu'il existe deux types de précision. L'un est le type auquel Grimes faisait référence, qui examine la fréquence à laquelle le système identifie correctement l'utilisateur.
Mais la seconde concerne les frictions du système; Il s'agit du nombre de tentatives que l'utilisateur doit faire avant même que le système biométrique ne reconnaisse la tentative.

La reconnaissance faciale souffre de problèmes dans ce second domaine, étant donné qu'elle ne peut analyser qu'un visage qui se trouve à une distance précise de l'écran. Avec certaines implémentations de smartphones, les utilisateurs doivent parfois faire deux ou trois tentatives avant même que le système n'enregistre l'utilisateur.

La reconnaissance veineuse est coûteuse, mais sûre

Ant Allan, vice-président et analyste chez Gartner, affirme que son approche biométrique préférée est très populaire dans le secteur des soins de santé, mais qu'on le voit dans très peu d'autres secteurs verticaux: la reconnaissance veineuse.

« C'est une option plus coûteuse parce que vous avez besoin d'un équipement spécialisé de balayage et infrarouge, d'un équipement d'imagerie.
C'est souvent deux, trois ou quatre fois le prix des capteurs d'empreintes digitales », dit-il, ajoutant que la plupart des environnements de soins de santé limitent l'équipement à un petit nombre de postes de travail partagés pour réduire le coût.

Les RSSI ne devraient pas « se fier à la biométrie comme facteur unique, à l'exception peut-être des veines parce que [les modèles veineux] sont si difficiles à falsifier », dit Allan.

Comblez les lacunes grâce à la superposition

Certaines données biométriques sont meilleures que d'autres, à l'époque de Grimes.
« La voix est de loin la plus faible, puis la reconnaissance faciale.
La voix est assise dans sa propre classe pour sa faiblesse.
C'est si facile à simuler », souligne-t-il.

Grimes parle des problèmes de précision biométrique depuis des années.
À la fin de l'année dernière, il a souligné l'analyse de la précision biométrique du NIST, qui a révélé que la reconnaissance faciale et les empreintes digitales se rapprochent rarement de leur précision revendiquée.

« Si je vole votre téléphone, vos empreintes digitales partout sur votre téléphone », dit-il.

Et c’est là que réside un problème critique: les méthodes biométriques les plus faciles ont tendance à être moins précises, mais elles ont également tendance à être beaucoup moins coûteuses et, par conséquent, choisies plus souvent.

Une stratégie MFA solide est un bon moyen d’intégrer la biométrie, dit Allan de Gartner.

« L’utilisation d’un seul mode va vous donner quelques lacunes », note-t-il.
« Toute authentification est vulnérable.
Il n’y a pas de méthode qui soit à l’épreuve des balles. »

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230731
"C'est ensemble qu'on avance"