HOE VEILIG ZIJN DRAADLOZE NETWERKEN NU ÉCHT?

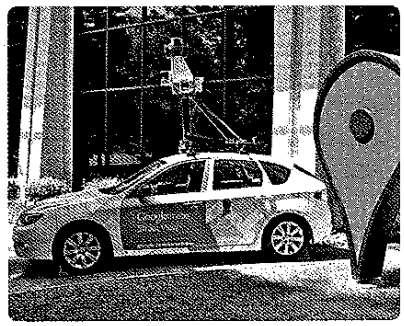
12 jaar geleden onderzochten Better Access en Data News voor de eerste keer de beveiliging van draadloze netwerken, die je toen overal zag opduiken. Is de situatie nu verbeterd?

Met een oude laptop, externe antenne, een gps en wat software gingen we twaalf jaar geleden *wardriven* en maakten we een inventaris van welke netwerken we konden vinden en of en hoe ze beveiligd waren.

De resultaten waren verbluffend: van de 263 draadloze netwerken die we konden vinden in en rond Leuven, was amper 15% beveiligd. Al de rest stond wagenwijd open om misbruikt te worden zonder enige vorm van beveiliging. Overal in Europa waar we de test opnieuw uitvoerden kregen we ongeveer dezelfde resultaten. De lijst van organisaties die het niet zo nauw namen met de beveiliging van hun wireless netwerk bevatte opvallende namen zoals politiediensten, gerenommeerde advocatenkantoren, banken en zelfs een grote lokale brouwerij.

De netwerken die beveiligd waren, deden dit meestal nog met het 'wired equivalent privacy' (wep) protocol. In een systeem waarvan de FBI, in navolging van vele hackers met witte of zwarte hoed, al in 2005 aantoonde dat het in minuten te kraken valt en waar vandaag de dag tientallen programmaatjes voor te vinden zijn die dit zelfs voor niet-technische surfers mogelijk maakt. Het is dan ook geen goed idee om nog wep te gebruiken. Trouwens, veel van die dingen waren bovendien slecht geconfigureerd met een triviaal of het standaard wachtwoord waarmee het wireless access point geleverd werd.

Geen wonder dan ook dat wardriving in de jaren nadien zowat de nationale sport werd voor nerds zonder sociaal leven, die enkel buitenkwamen om op zoek te gaan naar nieuwe draadloze netwerken. Maar

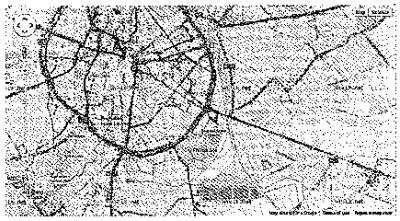


Wardriving Google style

ook Google bouwde wardriving-technologie in zijn Streetview-wagens waarmee ze de informatie van alle draadloze netwerken die ze tegenkomen inventariseerden.

Een decennium later

Vandaag de dag is er veel veranderd, wifi is explosief gegroeid. Waar je in 2002 moeite moest doen om een paar honderd draadloze netwerken te vinden, zie ik vandaag op mijn bureau in Leuven zonder extra antenne 58 draadloze netwerken van



Alle draadloze netwerken in Leuven, gebaseerd op Wigle.

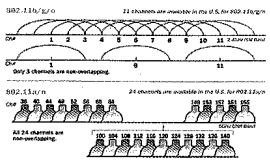
allerlei pluimage en met vaak humoristisch gekozen netwerknamen.

Een online community als Wigle (https://wigle.net) die de resultaten van grote groepen wardrivers online verzamelt en analyseert, heeft in zijn database meer dan 134 miljoen draadloze netwerken zitten. Deze collectie van netwerken kan je in onvervalste big data stijl gebruiken om het draadloze spectrum te analyseren dat door 802.11-netwerken is ingenomen. Of gebruik het om te zien of wardrivers jouw draadloze infrastructuur al opgemerkt hebben.

