Les attaques de l'homme du milieu

De quoi s'agit-il et comment les éviter?

Août 2022

Lorsque nous utilisons Internet, nous nous attendons à ce que nos communications soient confidentielles et ne soient pas modifiées ni altérées en cours de transfert. Quand vous saisissez votre mot de passe pour la gestion de votre compte bancaire en ligne, vous partez du principe que: a) votre mot de passe correspond à celui que la banque possède, b) la banque reçoit le mot de passe sous sa forme correcte, et c) aucun tiers ne peut voir, modifier, falsifier ou réutiliser votre mot de passe. Il s'agit d'un exemple simplifié, mais, pour l'essentiel, les « attaques de l'homme du milieu » (HDM) fonctionnent en s'attaquant au deuxième ou au troisième de ces principes.

Une attaque HDM ne se contente pas nécessairement de perturber les communications entre humains, mais elle peut également affecter des interactions entre machines, qui sont vitales pour la fiabilité des produits connectés et services Internet. Par exemple, un appareil connecté, comme un assistant virtuel, partage généralement des informations avec un serveur central qui héberge les données.

Si vos connexions aux sites Internet et aux services en ligne ne sont pas fiables, vous pouvez être vulnérable à des risques de sécurité tels que la fraude, l'usurpation d'identité, les malwares, etc. Si vos appareils et objets connectés ne peuvent pas communiquer de manière sécurisée, ils peuvent vous exposer, ainsi que les membres de votre foyer, à des risques physiques.

Qu'est-ce qu'une attaque HDM?

Lors d'une attaque HDM, un tiers intercepte une communication entre utilisateurs (ou machines). Les attaques HDM se présentent généralement sous deux formes. La première est essentiellement l'écoute clandestine: une personne mal intentionnée surveille passivement une conversation ou lit le contenu d'un message; la seconde, une attaque « active », implique que la personne mal intentionnée change le contenu du message ou modifie autrement la communication (par ex. en envoyant un logiciel malveillant à la victime). La première attaque concerne la confidentialité de la communication, la seconde son intégrité. Bien que certaines attaques HDM soient effectuées à l'insu des fournisseurs d'accès aux services de communication, d'autres sont conçues au sein même de l'infrastructure des services de communication.

En 2013, des médias ont signalé[1] que certains gouvernements avaient mis en œuvre d'importants systèmes de collecte de données sur Internet avec des techniques de HDM. L'ajout de capacités HDM à des parties de l'infrastructure d'Internet, parfois avec l'aide des fournisseurs d'accès à Internet, a permis à des agences de sécurité nationale d'intercepter et de lire une partie du trafic sur Internet. Si la totalité du trafic était cryptée, il serait plus difficile pour ces agences d'accéder aux données. Après avoir appris l'existence de ces activités de surveillance, d'importants fournisseurs d'accès ont pris des mesures visant à crypter leurs services, en ajoutant un cryptage de bout en bout et en activant le cryptage par défaut.

Les attaques HDM sont une réelle menace pour Internet, quelle que soit l'entité qui y a recours. Les attaques HDM affaiblissent la confiance de l'utilisateur dans la confidentialité de ces communications durant leur transit. Les attaques HDM ébranlent donc la confiance qui accompagne les fonctions de base et la fiabilité d'Internet.[2]

Le cryptage aide à se prémunir contre les attaques HDM

Le cryptage est un moyen pour les individus de se protéger contre une attaque HDM. Il leur permet d'éviter que les données de leurs communications soient lues ou modifiées par des tiers. Par exemple, si vous envoyez un courriel non crypté, son contenu est visible par tout intermédiaire et nœud du réseau par lequel le trafic passe. Envoyer un courriel non crypté, c'est comme envoyer une carte postale: le facteur, le personnel du centre de tri et toutes les personnes ayant accès à la boîte aux lettres du destinataire peuvent, s'ils le souhaitent, en lire le contenu.[3]

Crypter le message protège sa confidentialité: il ne peut pas empêcher une personne mal intentionnée de visualiser le contenu, mais ce contenu sera incompréhensible, car le message aura été brouillé.

Utiliser le cryptage pour la signature numérique de données, d'un document ou d'une communication permet de s'assurer que, si un tiers parvient à modifier ces données, cette modification sera flagrante. Avec la plupart des algorithmes de cryptage, la modification du moindre élément du message initial engendre une version cryptée du message entièrement différente. Cette propriété peut servir à aider le destinataire à s'assurer que le message original n'a pas été altéré, de la même façon qu'un sceau sur une enveloppe.

