Jordy RIts

Verslag Information Security: Wardriven

- Wetenschappelijk Rapport

    - Anno 2016 is het voor velen niet vanzelfsprekend om zich een huishouden voor te stellen zonder computers, het informaticatijdperk waarin we momenteel leven heeft het leven op vele vlakken beter, sneller en mobieler gemaakt.
      Informatica en worden niet enkel gebruikt bij de toepassingen en workflow van grote bedrijven, maar ook bij de alledaagse handelingen van de gewone mens. Vele mensen kijken dan ook niet meer op als ze een kind, dat nog op de lagere school zit, al met een smartphone of laptop zien.
      Het meerendeel van de mensen kunnen dan ook vlot werken met deze ict toestellen en integreren de toepassingen die deze toestellen met zich meebrengen heel vaak in hun privé of werk (denk email, smartphone, sociale media, ...). Wanneer we echter hun kennis betreffende deze zaken verder gaan bestuderen zal gauw blijken dat hun kennis van de achterliggende veiligheidsmaatregelen van deze toestellen, alsook de werking van deze toestellen geheel onbestaande is. De gemiddelde gebruiker zal zich inwerken in de high-level applicatie en de toepassingen ervan proberen te snappen en gebruiken. Het two-factor authenticatie proces met gebruikersnaam en wachtwoord is ondertussen zo ingeburgerd dat velen dit authorisatie en authenticatie proces als vanzelfsprekend en soms zelfs vervelend beschouwen. Het besef van hoe dit (authenticatie of authorisatie)proces achter de schermen nu juist werkt en hoe de veiligheid nu uiteindelijk wordt geïntegreerd is bij de meeste mensen onbestaande.

      Doordat dit proces zo abstract wordt geïnterpreteerd door de gebruikers en de gebruikers van de functionaliteit achter de schermen worden afgeschermd ontstaan er veiligheidsrisico's die de gebruikers data toch in gevaar kunnen brengen, ookal vermoed deze dat zijn/haar data onvoorwaardelijk beschermd wordt door de gebruikersnaam en wachtwoord. De gebruikers zijn niet op de hoogte van een aantal belangrijke zaken in verband met het beveiligen van dit wachtwoord, waardoor ze met deze zaken ook geen rekening kunnen houden.
      Een belangrijk aspect bijvoorbeeld bij de veiligheid van het gekozen wachtwoord is het aantal karakters of lengte van het passwoord, vele platformen integreren een basis sterkte van wachtwoord door een requirement op de lengte van het wachtwoord te zetten, waardoor te korte wachtwoorden die in een mum van tijd zouden kunnen worden gehack via een brute force attack, waarbij letterlijk alle mogelijke combinaties van karakters worden uitgeprobeerd, waardoor de lengte van het wachtwoord hierdoor

rechtstreeks in verband staat met de veiligheid die exponentieel verhoogt met elk extra karakter.
Een ander belangrijk punt waarmee rekening zou moeten worden gehouden bij het aanmaken van een gebruiker's wachtwoord is dat hackers in staat zijn om lijsten met woordenboeken over alle denkbare onderwerpen kunnen uitproberen tegenover een wachtwoord. Waarbij niet enkel alle woorden van dit woordenboek worden uitgeprobeerd maar ook alle combinaties van de woorden uit deze woordenboeken, woorden achterstevoren, nummers achter de woorden worden geplaats of bepaalde karakters gaan vervangen (veel mensen gebruikern $ als S, 3 als E, 0 als O, 1 als I,... hackers kunnen dit zelf integreren in hun woordenboeken waardoor deze veiligheidsmaatregel niet altijd veel nut heeft).

