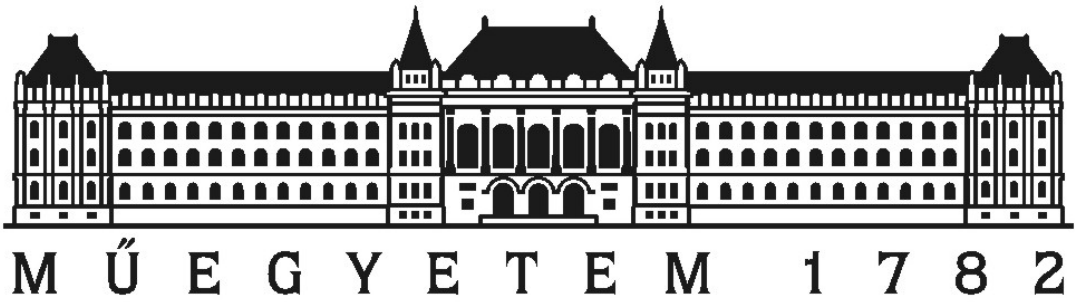


Nyilvános WiFi szolgáltatások biztonságos használata

Szerző: Gáspár Norbert

Konzulens: Dr. Fehér Gábor

2012

Tartalomjegyzék

1. Bevezetés 4

2. WPA PSK hátrányai 6

2.1 Otthoni hálózatokban 6

2.2 Publikus helyeken 7

3. WPA Enterprise előnyei, hátrányai 11

3.1 Vállalati környezetben 11

3.2 Otthoni megvalósítás 12

3.3 Nyilvános helyen 13

4. Captive Portal 15

5. Nyílt hálózat 16

6. Man In The Middle támadások 17

6.1 Adatlopás 17

6.2 ARP Poisoning 18

6.3 DNS Poisoning 20

6.4 Evil Twin 21

6.5 Rogue Access Point 22

6.6 Példák támadási fajtákra 22

6.7 Védelmi megoldások 24

7. WPS hátrányai, használhatósága 27

7.1 WPA PSK használata 27

7.2 WPA PSK használatának okai 27

7.3 Könnyen feltörhető PIN 27

8. Saját megoldás 29

8.1 Alapötlet 29

8.2 Ötletből adódó korlátok 29

8.3 ELŐNYÖK 30
8.4 MAN IN THE MIDDLE TÁMADÁSOK LEHETŐSÉGE 32
8.5 MEGVALÓSÍTÁS 34
8.5.1 Dinamikus adatok átvitele *35*
8.5.2 Statikus adatok átvitele *35*

1. Bevezetés

A jelenleg létező WiFi biztonsági megoldások nem nyújtanak megfelelő védelmet otthoni és kis üzleti felhasználók számára. Az adatforgalom lehallgatása ezeken a helyeken csak részben elkerülhető, vagy egyáltalán nem. A WEP titkosítás régóta köztudott, hogy gyakorlatilag nem nyújt semmilyen védelmet a felhasználók számára, hiszen már komoly szakértelem nélkül is vannak olyan szoftverek, amelyek képesek megfejteni a szükséges kódot, hogy aztán a támadó lehallgathassa az áldozat adatforgalmát. Ennek megfelelően létrejött a WPA, valamint a WPA2 titkosítás. A dolgozatomban ennek kétféle változatát vizsgálom meg. Egyrészről az otthoni, valamint kis cégek esetén használt változatot, a PSK-t. Másrészt a vállalati környezetre kifejlesztett Enterprise változatot. Biztonsági szempontból a kettő között fontos különbség, hogy míg az Enterprise megoldás esetén a felhasználók elől el van rejtve a többiek kommunikációja, addig PSK esetén erre a lehetőségek korlátozottak. További megoldást jelent a Captive portal, amikor egy gyakorlatilag nyílt hálózat használatához férnek hozzá a felhasználók egy jelszó beírása után. Ezen kívül kitérek dolgozatomban arra is, hogy a WPA által kínált védelem hogy alakult a WPS bevezetésével. A különböző lehetőségeket megvizsgálva arra jutottam, hogy a legegyszerűbben és a leghatékonyabban a nyilvános helyeken kínálható ingyenes WiFi használatánál lehetne javítani a felhasználók biztonságán, így a dolgozatomban megvizsgálok egy megoldást a nyilvános helyeken használt WiFi hálózatok titkosításával kapcsolatban, aminek a segítségével a felhasználók nem látják egymás forgalmát. Ezzel kiküszöbölhetik a nyilvános helyeken használható ingyenes WiFi szolgáltatások fő biztonsági gyengeségét. Ez a megoldás mobil eszközök hálózatra csatlakozását teszi lehetővé úgy, hogy egy szükséges tanúsítványhoz való hozzáférést biztosan garantál. Ezzel kapcsolatban megvizsgálom, hogy egy tanúsítvány átvitele elég lehet-e a biztonságos kapcsolat kialakításához, illetve ennek az átvitele hogyan lehetséges. Erre megoldás lehet egy NFC kártya, vagy QR kód. A dolgozatomban az ezek közti különbséget is megvizsgálom gazdaságossági, elérhetőségi szempontból, valamint áttekintve, milyen előnyökkel jár egyik, illetve másik, illetve statikus adat átvitelével ha lehet, akkor hogyan lehet kialakítani egy kielégítően biztonságos kapcsolatot. A dolgozatomban először kifejtem a jelenleg használatos főbb biztonsági megoldásokat, amiket vezeték nélküli hálózatok kialakításánál tudnak alkalmazni az ezért felelős szakemberek. A következő részben bemutatom azokat a támadási fajtákat, amik a legfőbb problémát jelentik vezeték nélküli hálózatok esetén, majd teszek egy kitérőt egy megoldásra, ami korábban már majdnem megoldotta az eddig biztonsági hiányokat. Szót ejtek arról a hiányosságról is ebben a

