WPA2 enterprise niet OK voor gastnetwerken

Geert Jan de Groot

Bezorgd lurker

Context

Dit document vormt een reactie op de internet-consultatie: *Open standaard WPA2 Enterprise* (https://www.internetconsultatie.nl/wpa2enterprise).

Eerste reactie

Toevallig ontdekte ik deze consultatie en heb het voorstel met verwondering gelezen. Mijn conclusie is dat in het document implementatie-ervaring lijkt te ontbreken. Ik heb ruim 8 jaar ervaring met het aanbieden van een WPA2-enterprise netwerk voor een jeugdinstelling (waar we graag de gebruikers individueel toegang willen kunnen geven omdat we een leeftijdsgrens hanteren; jeugd moet bezig zijn met “buiten” en niet met “internet”) en gebaseerd op deze ervaringen mis ik een aantal aspecten in het voorstel, aspecten die dit wellicht een wat minder gelukkig voorstel maken.

WPA2-enterprise is een prima oplossing bij een “enterprise”, dat is, een verzameling computers, netwerkapparatuur en infrastructuur die door dezelfde organisatie worden beheerd. Diverse leveranciers hebben kant-en-klare oplossingen waar je met “group policy” de boel in kunt richten omdat je controle hebt over alle componenten in het netwerk.

WPA2-enterprise is ook een goede oplossing voor confederaties, dat wil zeggen gerelateerde organisaties die onderling uitwisselen. Een goed voorbeeld daarvan is Eduroam en afgeleiden, zoals Govroam. Dit veilig inrichten is al ingewikkelder, ik ga hier verder op in.

Het voorstel behelst echter “*gebruik van WPA2-enterprise voor gast-toegang*”. In dit geval is er niet noodzakelijk een organisatorische relatie en dan wordt ‘t ingewikkeld.

Bij gebruik van WPA2-enterprise wordt er geauthenticeerd tegen een RADIUS server. De verbinding is versleuteld waarbij voor de versleuteling gebruik gemaakt wordt van TLS-certificaten. En hier zit het grote probleem met dit voorstel.

Authenticatievormen

Bij WPA-enterprise kan op diverse manieren worden geauthenticeerd, waaronder:

- Username/password
- Client certificaat
- Hardware token

Bij enterprise oplossingen wordt vaak gebruik gemaakt van client certificaat oplossingen. Als je de hele infrastructuur controleert kan dat ook. Bij gastgebruik is de controle van het client certificaat een stuk ingewikkelder (hoe controleer je het certificaat?).

Daarom wordt als de gebruiker en netwerk verschillende beheerders hebben, vaak gebruik gemaakt van Username/password. Een voorbeeld daarvan is Eduroam.
Een probleem daarbij is dat de username/password ook voor andere authenticatie gebruikt worden en dus niet uit mogen lekken.

SSL certificaten

Om het authenticatieproces af te schermen, wordt voor de communicatie tussen client en RADIUS server gebruik gemaakt van TLS met een certificaat. En daar zit het probleem met WPA2-enterprise bij gastgebruik:

- Het te gebruiken certificaat moet betrokken worden bij een “officiële CA”, waarbij bijvoorbeeld Windows een whitelist van toegestane CA’s heeft. Een certificaat van bijvoorbeeld *Lets Encrypt* wordt niet geaccepteerd.
- De CA’s op deze lijst zijn commerciële bedrijven die geld vragen voor het certificaat. Dit werkt kostenverhogend (in mijn netwerk is dit kostenaspect een no-no).
  Bij een enterprise-implementatie wordt veelal het certificaat van de domain controller gebruikt en heb je dit probleem niet, maar bij gastgebruik wel.
- Het is (soms) mogelijk om de “certificaat controle” uit te schakelen, waardoor een certificaat van een CA die niet op de whitelist staat, toegestaan wordt. Hiermee wordt o.a. ook een self-signed certificaat mogelijk (en is de door mij gekozen oplossing). Maar, dit vereist een aantal administratieve handelingen op ieder apparaat die boven de kunde van de eindgebruiker gaan.
- Voor deze handelingen is vaak beheer-rechten nodig. Bij apparaten die door een andere organisatie beheerd worden, heeft de eindgebruiker dit vaak niet, en daardoor kan zo’n certificaat niet “werkend gemaakt worden” waarmee gastgebruik onmogelijk geworden is! Tegen dit probleem liep ik aan toen ik een iPhone toegang wilde geven die MDM-managed was bij een school: certificaat toevoegen kon niet (meer)
- De standaard enrollment (met een gewhite-list-CA) vraagt alleen om de username/password en controleert de rest van het certificaat niet (zolang het CA maar een whitelist-CA is). Als een gebruiker dus authenticeert, maar verbinding maakt met een andere server die ook een whitelist-certificaat gebruikt, zal de verbinding slagen: de gebruiker ziet geen verschil tussen de radius-server radius.example.org en de radius-server radius.evil.net, mits het laatste certificaat ook van een “goede CA” is. De CN van het certificaat hoort veelal niet bij de inlog-instructie en wordt niet gecontroleerd tenzij dit expliciet is ingesteld.
  MITM aanvallen zijn hierdoor nog steeds mogelijk, voor een aanvaller is het niet zo moeilijk om een goed certificaat te krijgen en hiermee worden username/password bekend. (Dit is een argument om een self-signed certificaat te gebruiken, mits dit gecontroleerd wordt; op een gastnetwerk is dit natuurlijk een probleem)
- De controle op certificaat-wisselen ligt bij de eindgebruiker. Dat is niet veilig!

- Bij gebruik van een confederatie, en mits de thuis-organisaties de kosten van een whilelist-CA betalen, zijn een aantal problemen ondervangen, **mits** de gebruikers correct worden geinstrueerd (controle van CA, controle van CN).
  Het probleem van gastgebruik is echter dat er wellicht geen confederatie-relatie is (hoe logt iemand met GovRoam credentials in op een Eduroam netwerk?)

Andere overwegingen

Bij de bezwaren van dit voorstel zijn behalve de certificaat-problemen, nog andere issues:

- De vraag is hoelang Wifi-gastgebruik relevant is. Wifi gastgebruik wordt, behalve het verlenen van toegang, ook gebruikt voor het ontlasten van een mobiel-internet abonnement, zeker een issue als mobiele data kostbaar is.
  Maar ik heb bij problemen in ons netwerk ook de reactie “geeft niet, ik gebruik wel m’n mobiel, ik heb 20GB data per maand en die maak ik niet op….” gehad. Dit zal met nieuwere technologie alleen maar beter worden.
- Het gebruik van een “veilig Wifi netwerk” geeft een vals gevoel van veiligheid. Netwerk-verkeer kan verderop in het netwerk alsnog onderschept worden. De oplossing hiervoor is volledig end-to-end versleutelen van het netwerkverkeer. Doe je dat, dan is de noodzaak van een “veilig Wifi netwerk” veel minder.

Conclusie

- Aan het gebruik van WPA2-enterprise voor gast-toegang kleven nadelen, met name vanwege de noodzaak tot het gebruik van certificaten.
- De eis tot het gebruik van commerciële CA’s die op een whitelist staan, is een probleem. Een grote organisatie kan de kosten mogelijk wegwuiven, maar het is natuurlijk helemaal de verkeerde situatie. Bovendien geeft dit een vals gevoel van veiligheid daar het certificaat niet volledig gecontroleerd wordt.
- Het gebruik van WPA2-enterprise wanneer er geen organisatorische relatie is tussen gastheer en gast, levert problemen op. Zeker voor gasten die geen beheer-toegang hebben op hun randapparatuur kan dit ervoor zorgen dat gast-toegang niet mogelijk is.
- Voor gebruik waar wel een organisatorische relatie bestaat, is WPA2-enterprise een goede oplossing; het succes van Eduroam is een goede demonstratie daarvan. Maar, dat succes geldt alleen als er een relatie bestaat en die relatie is er niet bij alle “gastgebruik”.
- Het gebruik van WPA2-enterprise is geen vervanging van het gebruik van volledig end2end versleutelde verbindingen.

Mijn conclusie moet daarom zijn dat **het voorstel tot het verplichten van WPA2-enterprise voor gastgebruik, heroverwogen moet worden** en dat WPA2-enterprise in deze situatie wellicht niet de meest geschikte oplossing is.