Beperkt door de wetten van de natuur

De reden waarom 2,4 Ghz en in mindere mate 5 Ghz draadloze netwerken zoveel succes hebben, is doordat beide banden vrij te gebruiken zijn; je hoeft er dus geen specifieke licentie voor aan te vragen. Daarnaast zijn de chipsets voor draadloos zo goedkoop geworden dat het voor

alles en nog wat gebruikt wordt. Voor voor de hand liggende 802.11 wifi-netwerken zoals smartphones, tablets en laptops, maar ook voor draadloze telefoons, toetsenborden, wimax, enzovoort. Onverwachte dingen als babyfoons, draadloze microfoons en bewakingscamera's

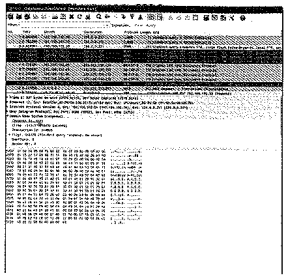


Het draadloze spectrum uitgelegd.

gebruiken vaak deze frequentie. En als dat nog niet genoeg is kan je op die band ook nog gestoord worden door microgolfovens en zelfs door slechte elektrische bekabeling.
2,4 Ghz heeft bovendien slechts 13 kanalen die je kan gebruiken, die mekaar bovendien gedeeltelijk overlappen. In feite zijn er maar drie (kanaal 1, 6 en 11) die mekaar niet overlappen. Het spectrum op een locatie zit dan ook heel snel vol en gezien het een vrije band is, kan iedereen in je buurt een toestel inpluggen dat dezelfde kanalen als jouw infrastructuur gebruikt met alle gevolgen van dien. Een 2,4 Ghz netwerk bewust of onbewust platleggen is dan ook meestal een koud kunstje.
Om dit tegen te gaan, schakelt iedereen voor echte productiedoeleinden zoveel mogelijk over naar de 5 Ghz band. Hier heb je in totaal 24 kanalen ter beschikking waardoor er meer ruimte is om te schipperen tussen de verschillende kanalen. Alleen wil iedereen steeds meer bandbreedte tot 1 Gbit over draadloos trekken en om dit mogelijk te maken wil men bredere kanalen gaan gebruiken tot 160 Mhz. Het resultaat is dat je wel 1 Gbit zal halen over je 802.11ac-netwerk maar dat in het 5 Ghz spectrum opnieuw slechts 3 kanalen mekaar niet overlappen.
De stortvloed aan draadloze toestellen heeft de industrie heel sterk veranderd. Vandaag heeft een ietwat zichzelf respecterende digitale burger twee of zelfs drie draadloze toestellen bij zich die hij liefst zoveel mogelijk via wifi permanent verbonden heeft met het internet. Draadloze internettoegang wordt tegenwoordig zowat aanzien als een fundamenteel mensenrecht.
Alleen biedt dit wel een grote uitdaging voor mensen die bijvoorbeeld draadloze infrastructuur gaan bouwen in hotels, voetbalstadia en andere locaties waar veel draadloos volk zich verzamelt.
Het resultaat is dat draadloze netwerken helemaal anders gebouwd worden: vroeger probeerde je met veel kunst-, vlieg- en ander antennewerk zoveel mogelijk oppervlakte te bestrijken met één AP. Alleen kan zo'n AP maar een beperkt aantal gebruikers aan. Als je dan 30.000 devices in één stadion wireless toegang wil geven dan wordt dit heel moeilijk. Vandaar dat men tegenwoordig meerdere AP's gebruikt, die liefst een zo klein mogelijke zone bestrijken om de verschillende AP's elkaar zo weinig mogelijk te laten storen.

Risico's voor de draadloze gebruiker

Ondertussen gebruikt iedereen elke hotspot die hij of zij kan vinden om er zijn telefoon, tablet of laptop mee te verbinden en zo toegang te krijgen tot het internet. Haast niemand stelt de vraag of dit allemaal wel zo risicoloos en veilig is.
Een draadloos netwerk is immers een gedeeld netwerk, dit wil zeggen dat alle toestellen die met hetzelfde netwerk of ssid verbonden zijn, mekaar 'zien' en met de juiste software elkaars netwerkverkeer kunnen afluisteren of 'sniffen'.
De industrie heeft om dit tegen te gaan een oplossing genaamd wireless isolation of client isolation ingevoerd, waarbij dit onmogelijk gemaakt wordt. Alleen staat die feature verre van overal aan en niemand doet de moeite om te controleren of dit al dan niet het geval is.
Een praktisch voorbeeld: op de Thalys naar Parijs wordt tot grote appreciatie van de passagiers draadloos internet aangeboden. Alleen, wanneer je een sniffer zoals Wireshark of Tcpdump opstart,