fejezetben, amit éppen ez a megoldás hozott a hálózati biztonság terén. Az utolsó fejezetben felvázolom a saját megoldásomat, ami megoldást jelent egy olyan biztonsági kockázatra, amit eddig csak részben tudtak kivédeni vezeték nélküli hálózatok tervezésénél. Kifejtem a megoldás részleteit, valamint hogy ez milyen esetekben és mennyit javít az eddigi megoldásokon.

2. WPA PSK hátrányai

2.1 Otthoni hálózatokban

A WPA PSK védelme azon az egyszerű feltevésen alapul, hogy létezik egy csak a jogosultak által ismert jelszó. Ennek a jelszónak a segítségével ők képesek felcsatlakozni a hálózatra, míg mások ennek a tudásnak a hiányában nem tudják használni az adott hálózati eszköz által nyújtott szolgáltatást. Kijelenthető, hogy ebben a hálózatban nem kell tartaniuk a felhasználóknak attól, hogy egy másik jogosult felhasználó lehallgatná az általuk generált adatforgalmat. Ennek egyszerű oka az, hogy egy családon belül nem valószínű, hogy valaki le akarja hallgatni a másik adatfogalmát. Ugyanakkor a jelszó ismerete elegendő biztosítékot adhat (megfelelően összetett jelszó használata esetén) arra, hogy csakis azok a felhasználók férjenek hozzá a hálózathoz, akik tényleg jogosultak erre. A WPA, illetve WPA2 titkosítások eddig csupán brute force módszerrel voltak feltörhetők. Ugyanakkor a dolgozatom írásának időpontjában a WPA jelszavak feltörése 84399548 szó/másodperc[1] sebességgel képes végigmenni egy könnyen elérhető videó kártya segítségével, amennyiben a vizsgálni kívánt jelszavakhoz tartozó hash kódokat előre legyártjuk. Bár ez elvárja, hogy az adott access point azonosítóját is ismerje a támadó, a gyakorlatban ezeknek a beállítása is sok esetben alapértelmezetten van hagyva. Ennek megfelelően már az access point SSID-jának megváltoztatása is jelenthet megoldást erre a problémára, hiszen ekkor sem lehet találni egy meglévő sablont az interneten, amit ahhoz az adott SSID-hoz gyűjtöttek össze. Viszont még ekkor is könnyen elő lehet állítani az adott azonosítóhoz egy újabb szivárvány táblát. Sok esetben így is gyorsabb lehet a hálózat feltörése, mert a szivárvány tábla előállításához szinte tetszőleges számítási kapacitással is rendelkezhet a támadó, amennyiben elosztottan, egyszerre akár több gépen is végzi ezt a műveletet. Mivel ráadásul ilyen táblázatok a leggyakoribb azonosítókhoz elérhetők az interneten, ezért innentől kezdve ezzel számolok. A 84 399 548 szó/másodperc sebességhez összehasonlításképp egy átlagos ember aktív szókincse nagyjából 3000-5000 szó[2]. A passzív szókincse egy átlagos embernek megközelítőleg 5000-10000 szó, és az egyes nyelvek beszélői is maximum 10-20 ezer szót használnak. Ez azt jelenti, hogy a jelszavak beállításának gyakori módját eltekintve (egy szó,

[1] http://www.academia.edu/1501652/GPU_-_accelerated_WPA_PSK_cracking_solutions

[2] http://hu.wikipedia.org/wiki/Sz%C3%B3kincsm%C3%A9retek_%C3%B6sszehasonl%C3%ADt%C3%B3_list%C3%A1ja