Er gebeuren vaak studies naar de wachtwoorden die gebruikers vaak gebruiken, hieruit blijkt steeds dat kennis over de wachtwoordbeveiliging en de keuze van het wachtwoord in termen van security ongekend is bij de gebruikers. Aangezien de meest gebruikte wachtwoorden globaal steeds enorm onveilig zijn (meest gebruikte passwoorden: 123, 321 , password,.... dit soort wachtwoorden kan een hacker zelfs raden zonder enige technologische vereisten, een brute force kraakt dit soort passwoorden ook in enkele seconden). De gemiddelde veiligheid van de wachtwoorden die globaal gekozen worden door de gemiddelde gebruiker is dus ruimschoots onvoeldoende als er wordt gekeken naar de veiligheid die dit wachtwoord met dit meebrengt of dus eigelijk zou moeten meebrengen, aangezien door de slechte keuze van wachtwoord deze veiligheid maar een illusie is naar de gebruiker toe.
De gebruiker zelf is niet bewust van de gevolgen die de slechte keuze van hun wachtwoord met zich meebrengt, de gebruiker wordt ook via geen enkele instantie op geen enkel punt bewust gemaakt over deze gevolgen.

In de huidige maatschappij waar we leven in een informaticatijdperk met een digitalisatie van zoveel diensten waarbij vaak een authenticatie is vereist is deze slechte bewustheid over de gevolgen en belangrijkheid van de juiste keuze van wachtwoord ontdenkbaar en eigenlijk onaanvaardbaar. Wanneer deze online diensten zullen evolueren en meer gevoelige data gaan bevatten zal dit probleem pas echt gaan resulteren in erge gevolgen van dataverlies voor de gebruikers.

Om te verzekeren dat er enkel kan geauthoriseerd worden als een gebruiker de juiste credentials heeft wordt er bij het verbinden met een draadloos wifi netwerk gebruik gemaakt van verschillende encryptie standaards. Waarbij de belangrijkste WPA2, WPA en WEP zijn, opgelijst volgend veiligheid van het encryptie proces, waarbij WPA2 het veiligste encryptieproces is met geen serieuze kwetsbaarheden die een hacker kan gaan exploiten en WEP veel kwetsbaarheden bevat waardoor een hacker data kan gaan compromiseren.

De beschikbaarheid van de veilige WPA2 standaard zou de oplossing moeten bieden voor alle kwetsbaarheden die de oudere, vorige encryptiestandaarden met zich meebrachten. WPA en WEP zijn beiden onvoeldoende gebleken om data veilig te houden, anders zou er ook nooit een WPA2 standaard moeten zijn ontwikkeld. Maar net zoals bij het gebruik van veilige wachtwoorden is de kennis de die gemiddelde gebruiker heeft over de juiste encryptie standaarden die moet worden gebruikt om alle data op een zo veilig mogelijke manier te encrypteren onbestaande, resulterende in een nog wijd gebruik van de oudere WPA en WEP standaarden in veel huishoudens.

Om de verspreiding van het gebruik van de standaarden en de verdeling van het percentage gebruikers die de standaard gebruiken, kan worden gemonitord en in kaart worden gebracht door een actie genaamd wardriven. Bij wardriven zal een hacker op een actieve of passieve manier netwerken in kaart gaan brengen, waarbij op de actieve manier er effectief malicious acties worden uitgevoerd op netwerken waarbij de security setting niet optimaal zijn, doordat bijvoorbeeld gebruik wordt gemaakt van de WEP encryptie standaard, die kwetsbaarheden bevat.
Bij wardriven zal de hacker die wardrive sessie uitvoert scans gaan uitvoeren naar de access points van draadloze netwerken. Uit deze scan kan per access point allerlei informatie getoond worden aan de hacker. Het effectieve wardriven gebeurd door middel van een toestel uitgerust met een GPS en een wifi scanner (eventueel met versterkt signaal), dit toestel gaat dan eerst scannen naar alle wifi netwerken in de buurt en de data die hierbij binnenkomt wordt dan opgelijst zodat de data later te analyseren is. Bij een actieve scan wordt meteen een hack uitgevoerd op slecht beveiligde netwerken. Doordat de meeste toestellen maar tot een tiental meters ver wifi netwerken kunnen ontdekken zal een wardriven zich door een gebied verplaatsen terwijl de scan wordt uitgevoerd. (auto, fiets, ..).