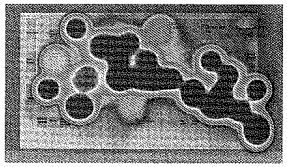
En er zit een pastoor op de trein met zijn laptop...

merk je dat je het netwerkverkeer van alle andere passagiers die op dezelfde AP verbonden zijn, kan lezen. Geen client isolation dus en als je je verveelt kan je de andere passagiers gaan analyseren. Wat kan je allemaal zien/doen?
De naam van het toestel wordt door de meeste Apple- en Microsoftsystemen continu het netwerk opgestuurd. Zo zit ik op dezelfde trein met o.a. de Windows-laptop van een priester (FatherBryan), de iPhones van Raoul en Ramon, de iPads van Mohammed en Thierry, de Macbook Pro van Giacinto en Jean-Francois-Ravagnan, de iPod van Anke en een Toshiba Tecra laptop die Windows 7 draait.
De reden hiervoor is vooral het feit dat het toestel zich via dns probeert kenbaar te maken aan de buitenwereld. Bovendien gaan alle processen die normaal binnen het interne netwerk gebruikt worden, ook via wireless proberen verbinding te leggen. Zo weet ik bijvoorbeeld dat Jean-Francois in zijn interne netwerk een Ricoh-printer heeft, hoe de interne file-

en Exchangeserver heet en nog wat potentieel interessante info over het bedrijf waar hij werkt.
Maar het gaat verder dan dat: ik zie ook alle netwerkverkeer die ze doorsturen en luister die af. In zoverre die op een correcte manier versleuteld is, kan ik er weinig mee doen, maar dit betekent dat je volledig afhankelijk bent van de encryptiestandaarden van de gebruiker. Als je een onveilige encryptie gebruikt met bijvoorbeeld een zelf ondertekend, niet door een vertrouwde derde partij uitgegeven certificaat wordt het mogelijk om een zogenaamde *man-in-the-middle attack* uit te voeren waarbij je de client probeert zo ver te krijgen om jouw certificaat in plaats van dat van de server te gebruiken, om het verkeer dat hij uitstuurt te versleutelen. Op die manier kan een aanvaller meelezen zonder dat je het eigenlijk merkt.
Ook als producenten als Apple bugs in hun ssl-software hebben zoals die recent boven kwam of wanneer sociale netwerken als Facebook, Twitter en LinkedIn op een onveilige manier werken, kunnen ze overgenomen worden door potentiële hackers (Droidsheep-verhaal uit 2012.)
Ook alle apps die je op je telefoon of je tablet gebruikt, kunnen beter veilig communiceren.
Een pc die een tcp/3389, fileshare of een webserver openstaan heeft, kan op die manier potentieel gehackt worden. Documenten die op deze shares staan kunnen dan bekeken worden. En dit gebeurt meer dan je denkt: even iets delen met iemand op het interne netwerk en het nadien vergeten uit te schakelen is al voldoende.
Kortom: als gebruiker van een draadloos netwerk loop je wel degelijk risico. Zorg er dus voor dat je een degelijke firewall op je pc/laptop staan hebt en er geen diensten naar buiten draaien die niet strikt noodzakelijk zijn. Zorg ook dat alles wat je gebruikt over de draadloze verbinding volgens de regels van de kunst beveiligd en dus versleuteld wordt. Wie echt paranoïde is - zoals ik - kan alle verkeer over een beveiligde vpn-tunnel naar zijn datacenter sturen. Op die manier ziet de aanvaller enkel een vpn-tunnel en alle verkeer gaat daar beveiligd door.

