HTTPS OVER OPEN WI-FI BLIJFT KWETSBAAR

Het is al langer bekend dat open Wi-Fi netwerken niet veilig zijn op het moment dat gegevens onversleuteld worden verzonden. Het open karakter van deze netwerken maakt het onderscheppen en manipuleren van data door aanvallers erg eenvoudig. Echter, veel internetgebruikers veronderstellen dat het gebruik van een versleutelde HTTPS-verbinding op een open Wi-Fi netwerk toch nog voldoende bescherming biedt tegen deze aanvallers. En dat is helaas niet waar…

Ir. Dennis Baaten is information security officer bij de ANWB en bereikbaar via dbaaten@anwb.nl

Computerapparatuur (laptops, tablets, telefoons) met een ingeschakelde Wi-Fi verbinding zoekt continu naar draadloze netwerken in de buurt. Vaak zijn deze apparaten ingesteld om automatisch verbinding te maken met bekende netwerken. Als er meerdere bekende netwerken in de buurt zijn, zal het apparaat het netwerk met het sterkste signaal selecteren. Heb je bijvoorbeeld vorige week verbinding gemaakt met het open Wi-Fi netwerk restaurant-wifi, dan zal je laptop ook op andere locaties naar dit netwerk zoeken om vervolgens automatisch te verbinden.

Een aanvaller kan dit mechanisme misbruiken voor het uitvoeren van een zogenaamde man-in-the-middle (MITM) aanval. Met behulp van speciale apparatuur (bijvoorbeeld de WiFi Pineapple t.w.v. $99) kan een aanvaller zich namelijk voordoen als een willekeurig Wi-Fi netwerk. De aanvaller vangt de zoeksignalen op van apparaten die zoeken naar bekende Wi-Fi netwerken. Wanneer het een zoeksignaal naar een open netwerk betreft, zal de aanvaller zich voordoen als het desbetreffende netwerk.

Het apparaat van het slachtoffer zal verbinding maken en denkt verbonden te zijn met het netwerk van het restaurant, terwijl er in werkelijkheid verbinding is gemaakt met het vervalste Wi-Fi netwerk van de aanvaller. Vanaf dat moment heeft de aanvaller de controle over de Wi-Fi verbinding tussen je laptop en het internet; de aanvaller is nu de man-in-the-middle.

Maar de aanvaller is nog niet klaar; alleen het onversleutelde (HTTP) verkeer is nu zichtbaar terwijl gevoelige gegevens vaak met behulp van versleutelde SSL-verbindingen (HTTPS) worden verstuurd. Het kraken van de sleutel van een SSL-verbinding is voor menig aanvaller onbegonnen werk, maar met behulp van speciale software (zoals SSL-strip) kan de aanvaller de browser van het slachtoffer forceren tot het gebruiken van een onversleutelde HTTP verbinding. Het gebruik van SSL tussen de aanvaller en het slachtoffer wordt daarmee omzeild, maar de verbinding tussen de aanvaller en de bestemming op internet blijft wel versleuteld met SSL. En dan is de aanvaller in staat om gevoelige gegevens te onderscheppen of te manipuleren alvorens deze hun beoogde bestemming op internet bereiken. Denk hierbij bijvoorbeeld aan het aanpassen van internetbankierentransacties of het onderscheppen van wachtwoorden.

Om het risico op misbruik te verlagen hebben veel website eigenaren maatregelen genomen of overwegen ze deze te nemen. Een populaire maatregel is het toepassen van de zogenaamde HSTS header die bij het bezoeken van een website door de server wordt mee gezonden naar de browser van de bezoeker. HSTS staat voor HTTP Strict Transport Security en zorgt ervoor dat browsers die dit ondersteunen gedurende de gespecificeerde periode (bijvoorbeeld een half jaar oftewel 15768000 seconden) uitsluitend een beveiligde verbinding opzetten met deze website. De browser zal dan geen onversleutelde HTTP-verbinding meer accepteren voor deze website.

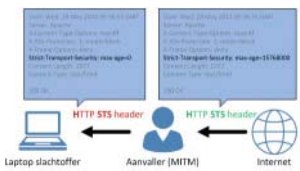
Op het moment van schrijven wordt het gebruik van deze header echter niet ondersteund door alle browsers. Zo heeft bijvoorbeeld nog geen enkele versie van Microsoft's browser Internet Explorer ondersteuning voor HSTS, waardoor deze browser zich ondanks het gebruik van een HSTS-header nog steeds laat forceren tot het gebruiken van een onversleutelde HTTP-verbinding.