Ik heb zelf een wardrive sessies uitgevoerd in Beveren en omstreken, waarbij ik 23.000 access points heb gescand en op een passieve manier data over heb verzameld over deze access points en hun encryptie methode, ik heb dus niet op een actieve manier bepaalde acties uitgevoerd op de access points met een slechte beveiliging. Uit deze wardrive sessies heb ik kunnen concluderen dat de veilige WPA2 encryptie technologie nog lang niet overal is toegepast, en een hele hoop wifi netwerken niet goed beveiligd zijn en dus kwetsbaar voor hacks.

Ik heb alle access points ook weergeven via markers op een google maps widget, waarbij ik verschillende kleuren heb toegekend aan markers van access points met verschillende encryptie technologieën. (access points met WPA2 encryptie standaard hebben groene marker iconen, WPA is orange en WEP is rood). Op deze manier kon ik op een duidelijke manier een overzicht krijgen van de verdeling alsook de preciese locatie van alle access points en hun encryptie standaard.

De resultaten van de verdeling naar encryptie type van mijn wardrive sessies zijn:

- WPA2 (22%)
- WPA (46%)
- WEP (1%)
- Open (28%)

Het merendeel van de open netwerken zijn publieke netwerken zoals bijvoorbeeld homespots.

Uit de wardrive sessies is gebleken dat de gemiddelde kennis over de beveiligingsmogelijkheden die gebruikers kunnen toepassen om hun data beter te beschermen niet overal gekend is aangezien ze niet overal is toegepast. WPA2 bestaat al sinds september 2004, dat deze standaard nog niet overal is toegepast is een indicatie van het falen van huidige veiligheidsnormen betreffende dit soort zaken vanuit bepaalde instanties, zijnde de overheid of de netwerk providers.

- Belgische wetgeving

Stelt dat het verboden is om toegangscodes te kraken om vervolgend toegang te krijgen tot een pc of een netwerk. Maar het is ook verboden om een onbeveiligde pc of netwerk zomaar te grbuiken. De wetgeving stelt ook dat:

Als de draadloze netwerken als een publieke elektronischecommunicatiedienst worden aangeboden, dan zijn de verplichtingen in de wet van 13 juni 2005 betreffende de elektronische communicatie van toepassing op de aanbiedende operatoren.

De grootste moeilijkheid die in deze problematiek wordt gesteld, is het feit dat dergelijke draadloze netwerken veelal door private personen of bedrijven zelf worden opgezet voor eigen, intern gebruik.