legfeljebb kiegészítve egy számmal) az otthoni hálózatok nagy részéhez tartozó jelszó könnyen visszafejthető már másodpercek alatt is. De 84 399 548 szó/másodperc sebességnél ha csak a teljesen brute force módszerrel végigvitt támadást is vesszük alapul (azaz nem tesszük fel, hogy értelmes szó a felhasznált jelszó), akkor is nagyjából 60-féle lehet egy karakter a jelszóban. Így egy 6 karakteres jelszó nagyjából tíz perc alatt kitalálható. Ugyanakkor a fő probléma ezekkel a – nem értelmes szóból kialakított – jelszavakkal, hogy természetükből adódóan nehéz őket megjegyezni. Egy hat karakteres véletlen generált jelszót például már nagyon kevés ember jegyezne meg, pláne amikor a beállítás után hónapokig nincs is rá szükség esetleg (hiszen a végberendezések képesek megjegyezni ezt a jelszót). Márpedig egy új eszköz vásárlásánál, vagy egy ismerős látogatása esetén szükség lehet erre a jelszóra. Ennek megfelelően megoldást jelenthetne ezt felírni valahová, de ez a papír elveszhet, vagy még inkább valaki észreveheti és felhasználhatja a – többnyire jól látható helyen tárolt – jelszót. Természetesen erre vannak bevált gyakorlatok, amik megkönnyítik a jelszóválasztást – ilyen például a jelmondat használata, amikor a felhasználó beállításkor nem egy szót, hanem egy egész mondatot ad meg, amit könnyen megjegyez. Hasonló, amikor egy központi jelszó által védett jelszógyűjteményben, védett helyen tárolja el a felhasználó az összes jelszavát. Így csak egyetlen komplex jelszót kell megjegyeznie, amit ennek megfelelően könnyebb észben tartania. Ugyanakkor ezekkel a legtöbb család a hálózat beállításakor nem foglalkozik, így a legtöbb esetben a támadónak csak egy könnyen kitalálható szót kell megfejtenie. Ezeknek a feltörése nagyságrendekkel gyorsabb, mint azonos hosszúságú véletlen karaktersorozatoké.

2.2 Publikus helyeken

A legfőbb problémát azonban nem az otthoni felhasználás jelenti. Ezekben az esetekben elegendő védelmet nyújthatna a fentebb említett legjobb gyakorlatok elterjesztése is, hogy több ember éljen ezekkel a módszerekkel. Így eléggé meg lehetne nehezíteni a támadók dolgát ahhoz, hogy ne legyen érdemes nekik elkezdeni a jelszavak végigpróbálgatását. Ugyanakkor mint már korábban is említettem, a WPA PSK titkosítást arra találták ki, hogy az otthoni hálózatok biztonságát tudja garantálni. Ennek megfelelően a megalkotásakor fontosabb volt a könnyű csatlakozás és használat, mint az, hogy a hálózat résztvevői ne lássák egymás forgalmát. Éppen emiatt az olyan helyeken, mint egy hotelben a legfőbb veszélyt az jelenti, hogy bármelyik felhasználó láthatja a többiek által generált adatforgalmat. Így a támadónak elegendő egyszer megszereznie – az egyébként minden vendég által könnyen elérhető – jelszót. Ezután megszerezheti a többi vendég jelszavait, bankszámlaadatait.

Egyszóval bármilyen beírt információt, amit az adott hálózaton kiad a védtelen felhasználó. Tovább súlyosbítja ezt a helyzetet, hogy a legtöbb ilyen nyilvános hálózathoz tartozó jelszót az első beállítás után nagyon ritkán, vagy soha nem változtatják meg. Így még csak ki sem deríthető később, ki hallgathatta le a többiek forgalmát. Ugyanis a támadó lehet, hogy csak hónapokkal azelőtt ivott meg ott egy kávét és a támadás időpontjában kilométerekre volt az adott helytől. Ugyan ott már nem elérhető alapvetően az adott vezeték nélküli hálózat, de szintén interneten rendelhetők olyan eszközök, amik több kilométer távolságról is biztosítják egy vezeték nélküli hálózat elérését. Ezeknek a segítségével nem kell a közelben lennie a támadónak. Bár csak egy bizonyos sugarú körből éri el a hálózatot még nagyon érzékeny berendezéssel is, ez már elég ahhoz, hogy ne kelljen közvetlenül a helyszínen tartózkodnia és így kiessen a vizsgált személyek köréből (például a hely biztonsági kameráin nem szerepel). Tehát ha később ki is derül, hogy hol történt az adatlopás, a támadó még csak nem is elérhető, hiszen kilométerekre van a helyszíntől. És magát a lehallgatást is könnyen véghezvitte, hiszen hozzáférést kapott az áldozat által generált forgalomhoz. Természetesen magasabb szinten is lehet védeni egy kapcsolatot. Azonban ezekre is csak korlátozott lehetőség áll rendelkezésre. Ezeket a lehetőségeket az 5.7 fejezetben fejtem ki bővebben. Ugyanígy, ha éppen a helyszínen van a támadó, egy mobiltelefonnal is képes lehet ellopni a bizalmas adatokat. Több ingyenesen elérhető program van már mobiltelefonokra is, amik automatikusan megvalósítanak például egy ARP Poisoning alapú támadást. A felhasználónak csak le kell töltenie egy ilyen programot (ingyenesen) és a program az indítása után automatikusan megcsinál mindent. A felhasználó ezután meg tudja tekinteni a számára fontos információkat, anélkül hogy az áldozat ebből bármit is érzékelt volna. Ilyen programokról az 5.6 fejezetben még lesz szó, bemutatva, milyen egyszerűen is kezelhetők. Ezeken a helyeken a hálózat jelszóval történő védelme csupán azt a célt szolgálja, hogy kizárólag a vendégek férjenek hozzá a hálózathoz. Ez a védelem semmit nem ad maguknak a felhasználóknak, akik kvázi védtelenek maradnak a támadásokkal szemben. Itt kell felhívni a figyelmet arra a hamis biztonságérzetre is, amit a vendégek éreznek a jelszó beírása után. Teljesen jogosan várják el, hogy miután megadtak egy titkos kódot, a kommunikáció amit megvalósítanak, ne lehessen elérhető senki más számára. Ez a hamis biztonságérzet pedig tovább növeli annak a valószínűségét, hogy egy átlagos felhasználó olyan oldalakat nyisson meg, amikhez kulcsfontosságú lenne, hogy egy támadó ne férjen hozzá. Így például egy bankszámlát, vagy e-mail fiókot. Ezeket ugyan védik a megfelelő magasabb szintű titkosítások (HTTPS, IMAPS). De ezek kijátszhatók úgy, hogy a felhasználó csak egy-két apróbb változást érzékeljen a normál működéshez képest. Így például el lehet hitetni az áldozattal, hogy új