Transport Layer Security 1.3 (TLS 1.3) est un important protocole de sécurisation d'Internet, qui assure une couche supplémentaire de protection face aux attaques HDM. TLS 1.3 rend la confidentialité de

1 https://www.amnesty.org/en/latest/news/2013/06/usa-revelations-about-government-surveillance-raise-red-flags/
2 https://datatracker.ietf.org/doc/rfc7258/
3 https://www.internetsociety.org/resources/doc/2018/encryption-brief/

transmission[4] obligatoire pour les sessions TLS. Cela garantit qu'une clé distincte est utilisée pour chaque session cryptée, ce qui signifie que le craquage d'une clé de session ne donne pas accès aux données cryptées des sessions précédentes, ni n'aide à découvrir les clés de session suivantes. Cela signifie qu'une personne mal intentionnée doit découvrir la clé de cryptage pour chaque session, ce qui augmente considérablement la difficulté des attaques HDM.

Les attaques HDM visant à accéder à des données cryptées

Plusieurs gouvernements dans le monde entier ont proposé ou mis en place diverses méthodes permettant d'obtenir l'accès à des communications ou à des appareils cryptés pour des motifs de sécurité nationale ou d'application des lois. L'une de ces méthodes est l'attaque HDM. Certains types d'attaques HDM - comme dans l'exemple ci-dessous - peuvent même saper la protection du secret de transmission de protocoles tels que TLS 1.3, car ils subvertissent potentiellement l'ensemble du mécanisme d'échange de clés sécurisé sur lequel repose le secret de transmission.

Exemple: une attaque HDM sur un trafic HTTPS

Selon Zdnet[5], en 2019, des utilisateurs des opérateurs de téléphonie mobile du Kazakhstan tentant d'accéder à Internet ont reçu des SMS leur indiquant qu'ils devaient installer les certificats racine attribués par le gouvernement sur leurs appareils mobiles et leurs ordinateurs. Le fait d'imposer aux utilisateurs l'installation de certificats racine appartenant au gouvernement peut donner à ce gouvernement la capacité d'intercepter le trafic HTTPS crypté et d'effectuer une attaque HDM pour accéder à des communications sécurisées. Cela signifie que le gouvernement peut voir, surveiller, enregistrer et même bloquer les interactions entre les utilisateurs kazakhs et tous les sites Internet, notamment les banques, les fournisseurs de messagerie, les réseaux sociaux, mais aussi des services publics essentiels, tels que l'électricité, les hôpitaux, les transports et les bureaux de vote. Une fois ces certificats installés, les utilisateurs n'ont aucun moyen de savoir si la sécurité de leurs communications est compromise. Les navigateurs afficheront toujours le symbole du cadenas ou un autre symbole pour indiquer que le trafic est « crypté et sécurisé », mais ce trafic, même s'il semble sécurisé, ne l'est pas. L'introduction de cette vulnérabilité compromet la sécurité de l'infrastructure mondiale à clé publique et érode la confiance dans les informations et les services accessibles via Internet.

Les attaques HDM ne se contentent pas de s'attaquer à la confidentialité et à l'intégrité; elles perturbent également l'accès à Internet. Par exemple, en 2012, la tentative d'attaque HDM par une

4 https://blogs.cisco.com/security/tls-1-3-and-forward-secrecy-count-us-in-and-heres-why

5 https://www.zdnet.com/article/kazakhstan-government-is-now-intercepting-all-https-traffic/

agence de sécurité en Syrie aurait détruit une partie essentielle de l'infrastructure d'Internet du pays, ce qui a privé la population syrienne d'accès à l'Internet mondial.[6]

Conclusion

Les gouvernements doivent s'abstenir de recourir à des attaques HDM pour permettre aux forces de l'ordre d'accéder à des communications privées. La création de moyens de ce type compromet la sécurité de tous les utilisateurs et nuit à l'infrastructure d'Internet. Les mêmes méthodes créées pour l'application de la loi peuvent être utilisées comme moyen d'attaque, à la fois par des utilisateurs autorisés et des tiers malveillants.7 Les attaques HDM présentent une menace réelle, non seulement pour la confiance des utilisateurs dans la confidentialité et l'intégrité des communications sur Internet, mais aussi pour la sécurité et la fiabilité d'Internet au niveau mondial.

Informations supplémentaires:

« Keys Under Doormats » – Rapport technique, MIT Computer Science and Artificial Intelligence Laboratory, 2015

6 https://www.wired.com/2014/08/edward-snowden/

7 https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal