TECHN 36

Periodieke publicatie van Smals

Augustus 2012

De beveiliging van Wi-Fi-netwerken

Cryptografische Aspecten

Julien Cathalo is doctor in de toegepaste wetenschappen. Sinds juni 2010 werkt hij als consultant bij de sectie Onderzoek van Smals. Hij is gespecialiseerd in cryptografie en hij bestudeert nuttige oplossingen voor de gezondheidssector en voor de sociale zekerheid. Hij volgt voornamelijk de problematiek op over de beveiliging van Cloud Computing.

Contact: 02 787 59 48

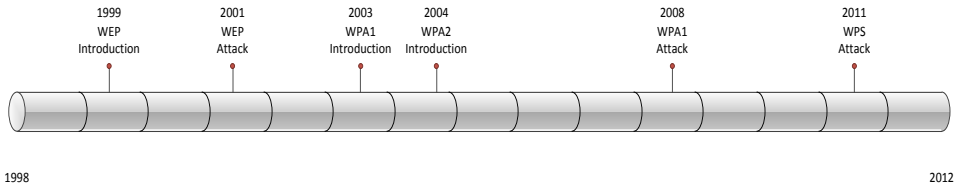
Julien.Cathalo@smals.be

Inleiding

Wi-Fi-netwerken maken deel uit van ons dagelijks leven. Ze zorgen voor de draadloze uitwisseling van gegevens op een informaticanetwerk. Of ze nu gebruikt worden voor privé- of werkdoeleinden, het is noodzakelijk dat ze beveiligd worden om de netwerktoegang en de vertrouwelijkheid van de verstuurde gegevens te beschermen. Het grote publiek lijkt zich daar nu van bewust te zijn: volgens een recente studie van de Wi-Fi Alliance uitgevoerd in de VS hebben inderdaad 86 % van de Wi-Fi-gebruikers basismaatregelen genomen ter bescherming[1].

Op technisch vlak omvat deze beveiliging drie facetten: authenticatie die zorgt dat enkel bevoegde machines toegang hebben tot het netwerk, vercijfering die zorgt dat de vertrouwelijkheid van de uitgewisselde gegevens op het netwerk gegarandeerd wordt, en integriteitscontrole van de uitgewisselde gegevens. Om dit uit te voeren, heeft de Wi-Fi Alliance meerdere beveiligingsprotocols voorgesteld. Dat was eerst WEP ("Wired Equivalent Privacy") in 1999 in de originele IEEE 802.11 standaard, die vervangen werd door WPA1 ("Wi-Fi Protected Access") in 2003, en vervolgens door WPA2 in 2004.

Waarom twee keer van protocol veranderen? De eenvoudige reden is dat grote veiligheidsgebreken bijgewerkt werden, eerst in het WEP-protocol en daarna in WPA1.



Figuur 1: Ontwikkeling van de Wi-Fi-beveiliging

De volgende hoofdstukken komen terug op deze ontwikkeling door de cryptografische werking van verschillende protocols en aanvallen uit te leggen. Het laatste deel handelt over de Wi-Fi Protected Setup (WPS) dat geen cryptografisch protocol is in de enge zin van het woord maar een standaard om beveiligde Wi-Fi-netwerken op een eenvoudige manier op te zetten.

[1] http://www.wi-fi.org/media/press-releases/wi-fi%C2%AE-security-barometer-reveals-large-gap-between-what-users-know-and-what

