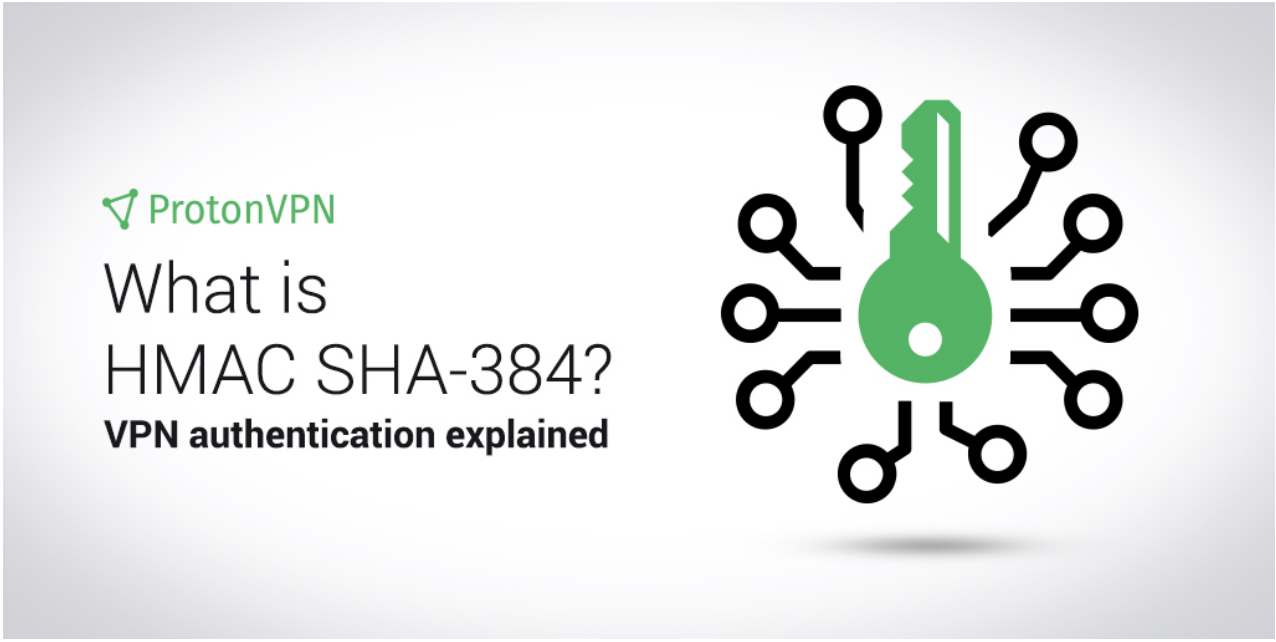
Co je HMAC SHA-384? Vysvětleno ověřování VPN

protonvpn.com/blog/hmac-authentication

Richie Kochem, Richie Koch

April 24, 2019



Vysvětlujeme, co znamená „HMAC SHA-384“ a jak přispívá k bezpečné VPN. Pokud uživatelé nechápou, co tyto technické termíny znamenají, nemohou učinit informované rozhodnutí.

Edit: Tento článek byl aktualizován, aby přesněji odrážel nabídky zabezpečení SHA-384 proti útokům typu length-extension.

Virtuální privátní sítě rády používají spoustu zkratek a technického žargonu k popisu své bezpečnosti. Jsme tím také vinni. Na naší stránce bezpečnostních funkcí zmiňujeme, že pro ověřování zpráv používáme HMAC SHA-384. Toto prohlášení vám poskytuje informace, které jsou nezbytné pro vyhodnocení toho, jak bezpečná je naše služba VPN, ale je k ničemu, pokud nevíte, co to znamená.

Stručně řečeno, HMAC SHA-384 je metoda, kterou Proton VPN používá k zajištění bezpečného cestování vašich zpráv mezi vaším zařízením a našimi servery VPN. Ověřuje, že provoz, který posíláme do vašeho zařízení, skutečně pochází z našich serverů a že s ním

nebylo po cestě manipulováno. Tím, že používáme HMAC SHA-384, říkáme, že si můžete být jisti, že jakmile se připojíte k jednomu z našich serverů, vaše připojení nemůže být narušeno ani podvrženo.

Ale jak to HMAC SHA-384 dělá? Pokud akronymy rozšíříte , **máte zakódovanou** zprávu **a ověřovací** kód **zabezpečený** hash **a algoritmus** 384bit . I když by to mohlo být přesnější, pro průměrného uživatele VPN to pravděpodobně není o nic užitečnější. Rozebereme to, jeden kus po druhém, počínaje „kódem pro ověření zprávy“.

Ověřovací kódy ověřují odesílatele

Nejprve rychlý základ o tom, jak funguje internetový provoz. Každý rozumí základním předpokladům připojení k internetu. Vaše zařízení (ať už je to počítač, mobilní telefon nebo chytrá televize) se připojí k vašemu poskytovateli internetových služeb, který vám pak pomůže připojit se k požadované webové stránce. Pokud jste náhodou připojeni ke škodlivému webu nebo pokud někdo zachytí vaše připojení, známý jako útok typu man-in-the-middle, mohl by sledovat vaše data nebo do vašeho zařízení vložit malware. Zjištění, že vaše připojení je s vaší zamýšlenou webovou stránkou, a ochrana tohoto připojení před neoprávněnou manipulací jsou zásadní pro používání internetu.

Ověřovací kód zprávy, neboli MAC, to dělá. Umožňuje příjemci dat vědět, že data, která obdržíte, jsou autentická (byla odeslána stranou, která tvrdí, že je odeslala) a nebyla s nimi manipulována (to je známo jako zachování „integrity“ dat).