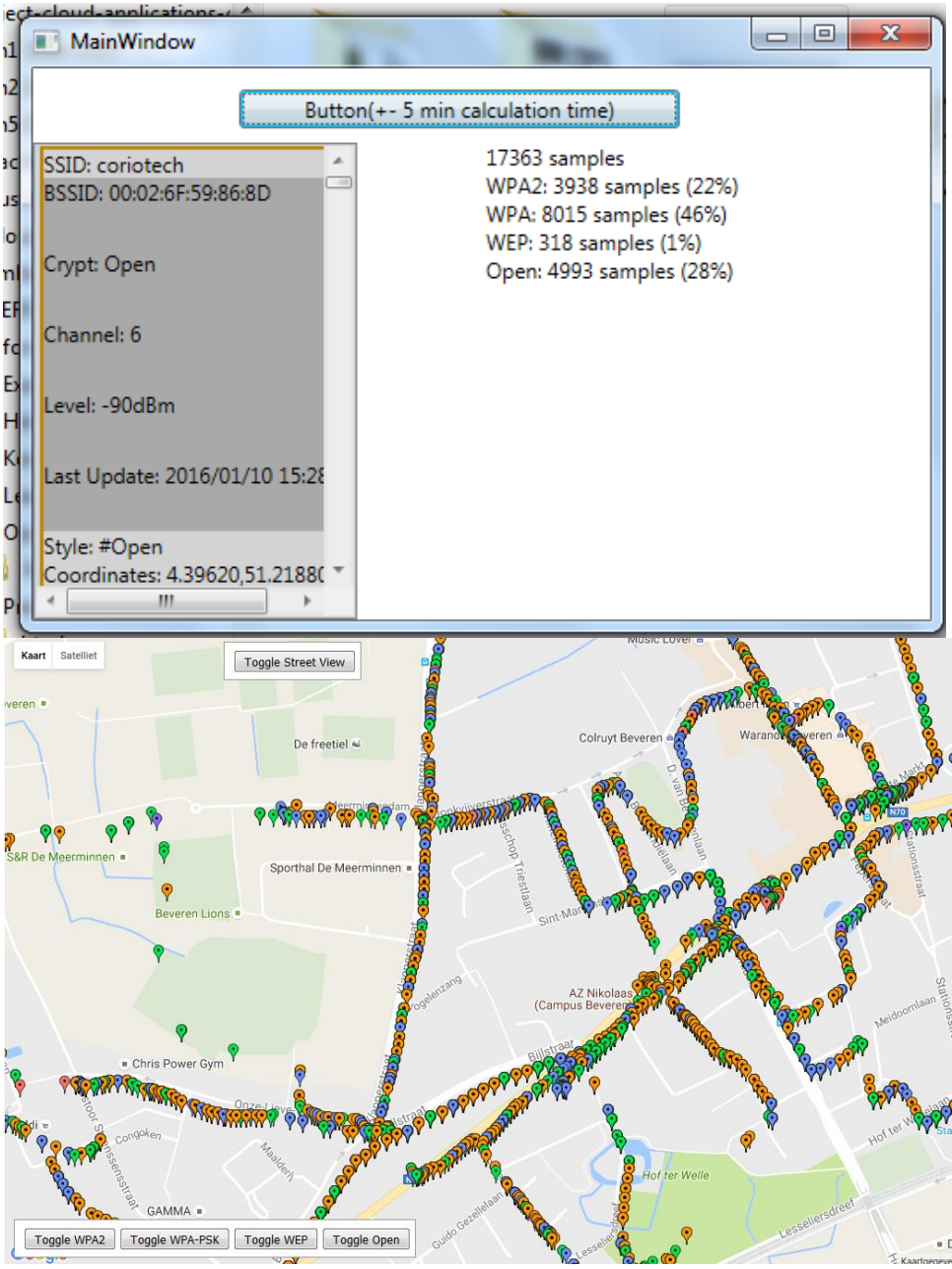
- Europese wetgeving

Voor de wetgeving betreffende wardriven in europa kan worden gesteld dat het niet illegaal is, maar er eerst toestemming moet worden gevraagd aan een legale authority. Enkele jaren geleden is bijvoorbeeld boven gekomen dat google aan wardriving deed via de auto's die camerabeelden maakten voor google street view. Hierbij werd de SSID en MAC adres van de access points verzameld, hierna is google wel aangeklaagd door verschillende instanties omdat er gevoelige data toch zou zijn verzameld en omdat google niet aan passieve scanning deed maar actieve, aangezien er ook een payload werd achtergelaten bij slecht beveiligde acces points, die kon worden gebruikt voor bepaalde google services.

- Artikel
    - Het is niet goed gesteld met de veiligheid van de draadloze netwerken in belgie.
      Het informaticatijdperk verwerkt informatie die als data beschreven staat. Deze data omvat ook een heleboel gevoelige informatie over de gebruiker, die niet altijd publiek mag worden getoond.
      Erwordt continu gewerkt door ingenieurs wereldwijd aan een totaaloplossing aan functionaliteiten die het beschermen van deze data garanderen.
      Oplossingen op maat die oplossingen bieden aan security uitdagingen en dus kunnen resulteren in het verder beveiligen van data bestaan en worden alom toegepast. De hoeveelheid gebruikers die werkt met de laatste technologieën , die nog niet gecompenseert en die geen vulnerabilities bevatten die kunnen wordeen geëxploiteerd door een hacker is echter nog veel te schaars, resulterende in een meerderheid van gebruikers met een niet optimaal beveiligde totaaloplossing van hun informaticasystemen.
      Om beter in kaart te brengen hoe het gestelt is met de verdeling van de veiligheidtechnologieën en om meet te weten te komen over individuele draadloze access points kunnen hackers aan wardriven doen. Bij de passieve versie van dit concept gaat een ethische hacker informatie verzamelen over de veiligheid van deze punten om deze dan te kunnen analyseren in functie van het verbeteren van (het inzicht in) de veiligheid. Bij actief wardriven zal een hacker op zoek gaan naar access points met een zwakke beveiliging die kwetsbaarheden bevat, om deze dan te exploiteren met als doel een malifide actie uitvoeren op het systeem waar de hacker geen toegang tot zou mogen hebben.
      Ik heb een passieve wardrive sessie uitgevoerd waarbij ik de veiligheid en verdeling van de enctyptie standaarden die worden gebruikt op de access points in Beveren in kaart heb gebracht en geanalyseerd . Uit deze wardrive sessies is gebleken dat de laatste encryptie methodologieën toch nog niet overal effectief worden toegepast, De meerderheid van de access points had een WPA encryptie, wat toch al lang verouderd is en plaats heeft gemaakt voor een veiligere methode namelijk WPA2.
      De concrete verdeling naar encryptie methode van de 23000 access points in beveren die ik heb gescand is als volgt:
      - WPA2 (22%)
      - WPA (46%)
      - WEP (1%)
      - Open (28%)