Enkele definities

- Een *symmetrisch vercijfersysteem* is een systeem waarmee dezelfde sleutel wordt gebruikt om berichten te vercijferen en te ontcijferen. Men kent voornamelijk twee types systemen voor symmetrische vercijfering: de “blokvercijfering” en de “stroomvercijfering”.
- *“Blokvercijfering” of “block cipher”* is een symmetrisch vercijfersysteem dat functioneert door niet-vercijferde blokberichten met een bepaalde grootte te vercijferen (bijvoorbeeld, 128 bits). De meest gekende blokvercijfering is AES (Advanced Encryption Standard) alsook zijn voorloper (nu verouderd en onveilig) DES.
- *“Stroomvercijfering” of “stream cipher”* is een type symmetrisch vercijfersysteem gebaseerd op het genereren van een keten van pseudo-random bits. De vercijfering bestaat erin, vanuit de sleutel, een keten van pseudo-random bits te genereren en om daarna de XOR te berekenen tussen deze keten en het niet-vercijferde bericht. Het resultaat is het vercijferde bericht. Om te ontcijferen, genereert men dezelfde keten van bits vanuit de sleutel, daarna berekent men de XOR tussen deze keten en het vercijferde bericht. Het resultaat is het niet-vercijferde bericht. Het RC4-algoritme is een van de meest gekende en gebruikte manieren van stroomvercijfering.
- De *“counter mode”* is een methode voor stroomvercijfering die onderliggend gebruik maakt van blokvercijfering. Bij elk nieuw blok wordt een teller eerst opgehoogd en vervolgens geëncrypteerd met de symmetrische sleutel, wat resulteert in een pseudo-randomwaarde. Vervolgens wordt, zoals bij stroomvercijfering, de XOR berekend tussen deze random waarde en het te vercijferen blok.
- Een *cyclische redundantiecode* (CRC) is een systeem gebruikt om toevallige veranderingen in de gegevens op te sporen.
- Een *Message Authentication Code* (MAC) is een authenticatiealgoritme met een gedeelde geheime sleutel.
- In deze tekst verwijzen de termen *"client"* en *"toegangspunt"* naar respectievelijk het apparaat dat zich op het netwerk connecteert en het apparaat dat toegang tot het netwerk mogelijk maakt.

WEP: Wired Equivalent Privacy

Het protocol “Wired Equivalent Privacy” of WEP maakte deel uit van de eerste Wi-Fi-standaard IEEE 802.11. Zijn naam beloofde een beveiliging gelijk aan een draadverbinding, maar we zullen zien dat dit helemaal niet zo is.

De WEP gebruikt de volgende algoritmes:

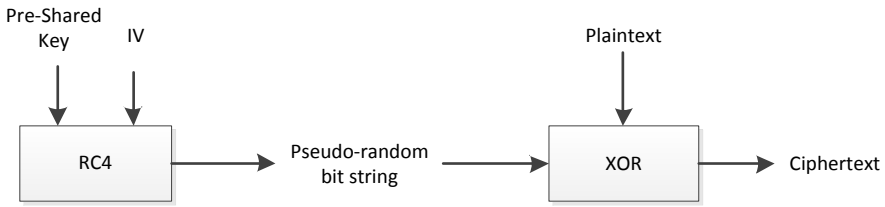
- De stroomvercijfering RC4 om de gegevens te vercijferen en de client te authenticeren bij een toegangspunt.

- De redundantiecode CRC32 om de integriteit van de gegevens na te gaan.

De WEP-vercijfering functioneert als volgt.

De client en het toegangspunt zijn voorzien van eenzelfde sleutel, de Pre-Shared Key of PSK. Meerdere sleutelgroottes voor PSK zijn mogelijk: 40 bits, 104 bits en 232 bits.

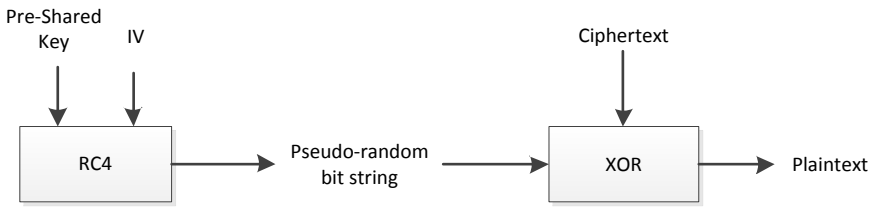
Het RC4-algoritme zal, vanuit deze sleutel en vanuit een willekeurige IV ("initialization vector") van 24 bits, willekeurige bits genereren. Een nieuwe IV wordt willekeurig gegenereerd voor elk pakket. Zo zal de keten van bits telkens verschillend zijn. Het vercijferde bericht wordt verkregen door de XOR tussen deze willekeurige keten en het niet-vercijferde bericht te berekenen.



Figuur 2: WEP-vercijfering

Het vercijferde bericht alsook de IV wordt vervolgens verstuurd naar de bestemmeling.

De ontcijfering bestaat erin eenvoudigweg dezelfde willekeurige ketting te genereren vanuit de PSK en de IV. Daarna berekent men de XOR tussen het vercijferde bericht en de willekeurige ketting om het niet-vercijferde bericht te reconstrueren.