tanúsítványa van az általa ismert oldalnak, vagy hogy az adott weboldal titkosított forgalommal működik, miközben valójában nem. Bár a bankszámlák nagy részénél egy plusz biztonsági szolgáltatás, hogy küldenek egy sms-t egy jelszóval, amit az ügyfélnek be kell írnia az internetes felületen, utalás előtt. Sok helyen ez azonban nem feltétlenül van így. Ráadásul egy e-mail fiók esetén ez nem is áll fenn, ennek elérésével pedig végtelen lehetőséget nyit a támadó arra, hogy megszemélyesítse az áldozatot.

Márpedig jelenleg ha egy nyilvános WiFi hálózat védelmét WPA titkosítással szeretné valaki megoldani, akkor sok esetben ezt a PSK titkosítással oldják meg, hiszen ezt egyszerűbb beállítani és olcsóbb is. Emellett az Enterprise megoldást sem erre találták ki, így ez sem igazán a szükséges védelmet garantálja. Ez már ugyan elkülöníti a felhasználók adatforgalmát, de a kommunikáció kezdetén meg kell osztania egy egyéni kódot a felhasználóval, ami így lehallgatható. Erre létezik olyan megoldás, amikor a blokkra nyomtat a pénztárgép egy jelszót, amit beírva a felhasználó tudja használni a hely által biztosított internetet. Ezzel egy időben a pénztárgép a jelszót elküldi egy RADIUS szervernek, ami azért felelős, hogy csak a megfelelő jogosultsággal rendelkező felhasználók férjenek hozzá a hálózathoz. Ugyanakkor egyrészt a blokkon lévő kódot egy ügyesebb támadó is megszerezheti, másrészt ez még mindig nem nyújt megoldást arra nézve, hogy mi van, ha a támadó szintén egy ottani access pointnak adja ki magát. Ez az evil twin jellegű támadás ugyanígy működhet ebben az esetben, hiszen a támadó egyetlen dolga, hogy létrehozzon egy ilyen hálózatot, ami minden jelszót elfogad. Még ha küld is tanúsítványt a felhasználónak, annak hitelességét a felhasználó nem igazán tudja ellenőrizni. Az Enterprise lehetőséget nyújt arra is, hogy a hálózat lefedettségi körén belül elnémítson minden vele azonos SSID-val rendelkező hálózatot azáltal, hogy jelzi a felhasználónak, hogy az a hálózat nem megbízható. Ezzel ugyanakkor nem oldja meg a problémát, hiszen ha a támadó szintén nem megbízhatónak állítja be az eredeti hálózatot, akkor csak egy patt helyzet alakult ki, a felhasználó vagy egyikhez sem tud csatlakozni, vagy kényszeríti a végberendezését, hogy az egyikre csatlakozzon. Ugyanakkor ezzel megint csak nem oldódott meg a probléma, hiszen nem tudhatja, melyik hálózat az igazi. Mivel napjainkban már alapelvárás bármilyen vendéglátó egység esetében egy ilyen hálózat kiépítése, így fontos lenne, hogy garantálható legyen a biztonságos kommunikáció minden ilyen hálózatra csatlakozó felhasználó számára. Mivel ennek a megoldása kulcsfontosságú lenne és maga a megoldás nem túl költséges, valamint könnyen hozzáépíthető bármilyen meglévő hálózathoz, így ennek a problémának a megoldását választottam dolgozatom fő témájának. A támadási fajták összefoglalása az 1. táblázatban található:

1. Táblázat:

Támadás típusa / Hálózat védelme	Nyílt hálózat	WPA PSK	WPA Enterprise
Adatlopás	X	X	
ARP Poisoning	X	X	
DNS Poisoning	X	X	
Evil Twin	X	X	X
Rogue Access Point	*	*	*

** Rogue Access Point támadásnál a támadó minden forgalmat lát és irányít, hiszen övé a hálózat. Ez ellen az egyetlen védekezési módszer, ha nem kapcsolódik rá a felhasználó ilyen hálózatra.*

X: WPA esetén akkor feltörhetők a bejelöltek, ha a támadó előtte hozzáférést szerzett a hálózathoz.