      Slechts 22% van al deze netwerken maakt gebruikt van de WPA2 technologie, wat enorm weinig is als je bedenkt dat de WPA2 standaard al bestaat sinds 2004.

- Screenshots



  - Groene markers = WPA2
  - Orange markers = WPA
  - Rode markers = WEP
  - Blauwe markers = Open
  - Paarse markers = other/unknown

- Code

```
function initMap() {
   var xhttp;
   xhttp = new XMLHttpRequest();
   xhttp.onreadystatechange = function() {
     if (xhttp.readyState == 4 && xhttp.status == 200) {
        loadMarkers(xhttp);
     }
   };
   xhttp.open("GET", "wardrive.xml", true);
   xhttp.send();
}



function loadMarkers(xml) {
  var astorPlace = {lat:  51.21256469999999, lng: 4.255287899999985};

  var map = new google.maps.Map(document.getElementById('map'), {
    center: astorPlace,
    zoom: 18,
    streetViewControl: false
  });


   var _list, i, xmlDoc;
   xmlDoc = xml.responseXML;
   console.log("xmlDoc= " + xmlDoc);
   _list = xmlDoc.childNodes[0];
   console.log("_list= " + _list);

   var list = _list.getElementsByTagName("Placemark");
   console.log("list :" + list);
   console.log(list.length);

   for (var i = 0; i < list.length; i++){
     var ap = list[i];
     var crypt = ap.getElementsByTagName("styleUrl")[0].innerHTML;
     var coordinates = ap.getElementsByTagName("coordinates")[0].innerHTML;
     var description = ap.getElementsByTagName("description")[0].innerHTML;
     var tmp = coordinates.split(',');
     var longitude = Number(tmp[1]);
     var latitude = Number(tmp[0]);

     var icon = {
```

```
      url: iconType(crypt), // url
      scaledSize: iconSize(crypt), // scaled size
      origin: new google.maps.Point(0,0), // origin
      anchor: new google.maps.Point(0, 0) // anchor
     };
     var _marker = new google.maps.Marker({
      position: {lat: longitude  , lng:  latitude},
      map: map,
      icon: icon,
      title: description
     });
     assignToArray(_marker);
    }
    panorama = map.getStreetView();
    panorama.setPosition(astorPlace);
    panorama.setPov(/** @type {google.maps.StreetViewPov} */({
     heading: 265,
     pitch: 0
    }));


  function iconType(crypt){
     if(crypt=="#WPA2")
         iconUrl = 'http://maps.google.com/mapfiles/ms/icons/green-dot.png';
       else if(crypt=="#Wep")
         iconUrl = 'http://maps.google.com/mapfiles/ms/icons/red-dot.png';
       else if(crypt=="#WpaPsk")
         iconUrl = 'http://maps.google.com/mapfiles/ms/icons/orange-dot.png';
       else if(crypt=="#Open")
         iconUrl = 'http://maps.google.com/mapfiles/ms/icons/blue-dot.png';
       else
         iconUrl = 'http://maps.google.com/mapfiles/ms/icons/purple-dot.png';
       return iconUrl;
    }

    function iconSize(crypt){
       if(crypt=="#WPA2")
         return new google.maps.Size(20, 20);
       else if(crypt=="#Wep")
         return new google.maps.Size(20, 20);
       else if(crypt=="#WpaPsk")
         return new google.maps.Size(20, 20);
       else if(crypt=="#Open")
         return new google.maps.Size(20, 20);
       else
         return new google.maps.Size(20, 20);
    }
```

```
    function assignToArray(marker){
      if(crypt=="#WPA2")
        markers_wpa2.push(marker);
      else if(crypt=="#WpaPsk")
        markers_wpapsk.push(marker);