Figuur 3: WEP-ontcijfering

Veiligheidsgebreken van de WEP

Men merkt al een eerste zwakte van dit systeem op: de grootte van de IV's (24 bits) is onvoldoende. Na 5000 uitgevoerde vercijferingen is er gemiddeld 50 % kans dat dezelfde IV twee keer gebruikt wordt. Dit impliceert dat dezelfde pseudo-random ketting wordt gegenereerd… Men heeft dus twee paar berichten (*cml*, *eml*) en (*cm2*, *em2*) waar *cm* niet-vercijferd bericht betekent ("clear message") en *em* vercijferd bericht betekent ("encrypted message"), zodat:

- *em1* = *cm1* XOR RC4 (PSK, IV)
- *em2* = *cm2* XOR RC4 (PSK, IV)

Door de XOR tussen de twee regels te berekenen en dankzij het feit dat RC4(PSK, IV) XOR RC4(PSK, IV) = 0000000000, verkrijgt men dat *eml* XOR *em2* = *cml* XOR *cm2*. Men ziet dus dat een aanvaller die de PSK-sleutel niet kent en twee vercijferde berichten met dezelfde IV vindt, de XOR tussen twee overeenkomstige niet-vercijferde berichten kan

verkrijgen. De aanvaller heeft dus veel informatie over de twee niet-vercijferde berichten gevonden (maar niet de berichten zelf, noch de sleutel).

De onveiligheid van WEP gaat verder en de eerste echte aanval werd uitgevoerd in 2001. Hij staat beschreven in een artikel gepubliceerd door Fluhrer, Mantin en Shamir[2].

De aanval exploiteert de zwakheden in het RC4-algoritme. Door meerdere vercijferde pakketten te bestuderen, kan een aanvaller de PSK-sleutel ontdekken. Het systeem wordt dus beschouwd als volledig gebroken. De aanval kan ingezet worden met behulp van software zoals aircrack-ng op voorwaarde dat men over een compatibele Wi-Fi-kaart beschikt (dat hangt af van de chipset van de kaart).

WEP wordt dus beschouwd als cryptografisch gebroken: WEP gebruiken om een Wi-Fi-verbinding te beschermen is dus af te raden, want deze biedt niet voldoende bescherming.

WPA1: Wi-Fi Protected Access

De WPA- of WPA1-standaard (“Wi-Fi Protected Access”), ook TKIP genoemd (“Temporal Key Integrity Protocol”), werd voorgesteld door de Wi-Fi Alliance in 2003. Gezien WEP van toen af gebroken was, was er dus nood aan een nieuw veiligheidsprotocol dat bovendien compatibel moest zijn met de reeds bestaande Wi-Fi netwerkkaarten. Het werd dus als een tijdelijke oplossing voorgesteld in afwachting van de IEEE 802.11i standaard. Deze voorwaarden leggen uit waarom WPA1 zo vlug werd aangevallen: het voorstel werd immers niet door derden gevalideerd.

WPA, net zoals zijn opvolger WPA2, biedt twee modi aan:

- WPA-Enterprise, een modus waarin de clients zich moeten authenticeren bij een server om de toegangscodes tot het netwerk te ontvangen
- WPA-Personal, een modus waarin alle clients een gemeenschappelijke "passphrase" gebruiken