Toch vormt HSTS bij de browsers die het wél ondersteunen geen waterdichte maatregel. Deze maatregel werkt namelijk pas wanneer het slachtoffer de desbetreffende website eerst via een ongecompromitteerde internetverbinding heeft bezocht; pas ná het verwerken van de HSTS-header weigert de browser

Maak geen verbinding met open Wi-Fi netwerken, maar gebruik altijd een Wi-Fi netwerk dat minimaal is beveiligd met WPA

onversleutelde verbindingen met de website. Hierdoor lukt het de aanvaller in een aantal specifieke gevallen nog steeds om, ondanks de aanwezigheid van een HSTS-header de browser van een slachtoffer te forceren tot het gebruiken van een onversleutelde HTTp-verbinding:

1. Bij een eerste bezoek aan een website zal de browser nog niet weten dat de desbetreffende website alleen over HTTPS benadert dient te worden. Als de aanvaller de browser dan forceert tot het gebruiken van HTTP, en vervolgens ook nog in staat is om de HSTS-header te verwijderen of te veranderen naar nul (0) voordat deze bij de browser aankomt, dan kan de aanvaller zijn MITM blijven handhaven.



2. De browser slaat de HSTS waarde op in de browsergeschiedenis. Wanneer de browsergeschiedenis wordt gewist of wanneer de browser wordt gestart in de privé of incognito modus, dan zal de browser bij de eerstvolgende keer starten niet weten dat de desbetreffende website uitsluitend via HTTPS dient te worden benaderd. Voor de browser is de situatie dan namelijk gelijk aan het hierboven beschreven "eerste bezoek".

3. Na het verlopen van de HSTS-waarde (bijvoorbeeld na een half jaar) zal de browser bij de eerstvolgende keer opstarten ook weer in een situatie zitten die gelijk is aan het "eerste bezoek".

Kortom, als het nemen van maatregelen beperkt blijft tot het gebruik van een HSTS-header in combinatie met een browser die dit ondersteunt, is misbruik door een aanvaller tijdens het gebruiken van een open Wi-Fi netwerk niet uit te sluiten. Het risico is wel flink afgenomen, maar is niet nihil. Om het risico nog verder te verlagen kunnen aanvullende maatregelen worden genomen:

a. Verwijder alle Wi-Fi netwerken eenmalig uit je apparaat en begin opnieuw. Wen jezelf aan om vanaf dat moment alleen nog maar beveiligde netwerken op te slaan, zodat je apparaat niet meer automatisch zal proberen te verbinden naar open Wi-Fi netwerken.

b. Stel je apparaat bij voorkeur zo in, zodat deze niet automatisch verbinding maakt met bekende Wi-Fi netwerken. Smartphone gebruikers kunnen eventueel gebruik maken van apps (zoals bijvoorbeeld Wi-Fi Matic) die je Wi-Fi verbinding automatisch in- of uitschakelt afhankelijk van je locatie.

c. Maak geen verbinding met open Wi-Fi netwerken, maar gebruik altijd een Wi-Fi netwerk dat minimaal is beveiligd met WPA. De beveiligingsprotocollen WPA en WPA2 kennen namelijk een zogenaamde four-way handshake waarmee er op basis van het wachtwoord en de SSID een unieke sessie-sleutel per Wi-Fi gebruiker wordt gegenereerd. Dit is momenteel voor een aanvaller erg moeilijk te misbruiken, ook wanneer het wachtwoord bij de aanvaller bekend is. In het laatste geval is misbruik alleen mogelijk wanneer een aanvaller bewust een vervalst access point opzet met hetzelfde SSID en wachtwoord.

Wanneer een of meerdere van deze aanvullende maatregelen worden ingezet in combinatie met HSTS en een browser die hier ondersteuning voor biedt, dan wordt het aanvallers knap lastig gemaakt om een man-in-the-middle aanval op een open Wi-Fi netwerk uit te voeren. Voorlopig is het risico dan in de meeste gevallen acceptabel, totdat aanvallers weer nieuwe trucs uit de hoge hoed toveren.