Privacy

Vaak wordt ook vergeten dat een toestel dat zijn draadloos netwerk permanent aanstaan heeft, ook heel wat privé-gegevens van u kan lekken. Uw draadloze toestel heeft immers een uniek mac-adres dat altijd gebruikt wordt om draadloos te kunnen communiceren. Wanneer je draadloos toestel op zoek is naar een netwerk, stuur je permanent dat mac-adres



Hoe de bezoekers op Interop in Las Vegas rondliepen, gebaseerd op hun wireless toestel en Ruckus Spot technologie.

door en kan het door AP's in de buurt opgevangen worden. Op die manier kan de eigenaar van het AP weten dat jij in de buurt bent geweest. Heeft hij twee AP's en een beetje software, dan kan hij bij benadering gaan bepalen waar jij (of toch tenminste je toestel) exact stond en gewandeld hebt. En om dit te doen hoef je niet eens verbonden te zijn met dat netwerk; je toestel dat zoekt naar een netwerk is voldoende.
Wanneer ik jou als gebruiker zover krijg om je identiteit te geven door jou bijvoorbeeld gratis internet ter beschikking te stellen als je je authentificeert met bijvoorbeeld Facebook - zoals dit steeds meer gebeurt - kan ik aan het mac-adres ook een persoon koppelen en weet ik vanaf dan dat jij mijn AP voorbij wandelt.
De toepassingen hiervan zijn duidelijk. Ruckus biedt met Spot (Smart Positioning Technology) bijvoorbeeld een oplossing aan waarbij het op basis van de draadloze toestellen mogelijk is om te zien waar de klanten in de winkel geweest zijn en hoeveel tijd ze er door gebracht hebben. Dit is interessante informatie om het succes van hotspots (in dit geval de belangrijkste plaatsen in de winkel, bijvoorbeeld aan de kassa) en de campagnes die je daar voert te bestuderen - zeker als je ook aan het mac-adres een persoon kan koppelen of zelfs een getrouwheidskaart. Je kan hier heel ver in gaan. Waarom geen auto met AP voor de deur van je concurrenten parkeren en zien welke klanten daar gaan winkelen?

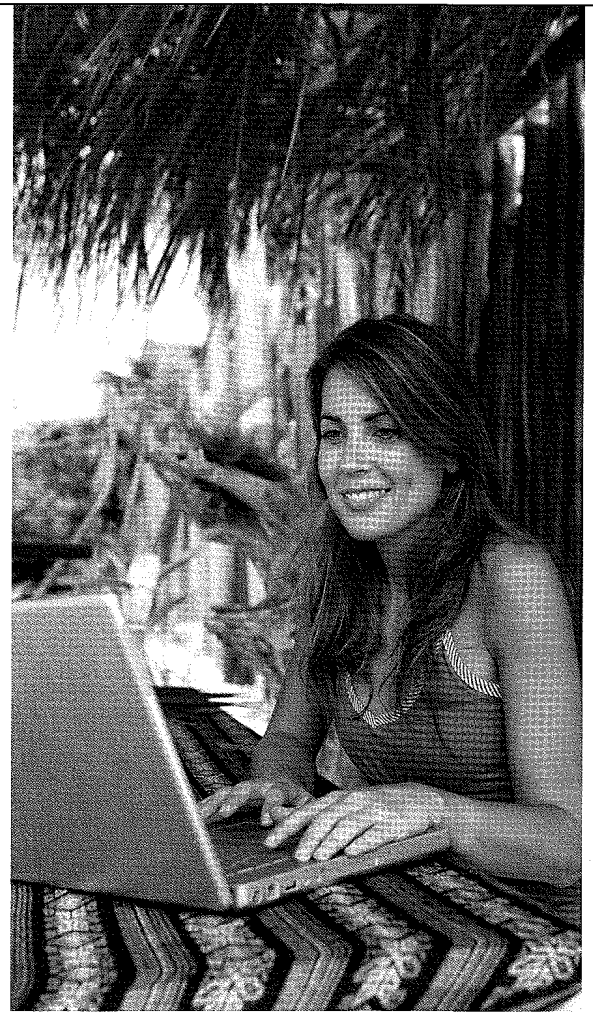
Veilige wireless infrastructuur voor je organisatie?