3. WPA Enterprise előnyei, hátrányai

3.1 Vállalati környezetben

A WPA Enterprise számos előnye közül a legfőbb, hogy minden felhasználó saját kulccsal kommunikál. Ugyanakkor ennek megvan a maga hátulütője is. Ilyen hátulütője, hogy a kulcs kiosztását megelőzően a vállalat informatikai felelősének (tipikusan rendszergazdájának) feladatai közé tartozik a felhasználók eszközeinek kézzel történő beregisztrálása. Miután az eszközöket a rendszergazda beregisztrálta, a felhasználók ezeket könnyen tudják használni. Még jelszó beírása sem szükséges a későbbiekben, hiszen minden felhasználó egy véletlen generált jelszót kap, aminek a használatával szabadon használhatja a vezeték nélküli hálózatot. Ahogy korábban is írtam, vannak más megoldások is a végberendezések beregisztrálására. Az automatizált beregisztrálás például a fenti blokkon adott jelszó esetében megoldható. Ugyanígy, történhet tanúsítvány cserével is a felhasználók felvétele. Ekkor jelszóra nincs szükség, mindkét fél a saját privát kulcsával és az előre egyeztetett publikus kulccsal oldja meg a kommunikációt. Az Enterprise megoldásnak természetesen komoly hátránya, hogy a vállalatnak rendelkeznie kell egy hozzáértő rendszergazdával, aki képes a hálózatot megfelelően beállítani. De miután ez megtörtént, a hálózatot bármelyik eszköz biztonságosan tudja használni. Ezzel szemben bár a PSK-t könnyebb beállítani, de az semmiképp nem oldja meg a biztonsági problémákat. A WPA, illetve a WPA2 titkosítás használatával ez a megoldás garantálja, hogy a hálózaton lévő felhasználók nem látják a többiek által generált adatforgalmat. Ezen kívül maga a WPA és WPA2 titkosítás a véletlen generált jelszóval egy biztosabb védelmet nyújt külön-külön is a felhasználóknak a külső támadókkal szemben is, mint az otthoni használatra kifejlesztett társa, a PSK. Ennek oka pont a korábban részletezett szótáron alapuló támadások gyakorisága, amikor azon alapul a támadás, hogy a jelszó nyilván egy értelmes szóból lett képezve. Mivel ez itt nem áll fenn, így az összes lehetőséget végig kell próbálni. Mivel a véletlen generált jelszót még csak meg sem kell jegyeznie a felhasználónak, így a jelszó lehet tetszőlegesen hosszú is. Ennek eltárolása nem jelent problémát még mobil eszközök esetén sem, hiszen nagyságrendekkel nagyobb tárolókapacitásokkal rendelkeznek a legegyszerűbb okos telefonok is, mint amire szükség van egy ilyen kód eltárolásához. Mivel nagyvállalati környezetben nem jelent problémát egy rendszergazda felvétele, így joggal állítható, hogy ez a védelem megfelel annak, amit egy ilyen hálózattal szemben elvárhatnak a felhasználók. Természetesen ezekben az esetekben sem szabad megfeledkezni arról, hogy egy esetleges látogatónak is lehet szüksége internetes

elérésre. Azonban ezekre az esetekre a bevett gyakorlat, hogy kialakítanak egy a Vállalat területén belül elérhető nyilvános hálózatot. Ugyan ezzel nem védik jobban a betérő látogatókat a támadások ellen, amennyiben azok használni szeretnék az internetet, mint amennyire egy kávézóban lennének védve. De egy minimális védelmet mégis jelent ez is, valamint ezeknél a hálózatoknál sok esetben az nyújtja a védelmet, hogy fizikailag nem elérhető külső használóknak az ehhez szükséges jelszó, vagy a hálózati eszköz hatósugara le van korlátozva az épület belsejére. Így csak azok láthatják ezt a forgalmat, akik ténylegesen betérnek ezekhez a cégekhez. Ők viszont könnyen nyomon követhetők. Valamint a fő szempont nyilvánvalóan az a cégeknek, hogy a saját, valamint a munkavállalóik adatai legyenek biztonságban. Így ezen a területen nem is találtam lehetőséget arra, hogy a már kialakított biztonsági lehetőségeket fejlesszem. Ez alól kivételt képezett a különböző IPS (Intrusion Prevention System) megoldások további fejlesztése. Jelenleg az Enterprise megoldások esetén ezen védelmi mechanizmusok megvalósítása jelenti a kihívást. Itt azt a biztonsági hiányosságot vizsgálják a vezeték nélküli hálózatok kialakításával foglalkozó cégek, hogy a vezeték nélküli hálózat mindenki által elérhető, így az azon küldött adatok módosíthatók is. Ennek megfelelően olyan mintákat keresnek a rádióhullámú jelekben, amik támadásra utalhatnak és ezeket próbálják meg jelezni. Ezzel komoly cégek tapasztalt munkavállalói foglalkoznak, így ebben nem éreztem lehetőséget, hogy érdemi újdonságot tudjak megvalósítani. Természetesen ahogy az elkészített megoldásom kiegészíti a nyilvános helyeken kínált vezeték nélküli szolgáltatások biztonságát, úgy ez itt ugyanúgy bevezethető a vendégek számára. De ez lényegét tekintve nem módosítja a meglévő megoldást a vállalat munkatársainak szemszögéből.