Působivá práce s ohledem na MAC je o něco více než blok informací, obvykle dlouhý jen několik desítek bajtů. MAC je tvořena tajným klíčem a algoritmem podepisování MAC. Klíč je pouze parametr, který určuje výstup algoritmu. MAC funguje, protože je prakticky nemožné znovu vytvořit MAC zprávy bez znalosti tajného klíče. I

kdyby byl hacker schopen zachytit MAC adresy z předchozích zpráv, které uživatel odeslal, nepomohlo by mu to prolomit MAC další zprávy tohoto uživatele.

Nenechte se zmást slovem „zpráva“. Netýká se to e-mailů nebo textů, i když k jejich ověření lze použít i MAC a HMAC. Místo toho, když uvidíte zprávu, myslete na data, která se odesílají mezi vaším zařízením a webem (nebo službou VPN), ke kterému jste připojeni.

MAC je tedy jedním ze způsobů, jak ověřit, že připojení, které jste navázali s webem (nebo poskytovatelem VPN), je bezpečné.

SHA-384

Než vysvětlíme, jak funguje ověřovací kód hashované zprávy, musíte pochopit, co je to hash. Hašování je proces, který transformuje zprávu libovolné velikosti na pseudonáhodný řetězec znaků, který má pevnou délku. Tento řetězec znaků je známý jako hash. I když znějí podobně, hash se liší od šifrování v tom, že funguje pouze jedním směrem. Nikdy nemůžete „de-hash“ hash vrátit k původní zprávě. Protože to nelze vrátit zpět, je hašování bezpečným způsobem sdílení citlivých dat.

Hashe jsou také užitečné, protože vám umožňují potvrdit informace, aniž byste tyto informace odhalili. Jednoduchý případ použití, který to pomůže ilustrovat, je ukládání hesel. Společnosti potřebují mít kopii vašeho hesla k ověření vašeho účtu, ale mít heslo v prostém textu je bezpečnostní riziko. Uložením hashované kopie vašeho hesla společnost odstraní toto bezpečnostní riziko. Když se přihlásíte, společnost vytvoří hash hesla, které zadáte, a porovná ho s hashem, který má v záznamech. Pokud se shodují, pak byla hesla stejná. (Toto však není nejbezpečnější metoda ověřování. Proton Mail používá mnohem bezpečnější protokol Secure Remote Password, který pomáhá předcházet útokům typu man-in-the-middle.)

SHA-384 (neboli zabezpečený hashovací algoritmus) je jedna kryptografická hashovací funkce v rodině hash SHA-2 . Hashovací funkce je algoritmus, který vezme zprávu a vytvoří hash. 384 označuje délku hash vytvořeného algoritmem, což je 384 bitů (nebo 48 bajtů). Existují hashovací funkce, které produkují delší a kratší hashe. Používáme SHA-384, protože poskytuje optimální úroveň zabezpečení a efektivity. Chcete-li vidět, jak by zpráva vypadala, když je hašována pomocí SHA-384, klikněte sem . Je to jedna z nejsilnějších hašovacích funkcí, které jsou v současnosti k dispozici, a nabízí zvýšenou ochranu proti některým známým hašovacím zranitelnostem, včetně útoků na prodloužení délky a útoků na kolize , ve srovnání s jinými hašemi SHA-2.

Jak HMAC naváže zabezpečené připojení

Hašovaný ověřovací kód zprávy (HMAC) je způsob, jak přeměnit kryptografickou hashovací funkci na MAC. Použití hash přidává do MAC další vrstvu zabezpečení. V případě Proton VPN je kryptografická hashovací funkce SHA-384.

Zde je návod, jak funguje HMAC ve své nejjednodušší podobě. Nejprve se server i klient dohodnou na použití stejné kryptografické hašovací funkce (SHA-384) a vytvoří sdílený tajný klíč. Odesílatel poté zkombinuje sdílený tajný klíč s odesílanými daty a vytvoří kombinaci obou. Stejný sdílený tajný klíč a první hash jsou poté *znovu hašovány* , aby se získal druhý hash (to pomáhá předcházet určitým druhům útoků). Data a konečný hash jsou poté předány serveru.

Když klient obdrží hash a zprávu, spustí stejnou kombinaci zprávy a své vlastní verze sdíleného tajného klíče pomocí stejného algoritmu HMAC. Pokud se hodnoty hash shodují, dokazuje to, že server měl stejný tajný klíč, který „ověřuje“ data. To také ukazuje, že zpráva nebyla žádným způsobem změněna třetí stranou. Jakmile klient ověří, že se dva hash shodují, ví, že datům lze důvěřovat.

Pokud by se hodnoty hash neshodovaly, což by znamenalo, že buď server neměl stejný sdílený tajný klíč, nebo do dat došlo při přenosu dat, klient by data zahodil a věděl by, že jim nedůvěřuje.

Zde je důležité poznamenat, že HMAC data nešifruje, pouze ověřuje původ a integritu dat. Proton VPN používá AES-256 k šifrování vašich dat a uchovává je v soukromí, která jsou poté odeslána spolu s HMAC.

I když existují další alternativy ověřování zpráv a dokonce i další MAC, jako UMAC a OMAC, HMAC je jedním z nejbezpečnějších způsobů, jak ověřit odesílatele zprávy. Navíc se stal téměř všudypřítomným. Používá se v protokolech TLS a IPSec.

Toto je velmi základní vysvětlení toho, co je SHA-384 a jak funguje hašovaný ověřovací kód zprávy, ale doufáme, že vám pomůže lépe porozumět a vyhodnotit, co dělá VPN bezpečnou a zabezpečenou.

S pozdravem
tým Proton VPN

Můžete nás sledovat na sociálních sítích, abyste měli přehled o nejnovějších verzích Proton VPN:

Získejte zdarma šifrovaný e-mailový účet Proton Mail