Binnen het bedrijfsleven is de druk zeer groot om alle draadloze toestellen van de medewerkers met het interne netwerk te verbinden. Het is dan ook heel moeilijk om een bedrijfsnetwerk zonder draadloze infrastructuur te gaan opbouwen. Maar hoe pak je dit het best aan?
Allereerst moet je altijd onthouden dat niet alle type gebruikers gelijk zijn: er zijn externe gebruikers die enkel toegang tot een internetverbinding nodig hebben, externe contractanten of consultants die je een beperkte toegang tot bepaalde interne diensten wil geven en er zijn de interne gebruikers waar je ook nog de nodige beperkingen kan gaan invoeren van waar ze precies allemaal naartoe moeten.
De sleutel tot deze opdeling ligt in het interne lan en een duidelijke opdeling daar. Wireless moet naadloos hiermee geïntegreerd worden. Zorg er dus voor dat er een goede opdeling is o.a. door de juiste vlan's te definiëren en ze op de juiste manier te isoleren met access control list of firewalling. Het valt geregeld voor bij audits dat je met een beetje kunst- en vliegwerk van de publieke wifi ook op het in-

terne netwerk geraakt omdat men de firewalling verkeerd of helemaal niet heeft ingesteld. Dus zorg dat die structuur goed is uitgewerkt en er de juiste beperkingen ingevoerd zijn.
Het is ook zeer gevaarlijk om wifi af te schermen met één wpa2-key voor alle gebruikers. Allereerst kan je geen opdeling maken tussen de gebruikers. Wanneer iemand vertrekt, heb je immers enkel de keuze om de key te veranderen op alle toestellen of de oude key gewoon te laten staan. Praktisch gezien is het ook niet zo moeilijk om een key te raden, zeker als het geen echte string is maar gewoon een woord dat je ook in een woordenboek kan terugvinden. Je hoeft immers ook niet voor de deur te staan om de wpa-key te kraken. Gewoon een paar pakketjes sniffen en de rest kan je netjes op je workstation thuis of op iaas-infrastructuur in de cloud doen. Er zijn bovendien online lijsten te vinden die je helpen bij het ontcijferen van keys (www.cloudcracker.com) om het nog vlotter te laten verlopen.

Hoe kan het beter?

Conclusie: de toegang tot de bedrijfswifi moet beter beveiligd zijn. De beste oplossing is door gebruik te maken van wpa2 enterprise authenticatie, in combinatie met 802.1x. Hierbij authentificieert elke gebruiker zich met een eigen userid en wachtwoord met een radiusserver (dit kan bijvoorbeeld ook de active directory in je omgeving zijn) en op basis hiervan wordt de gebruiker in het juiste vlan geplaatst. Als je bijvoorbeeld een strikte opdeling tussen administratie en r&d wil, wordt een gebruiker van de administratie in het administratie-vlan geplaatst en een onderzoeker in r&d, netjes gescheiden zonder verdere risico's. Het gebruik van 802.1x is trouwens ook een goed idee op je bekabelde netwerk omdat het deze opdeling dynamisch toelaat en het onbevoegden die gewoon hun pc inpluggen in een poort op een makkelijke manier buitenhoudt.



Bij de aanschaf van de infrastructuur is het een goeie vraag waar je te rade gaat. Ofwel kies je voor dezelfde leverancier die de rest van je netwerk levert in de vorm van de Cisco's, HP's en Extreme Networks van deze wereld. Bedrijven die stuk voor stuk de nodige acquisities in de draadloze wereld deden. Ofwel kies je voor een draadloze speler als Aerohive of Ruckus Networks die zich volledig gespecialiseerd hebben in het draadloze verhaal.