      else if(crypt=="#Wep")
        markers_wep.push(marker);
      else if(crypt=="#Open")
        markers_open.push(marker);
    }

}

function toggleStreetView() {
 var toggle = panorama.getVisible();
 if (toggle == false) {
  panorama.setVisible(true);
 }
 else {
  panorama.setVisible(false);
 }
}

function toggleWPA2(){
   if(wpa2_keer==2){
      for(i = 0 ; i< markers_wpa2.length; i++){
        var oldIcon = markers_wpa2[i].getIcon();
        var newIcon = {url: oldIcon.url, scaledSize: new google.maps.Size(20, 20) , origin:
oldIcon.origin, anchor: oldIcon.anchor};
        markers_wpa2[i].setIcon(newIcon);
        markers_wpa2[i].setVisible(true);
      }
      for(i = 0 ; i< markers_wpapsk.length; i++)
        markers_wpapsk[i].setVisible(true);
      for(i = 0 ; i< markers_wep.length; i++)
        markers_wep[i].setVisible(true);
      for(i = 0 ; i< markers_open.length; i++)
        markers_open[i].setVisible(true);
      wpa2_keer=0;
   }
   else if(wpa2_keer==1){
      for(i = 0 ; i< markers_wpa2.length; i++)
        markers_wpa2[i].setVisible(true);
      for(i = 0 ; i< markers_wpapsk.length; i++)
        markers_wpapsk[i].setVisible(false);
      for(i = 0 ; i< markers_wep.length; i++)
        markers_wep[i].setVisible(false);
      for(i = 0 ; i< markers_open.length; i++)
```

```
            markers_open[i].setVisible(false);
        wpa2_keer=2;
    }
    else if(wpa2_keer==0){

        for(i = 0 ; i< markers_wpa2.length; i++) {
            var oldIcon = markers_wpa2[i].getIcon();
            var newIcon = {url: oldIcon.url, scaledSize: new google.maps.Size(40, 40) , origin:
oldIcon.origin, anchor: oldIcon.anchor};
            markers_wpa2[i].setIcon(newIcon);
            markers_wpa2[i].setVisible(true);
        }
        wpa2_keer=1;
    }
}

function toggleWPAPSK(){
    if(wpapsk_keer==2){
        for(i = 0 ; i< markers_wpa2.length; i++)
            markers_wpa2[i].setVisible(true);
        for(i = 0 ; i< markers_wpapsk.length; i++){
            var oldIcon = markers_wpapsk[i].getIcon();
            var newIcon = {url: oldIcon.url, scaledSize: new google.maps.Size(20, 20) , origin:
oldIcon.origin, anchor: oldIcon.anchor};
            markers_wpapsk[i].setIcon(newIcon);
            markers_wpapsk[i].setVisible(true);
        }
        for(i = 0 ; i< markers_wep.length; i++)
            markers_wep[i].setVisible(true);
        for(i = 0 ; i< markers_open.length; i++)
            markers_open[i].setVisible(true);
        wpapsk_keer=0;
    }
    else if(wpapsk_keer==1){
        for(i = 0 ; i< markers_wpa2.length; i++)
            markers_wpa2[i].setVisible(false);
        for(i = 0 ; i< markers_wpapsk.length; i++)
            markers_wpapsk[i].setVisible(true);
        for(i = 0 ; i< markers_wep.length; i++)
            markers_wep[i].setVisible(false);
        for(i = 0 ; i< markers_open.length; i++)
            markers_open[i].setVisible(false);
        wpapsk_keer=2;
    }
    else if(wpapsk_keer==0){
        for(i = 0 ; i< markers_wpapsk.length; i++) {
            var oldIcon = markers_wpapsk[i].getIcon();
            var newIcon = {url: oldIcon.url, scaledSize: new google.maps.Size(30, 30) , origin:
```

```
oldIcon.origin, anchor: oldIcon.anchor};