3.2 Otthoni megvalósítás

Amikor valaki megpróbálja beállítani az otthoni hálózatát, sok hálózati eszközön választhat az otthoni, valamint a vállalati környezetre kifejlesztett WPA titkosítás között. Így felmerül a kérdés, hogy amennyiben tényleg biztonságosabb a vállalati megoldás, miért nem azt alkalmazzák az otthoni hálózatok esetén is? Természetesen ez ilyen esetekben nem megoldható. Egyrészt egy család nagyon ritkán tart fenn külön szervert, ami szükséges az Enterprise változat kialakításához. Emellett ez azt is jelentené, hogy minden egyes új vezeték nélküli internetezésre alkalmas készülék beüzemelésekor le kellene ülnie valamelyik családtagnak (vagy egy számítógépes szakembert kellene kihívni), aki beállítaná a hálózatot, hogy onnantól kezdve az új eszközt is felismerje. Ezen kívül minden új vendégnek is hasonlóan kellene hozzáférést biztosítani. Ha pedig a végberendezések automatikus

beregisztrálását elvégző hálózatot szeretnének kialakítani, akkor komoly összegeket kell kifizetniük a hálózat kiépítéséért és később karbantartásáért. Továbbá mint korábban ki lett fejtve, itt maga az Enterprise megoldás előnye nem igazán érződne. Ennek fő oka, hogy az általa nyújtott plusz védelemre ebben a helyzetben nincs szükség. Egy otthoni hálózat esetén nem kell attól tartani, hogy a hálózat többi használója esetleg rosszindulatú támadó lenne, aki vissza akar élni az ellopott információkkal. Így egy Enterprise jellegű megoldás bevezetése itt túlzott adminisztrációt igényelne anélkül, hogy további komoly előnyökhöz juttatná a hálózat használóit. A gyenge jelszó miatti kockázatot még mindig egyszerűbb kezelni egy hosszabb, összetettebb jelszóval, mint egy olyan megoldással, amihez egész vagyonokat kell költeni újabb informatikai berendezésekre, nem is beszélve a szakértelemről, amire szükség lenne ennek a kialakításához. Ez csak további kiadásokat jelentene egy átlagos család számára, hiszen egy megfelelő szakértőt kellene megfizetni, tekintve hogy a legtöbb családban nincs egy az informatika ezen ágához komolyabban értő családtag. Ilyen összeget egy átlagos család nyilvánvalóan nem fizetne ki azért, hogy ne kelljen megjegyezni egy hosszabb jelszót. Éppen ezért ebben a környezetben határozottan jobb megoldást nyújt a PSK változat, amit egy informatikus könnyen és gyorsan beállít, onnantól pedig egy jelszó megjegyzésével egyszerűen tudja használni a család minden tagja a beállított hálózati eszköz szolgáltatását.

3.3 Nyilvános helyen

A fenti két változat közül mindkettőre ki lett fejlesztve egy-egy megoldás. Míg a vállalati környezetre az Enterprise, addig az otthoni felhasználásra a PSK. Ugyanakkor egy környezetet egyik sem fed le biztonságosan. Ezek a nyilvánosan elérhető WiFi hálózatok. Ezeken a helyeken ugyanis a fő probléma nem az, hogy a felhasználóknak bizonyítaniuk kell a megbízhatóságukat, hanem éppen fordítva. Itt a hálózatnak kell biztosítania a felhasználót arról, hogy az maga a megbízható hálózat. Bár a jelenlegi védelmek megfelelnek annak a célnak, hogy a különböző kávézók, gyorséttermek lekorlátozhassák a hálózatot annyira, hogy csak a vendégek használhassák azt, a felhasználókat itt nem megfelelően védik és éppen ezért az itteni internet használat továbbra is veszélyes mindenkinek, aki bármilyen személyes adatot ad meg ezeken a helyeken. Ugyanakkor az sem várható el, hogy a felhasználók ne adjanak meg semmilyen személyes adatot, mint például a jelszavukat ezeken az oldalakon, hiszen sok oldal csak bejelentkezés után érhető el. Így például egy nyilvános levelezőrendszer, amit teljesen érthető, ha a vendég meg szeretne nyitni. Ebből látható, hogy ezeken a helyeken a meglévő megoldás közel sem kielégítő. Éppen ezért fontosnak tartom, hogy a nyilvános helyeken elérhető vezeték nélküli hálózatok biztonságára szülessen egy új megoldás. Ennek