Andere gevaren

Daarnaast zijn er voor het interne netwerk en de data die er op zitten nog andere gevaren. In de eerste plaats zijn er zogenaamde rogue access points. Van deze losgeslagen AP's zijn er eigenlijk 3 types.
Enerzijds heb je de interne gebruiker die draadloos wil werken op kantoor en dus maar een draadloos AP van de winkel of van thuis meebrengt, en dit (slecht beveiligd) in het interne netwerk plugt. Op die manier staat je interne netwerk potentieel wagenwijd open.
Anderzijds heb je hackers die een vals AP gebruiken dat doet alsof het een AP van het interne netwerk is en het wat meer zendvermogen geven (je kan bijvoorbeeld relatief makkelijk AP's of kaarten aankopen met een zendvermogen tot 3 watt vergeleken met de 100 mwatt die op legale toestellen mogelijk is). De eindgebruiker logt in op de verkeerde AP, geeft zijn credentials *et voilà*, de veiligheid van het aangevallen netwerk is omzeild. Dit soort aanvallen - ook wel *evil twin attacks* genoemd - zijn eigenlijk de draadloze netwerkversie van phishing.
Last but not least heb je ook af en toe een goeie AP, die om diverse redenen zijn configuratie verliest en met een standaard of open configuratie in het netwerk hangt, met alle potentieel slechte gevolgen van dien.
Eindgebruikers hebben soms ook de vervelende gewoonte om hun pc in het interne netwerk te hangen maar tegelijkertijd ook via een wireless hotspot, bijvoorbeeld van Telenet of Belgacom, naar het internet te gaan en op die manier een brug naar het interne netwerk toe te laten.
Soms wil je in sommige delen van een gebouw (bijvoorbeeld een gevangenis) ook helemaal geen wireless of zelfs gsm-netwerken toelaten. Daarnaast is het vaak een koud kunstje om een *denial of service* aanval uit te voeren door een zender neer te zetten die de frequenties van het draadloze netwerk stoort, zodoende dat het onveilig wordt.
Je wil ook een oog houden op rare dingen die in je netwerk gebeuren: mac-adressen die gespoofd worden (toestel dat zijn mac-adres verandert zodoende dat het een ander toestel lijkt) of wardrivers die continu kijken welke netwerken er zijn of andere abnormale netwerkactiviteit.
Allemaal dingen die moeilijk te bestrijden zijn en waartegen al geheel of gedeeltelijk systemen in de verschillende draadloze enterprise producten zitten. Bedrijven als Airtight leveren hiertegen wat ze noemen wireless intrusion detection (wids) of intrusion prevention systems. Ze werken analoog met ids en ips-systemen in een traditioneel netwerk en gaan dit soort aanvallen detecteren en proberen te verhinderen door aanpassingen in de (wireless) netwerkomgeving te maken en de rotte appels te blokkeren en van het netwerk te weren. Technisch werken ze door specifieke draadloze toestellen (sensors) in de buurt van het netwerk te plaatsen en alles in de gaten te houden en te rapporteren naar een centrale server die op zijn beurt beslissingen neemt om de draadloze aanvallen tegen te houden.

Conclusie

Samengevat: draadloze netwerken zijn niet zo onschuldig als ze lijken. Als gewone gebruiker van hotspots en open netwerken, loop je het risico dat wat je allemaal op het internet uitvoert afgeluisterd kan worden, en er zijn een aantal potentiële privacy-gevaren. Wees dus net als op het internet voorzichtig en beperk wat je laptop, tablet of telefoon allemaal aan informatie het draadloze netwerk opstuurt. Misschien is het ook geen slecht idee om je draadloos netwerk af te zetten en enkel in te schakelen als je het echt nodig hebt.
Als netwerkbeheerder is het draadloze netwerk de gevaarlijke buitengrens van je domein, het is dan ook belangrijk dat je alles volgens de regels van de kunst slim opzet en eventueel ook met het nodige gezond verstand correct implementeert. Voor sommige aspecten zoals een spectrum-onderzoek kan het nooit kwaad om ook echte specialisten in te huren.□

DENKEN ALS EEN STROPER

'The proof of the pudding is in the eating' is een kardinale levenswijsheid die ook op het vlak van draadloze netwerken geldt. Om een goede boswachter te zijn, is het belangrijk dat je ook een beetje als stroper denkt. Het is dan ook een goed idee om je eigen draadloze netwerk op lekken te controleren met dezelfde softwaretools als hackers gebruiken om je aan te vallen.
Een goeie start hierbij is Kali Linux (de opvolger van Backtrack). Een speciaal voor security-audits samengestelde linuxdistributie die een berg aan securitytools bevat om onder andere ook de veiligheid van draadloze netwerken te analyseren. Van wardrivingsoftware zoals Airmon, over wep/wpa krakers als Aircrack tot sniffers à la Ettercap en Wireshark. Je vindt ze allemaal in één boot-usb of cdrom.
Bovendien kan je je laptop met de livedvd of usbstick booten en zonder schade of herinstallatie nadien terug gebruiken.

Kali: het Zwitsers zakmes voor elke securityexpert