            markers_wpapsk[i].setIcon(newIcon);
            markers_wpapsk[i].setVisible(true);
        }
        wpapsk_keer=1;
    }



}



function toggleWEP(){
    if(wep_keer==2){
        for(i = 0 ; i< markers_wpa2.length; i++)
            markers_wpa2[i].setVisible(true);
        for(i = 0 ; i< markers_wpapsk.length; i++)
            markers_wpapsk[i].setVisible(true);
        for(i = 0 ; i< markers_wep.length; i++){
            markers_wep[i].setVisible(true)
            var oldIcon = markers_wep[i].getIcon();
            var newIcon = {url: oldIcon.url, scaledSize: new google.maps.Size(20, 20) , origin:
oldIcon.origin, anchor: oldIcon.anchor};
            markers_wep[i].setIcon(newIcon);
            markers_wep[i].setVisible(true);
        }
        for(i = 0 ; i< markers_open.length; i++)
            markers_open[i].setVisible(true);
        wep_keer=0;
    }
    else if(wep_keer==1){
         for(i = 0 ; i< markers_wpa2.length; i++)
            markers_wpa2[i].setVisible(false);
        for(i = 0 ; i< markers_wpapsk.length; i++)
            markers_wpapsk[i].setVisible(false);
        for(i = 0 ; i< markers_wep.length; i++)
            markers_wep[i].setVisible(true);
        for(i = 0 ; i< markers_open.length; i++)
            markers_open[i].setVisible(false);
        wep_keer=2;
    }
    else if(wep_keer==0){
        for(i = 0 ; i< markers_wep.length; i++) {
            var oldIcon = markers_wep[i].getIcon();
            var newIcon = {url: oldIcon.url, scaledSize: new google.maps.Size(40, 40) , origin:
oldIcon.origin, anchor: oldIcon.anchor};
            markers_wep[i].setIcon(newIcon);
```

```
            markers_wep[i].setVisible(true);
        }
        wep_keer=1;
    }
}

function toggleOPEN(){
    if(open_keer==2){
        for(i = 0 ; i< markers_wpa2.length; i++)
            markers_wpa2[i].setVisible(true);
        for(i = 0 ; i< markers_wpapsk.length; i++)
            markers_wpapsk[i].setVisible(true);
        for(i = 0 ; i< markers_wep.length; i++)
            markers_wep[i].setVisible(true);
        for(i = 0 ; i< markers_open.length; i++){
            var oldIcon = markers_open[i].getIcon();
            var newIcon = {url: oldIcon.url, scaledSize: new google.maps.Size(10, 10) , origin:
oldIcon.origin, anchor: oldIcon.anchor};
            markers_open[i].setIcon(newIcon);
            markers_open[i].setVisible(true);
        }
        open_keer=0
    }
    else if(open_keer==1){
        for(i = 0 ; i< markers_wpa2.length; i++)
            markers_wpa2[i].setVisible(true);
        for(i = 0 ; i< markers_wpapsk.length; i++)
            markers_wpapsk[i].setVisible(false);
        for(i = 0 ; i< markers_wep.length; i++)
            markers_wep[i].setVisible(false);
        for(i = 0 ; i< markers_open.length; i++)
            markers_open[i].setVisible(true);
        open_keer=2;
    }
    else if(open_keer==0){
        for(i = 0 ; i< markers_open.length; i++) {
            var oldIcon = markers_open[i].getIcon();
            var newIcon = {url: oldIcon.url, scaledSize: new google.maps.Size(30, 30) , origin:
oldIcon.origin, anchor: oldIcon.anchor};
            markers_open[i].setIcon(newIcon);
            markers_open[i].setVisible(true);
        }
        open_keer=1;
    }
}
```