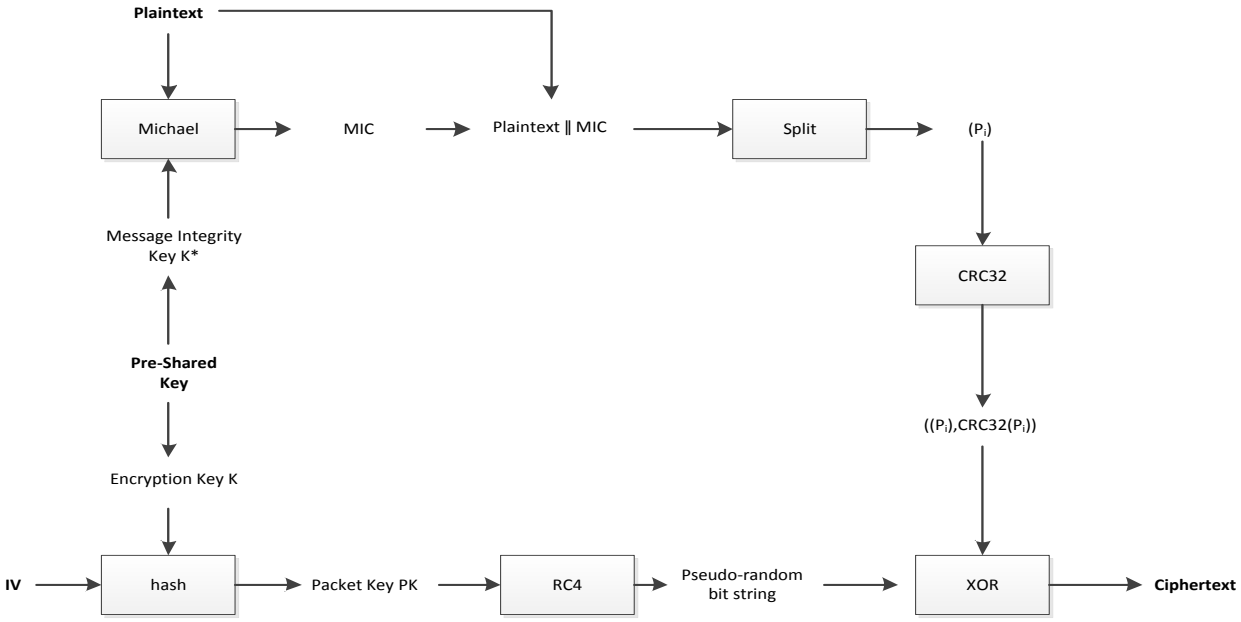
WPA-Enterprise vereist een server voor 802.1X authenticatie en werd dus eerder ontworpen voor de grote bedrijven. WPA-Personal is een lichtere oplossing, gemakkelijker te installeren en is bedoeld voor particulieren en kleine bedrijven.

Het WPA1-protocol gebruikt een “MIC” (Message Integrity Code) genaamd Michael en een hashing-functie genaamd "hash". Om een bericht te vercijferen en te authenticeren, gebruikt men een vrij ingewikkelde methode, die geïllustreerd wordt in figuur 4:

1. Vanaf een sleutel genaamd “pre-shared key” leidt men twee nieuwe sleutels af: een vercijfersleutel K en een integriteitssleutel K*.
2. Met de sleutel K en een initialisatievector IV berekent men een “packet key”. Vanaf deze sleutel leidt men een bitsstroom af met een RC4-algoritme.
3. Met de sleutel K* en het algoritme Michael berekent men een code vanaf het niet-vercijferde bericht. Vervolgens deelt men het resultaat (gevormd door het niet-vercijferde bericht en de code) op in fragmenten. Voor elk fragment berekent men zijn CRC32.

Het vercijferde bericht bestaat uit de XOR tussen de bitsstroom en de met behulp van CRC32 aaneengeschakelde fragmenten.

[2] Scott R. Fluhrer, Itsik Mantin, Adi Shamir: Weaknesses in the Key Scheduling Algorithm of RC4. Selected Areas in Cryptography 2001: 1-24



Figuur4: WPA1 - vercijfering en - authenticatie

Om de compatibiliteit met de bestaande Wi-Fi-hardware te garanderen, heeft men een systeem opgesteld gebaseerd op dezelfde componenten (RC4, CRC32) als WEP, maar ze worden op een andere manier gebruikt om de veiligheidsproblemen bij WEP te omzeilen.

Veiligheidsgebreken van de WPA1

Vanaf de invoering van WPA1 werden al zwaktes opgemerkt. Maar de eerste gepubliceerde doeltreffende aanval tegen WPA1 dateert van 2008 en werd opgezet door de onderzoekers Beck en Tews[3]. Hun aanval zorgt ervoor dat het niet-vercijferde bericht kan teruggevonden worden vanaf een vercijferd bericht, en dat het bericht vervalst kan worden. Het zijn dus tegelijk de vercijfering en de integriteit die gebroken zijn. Hun aanval beperkt zich tot de implementaties van WPA1 die QoS-functionaliteiten (Quality of Service) van de standaard IEEE802.11e ondersteunen. Een jaar later ontwikkelen Ohigashi en Morii een nieuwe aanval die doeltreffender is en die niet beperkt is tot de QoS.