nyilvánvalóan nem arra kell fókuszálnia, hogy csak a jogosult felhasználók férjenek a hálózathoz (amellett, hogy ennek biztosítása továbbra is megoldható, egy erre beállított Enterprise megoldással). Sokkal inkább azt a problémát kell megoldani, hogy a felhasználók megbízhassanak a hálózatban, amihez csatlakoznak. Erre teszek a későbbi fejezetekben ajánlást egy saját megoldás alapján. A megoldásom kifejezetten azon hálózatok biztonságának kialakítását teszi lehetővé, ahol a hálózatra gyakran csatlakoznak fel ismeretlen vendégek, akik egymást sem ismerik, így nem bízhatnak meg egymásban. Ezekben az esetekben a meglévő megoldás helyett (hogy kénytelenek mégiscsak megbízni egymásban) egy olyat ajánlok, aminek a segítségével a különböző felhasználók által generált forgalom elkülönül teljes egészében, elrejtve minden felhasználó kommunikációját a többiek elől. Ezen kívül biztosítható, hogy a felhasználó valóban ahhoz a hálózathoz csatlakozzon, amit az adott helység üzemeltet. Ennek a megoldásnak az alapelképzelése és megvalósítása a 7. fejezetben található.

4. Captive Portal

A WEP, valamint WPA titkosítások mellett létezik egy ezektől eltérő jellegű védelem is hálózatok esetén. Ez Captive portal névre hallgat. A lényege az, hogy alapvetően hozzáférést biztosít minden felhasználónak egy nyilvános hálózaton. Ugyanakkor az internetezéshez először be kell írni egy jelszót egy webes felületen. Ez a lehallgatás jellegű támadások esetén hasonlóan a WEP és WPA titkosításokhoz, nem nyújt semmiféle védelmet a felhasználóknak a többi hálózatra jogosulttal szemben. Otthoni felhasználása nem gyakori, hiszen hasonlóan a WPA Enterprise megoldáshoz itt is szükségesek egyéb informatikai eszközök a kapcsolat kialakításához. Nagyvállalati környezetben előfordul, de inkább csak a vendég felhasználók bejelentkezését szokták így megoldani, hogy egyszerűbb legyen ezeknek a felhasználóknak a beregisztrálása, ne kelljen a WPA titkosított hálózatra csatlakozniuk. A nyilvános hálózatok esetén a legfontosabb a használhatóságuk ezeknek a hálózatoknak, hiszen erre nincs kialakítva külön biztonsági módszer, ellentétben az otthoni és üzleti részekkel. Mivel azonban a bejelentkezés után a felhasználók ugyanúgy látják az egymás által küldött adatokat, mint ahogy nyílt, vagy WPA titkosított hálózatokban, így a lehallgatások ellen ez sem nyújt plusz védelmet. További lehetőség lenne, hogy a jelszó bevitelekor szét lehetne választani a felhasználók kommunikációját úgy, hogy mindenki különböző jelszót ad meg és onnantól kezdve ezt használva kommunikálhat. Így ugyan szét lennének választva a felhasználók, de egyrészt nem lehetne korlátozni azt, hogy kinek a kapcsolódását fogadja el a rendszer (hiszen bármilyen jelszót beírhat bárki), másrészt így minden felhasználó kulcsa látható lenne, csak a kapcsolódáskor kellene lehallgatnia a kommunikációt a támadónak. Onnantól pedig ő is tisztában lenne az áldozat által használt jelszóval. További problémát jelentene ezen kívül, hogy a bejelentkezési oldalt is meg lehetne hamisítani, így egyből a támadónak küldené el a felhasználó a jelszavát.