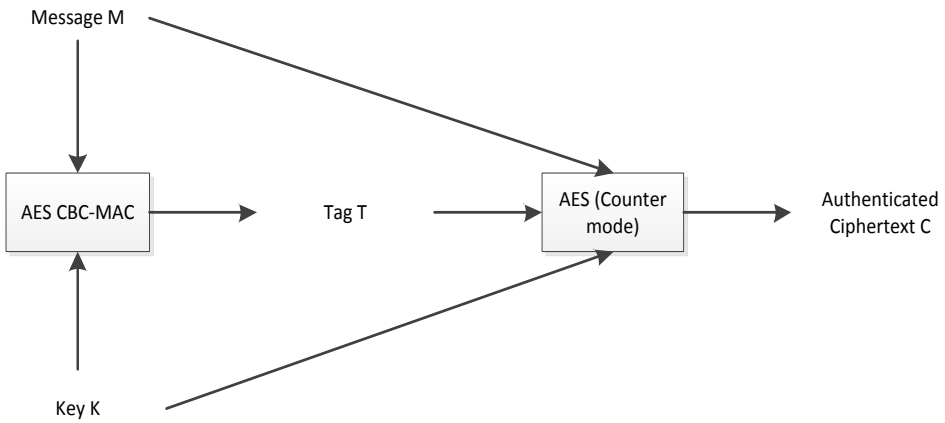
[3] Martin Beck, Erik Tews: Practical attacks against WEP and WPA. IACR Cryptology ePrint Archive 2008: 472 (2008)

WPA2: Wi-Fi Protected Access 2

WPA2 gebruikt het vercijferprotocol CCMP. Het principe van CCMP bestaat erin het vercijferalgoritme AES in CCM-modus (Counter with CBC-MAC) te gebruiken, wat dadelijk wordt uitgelegd. Het doel is om zowel de vertrouwelijkheid als de authenticiteit te garanderen.

Om een bericht M te vercijferen en te authenticeren met AES in CCM-modus met een sleutel K gaat men op de volgende manier te werk:

- Men berekent een tag T met een MAC vanaf een bericht M en sleutel K met AES in CBC-MAC-modus.
- Men vercijfert het bericht M alsook de tag T met AES in counter mode met sleutel K.



Figuur 5: CCMP-vercijfering en -authenticatie

Sinds 2006 moet alle materiaal dat het gedeponeerd merk Wi-Fi wil dragen verplicht WPA2 ondersteunen.

Beveiliging van WPA2

De standaard WPA2 steunt, in tegenstelling tot zijn voorlopers, op beproefde cryptografische methodes. De veiligheid van de gebruikte CCMP methode is formeel bewezen, wat betekent dat deze methode veilig is onder bepaalde aannames; voor een expert in cryptografie impliceert dit dat de methode robuust en goed gebouwd is. Het vercijferalgoritme AES is sinds 2001 een standaard van het NIST (National Institute of Standards and Technology) en de NSA keurt het gebruik ervan goed voor top secret informatie. De veiligheid werd niet formeel aangetoond, maar werd meerdere keren onderzocht zonder dat een praktisch haalbare aanval gevonden werd.

Deze elementen boezemen dus vertrouwen in wat betreft de veiligheid van WPA2, zelfs als ze geen 100% garantie kunnen bieden dat het protocol onaantastbaar is. De gebruikers moeten er vooral op letten dat ze een wachtwoord kiezen dat lang en ingewikkeld genoeg is om bestand te zijn tegen een "brute force"-aanval. Een "brute force"-aanval bestaat erin zeer veel wachtwoorden te proberen tot men het goede wachtwoord vindt.

Over “Wi-Fi Protected Setup” (WPS)

De Wi-Fi Protected Setup (WPS) is een standaard van de Wi-Fi Alliance, vastgelegd in 2007, die als doel heeft om op een eenvoudige en beveiligde manier een Wi-Fi-connectie te creëren. In tegenstelling tot WEP, WPA1 en WPA2 is het dus geen protocol voor het beveiligen van draadloze communicatie. Het gebruikersgemak mag dan wel verzekerd zijn, dat geldt echter niet voor de veiligheid zoals we verder zullen zien. Met deze methode voorkomt men dat de gebruiker een veiligheidsmethode moet bepalen en een ingewikkeld paswoord moet kiezen. Deze modus wordt standaard geactiveerd voor het merendeel van de recente Wi-Fi-routers. Meerdere opties bestaan om een client toe te voegen aan het netwerk:

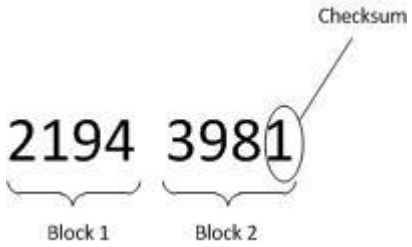
1. *Client PIN Method.* Een PIN wordt afgelezen van de client (via een scherm of een sticker) en moet door de gebruiker ingetypt worden op het toegangspunt.
2. *Router PIN Method*. De PIN wordt geschreven op het toegangspunt en moet ingevoerd worden in de client.
3. *Push-Button-Method.* De gebruiker moet op een knop drukken (eventueel virtueel) op de client en op het toegangspunt.

Veiligheidsgebreken van de Wi-Fi Protected Setup

In december 2011 hebben de onderzoekers Stefan Viehböck en Craig Heffner elk afzonderlijk een zwakte ontdekt in WPS[4]. Deze zwakte betreft de "Router PIN Method” waarmee de PIN geschreven op het toegangspunt ingevoerd wordt op de client die men wil toevoegen aan het netwerk. De aanval gaat uit van de vaststelling dat fysieke toegang niet nodig is en dat het enige benodigde element voor authenticatie de kennis van de PIN is; het volstaat om de PIN te kennen. Vooraf moeten er dus 100 000 000 PIN’s (10^8) getest worden voor een exhaustieve scan (of “brute force”-aanval); de PIN bestaat immers uit acht cijfers. Als men bij deze observatie blijft stilstaan, dan kan men denken dat een exhaustieve scan in de praktijk niet mogelijk is, gezien het te grote aantal combinaties.

Het toegangspunt gaat helaas eerst de eerste 4 cijfers na. Men kan dus beginnen met alle mogelijke combinaties van die 4 eerste cijfers te testen om achteraf de rest te testen, oftewel 10^4+10^4 = in totaal 20 000 combinaties om te testen. Het laatste cijfer van de PIN is bovendien een checksum van de 7 vorige cijfers; het aantal te testen combinaties komt dus op 10^4+10^3 = 11 000.

[4] http:// www.h-online.com/open/news/item/Wi-Fi-Protected-Setup-made-easier-to-brute-force-Update-1401822.html



Figuur 6: Formaat van een PIN WPS

De aanval bestaat er dus in om, gebruikmakend van de Router PIN method, een WPS te starten met een toegangspunt waarop men zich wil aansluiten en vervolgens gaat men de combinaties testen om verbinding te maken. Bepaalde toegangspunten blokkeren na het invoeren van meerdere foutieve PIN's. Dit houdt de aanval niet tegen, maar vertraagt hem enkel.

De tools Wpscrack en Reaver implementeren deze aanval door de PIN in enkele uren terug te vinden.

Er bestaan niet veel mogelijkheden om zijn eigen Wi-Fi-netwerk te beschermen tegen deze aanval: men moet wanneer het mogelijk is WPS deactiveren op het toegangspunt en de firmware van het Wi-Fi-toegangspunt bijwerken wanneer de updates beschikbaar zijn. Dat is overigens wat aanbevolen wordt door de CERTA (Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques), een Franse overheidsinstelling[5].

Als gevolg van de bekendmaking van deze aanval hebben meerdere constructeurs handleidingen gepubliceerd om hun gebruikers uit te leggen hoe ze WPS kunnen deactiveren.

Conclusie

De geschiedenis van de beveiliging van Wi-Fi-netwerken is bewogen en wordt gekenmerkt door de opeenvolgende aanvallen tegen de verschillende standaarden van de Wi-Fi Alliance. Momenteel is de enige raadzame oplossing WPA2. Enkel dit systeem biedt voldoende bescherming voor een Wi-Fi-netwerk. De andere protocols (WEP en WPA1) zijn niet veilig.

De Wi-Fi Protected Setup is overigens ook onveilig en moet gedeactiveerd worden op de toegangspunten. Het gebruik van WPA2 alleen is niet genoeg. De gebruiker moet waakzaam blijven; hij moet vooral nauwgezet zijn wachtwoord kiezen[6].

[5] http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-001/CERTA-2012-ACT-001.html

[6] Zie hierover het artikel van Kristof Verslype op de blog van de sectie Onderzoek: http://blogresearch.smalsrech.be/?p=4078