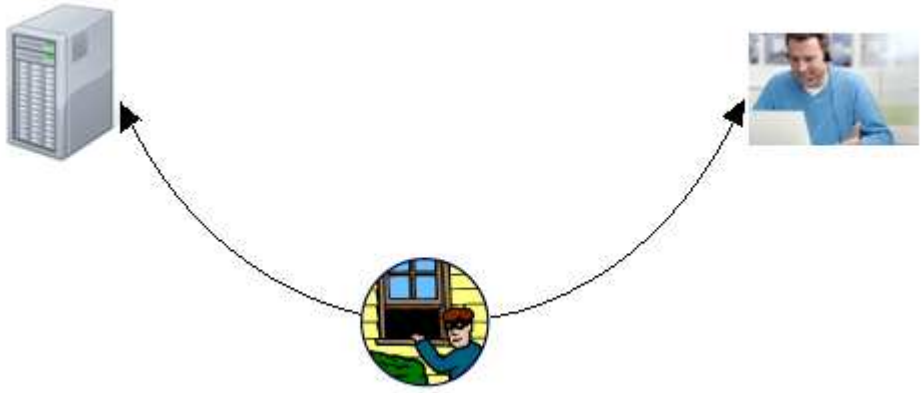
5. Nyílt hálózat

A WEP titkosítással védett hálózatokat egy kategóriába lehet sorolni a teljesen nyílt hálózatokkal, hiszen ma már egy mobiltelefonnal is könnyen feltörhetők ezek a hálózatok. Természetesen mivel maga a WEP titkosítás nem nyújt ilyen formában semmilyen védelmet – egész pontosan annyi védelmet nyújt, hogy a feltöréséhez kell egy letölthető program, így előbb ezt be kell szereznie, vagy meg kell írnia a támadónak. Mivel semmilyen gyakorlati védelmet nem nyújt a felhasználónak, így a dolgozatomban a továbbiakban nem is foglalkozok vele.

6. Man In The Middle támadások

6.1 Adatlopás

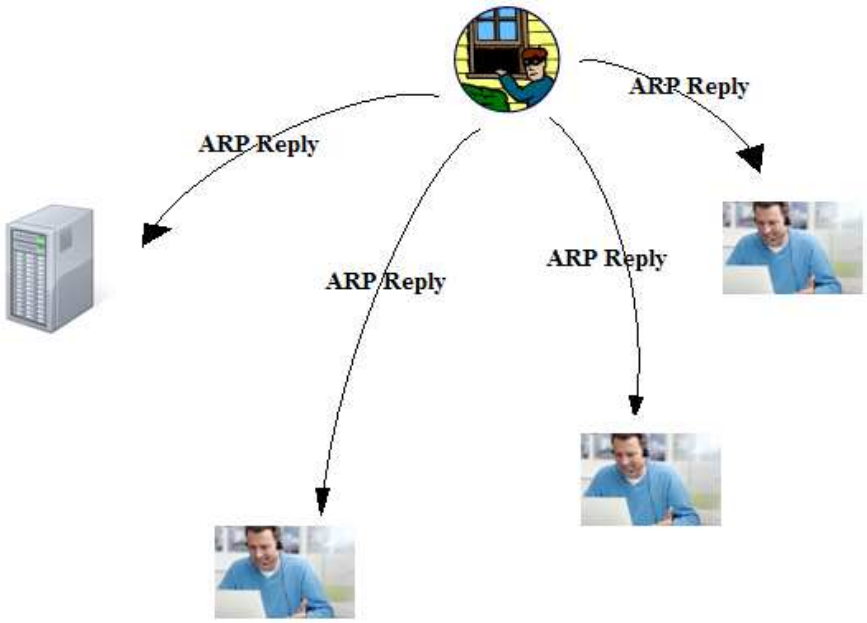
A Man In The Middle (továbbiakban MITM) jellegű támadásoknak legtöbb esetben az adatlopás a céljuk. Ezen fajta támadások közös pontja, hogy a támadó beáll az áldozat és a hálózati eszköz közé és a köztük lévő adatforgalmat lehallgatja. Ily módon tudomást szerez mindarról a kommunikációról, amit az áldozat folytat. Ennek a fő haszna a támadó szempontjából az, hogy az áldozat sokszor bizalmas információkat küld át a hálózaton, vagy éppen olyan információt, aminek az ismeretében fontos bizalmas információkhoz lehet hozzáférni (például a bankszámlájához tartozó jelszót). Ennek a fajta támadásnak a gyakorlatban sokféle megvalósítása létezik. A legegyszerűbb esetben a támadó egyszerűen lehallgatja a kommunikációt például egy vezeték nélküli hálózati eszköz és az áldozat számítógépe között (lásd 1. kép). Ilyenkor minden további tevékenység nélkül, egyszerűen nézi a hálózaton történő adatfogalmat és a számára szükséges információkat lehallgatva megszerzi a számára szükséges adatokat, így még MITM támadásnak sem lehet nevezni kifejezetten. Ez tipikusan olyan esetekben működik, amikor semmilyen védelem nem áll rendelkezésre a hálózat használói számára. Ilyen szempontból védelemnek tekintjük a magasabb szinteken lévő titkosításokat is, például a https protokoll használatát. Mivel a legtöbb oldalon ami bizalmas információt kezel már létezik legalább egy https jellegű védelem, így csak meglehetősen kevés esetben fordul elő, hogy a támadó tényleg fontos információt tud szerezni ilyen módon. Ennek megfelelően a továbbiakban bonyolultabb támadási módszereket ismertetek, amik a gyakorlatban többször előfordulnak és amik több esetben is használhatóak.



1. ábra: Adatlopás

6.2 ARP Poisoning

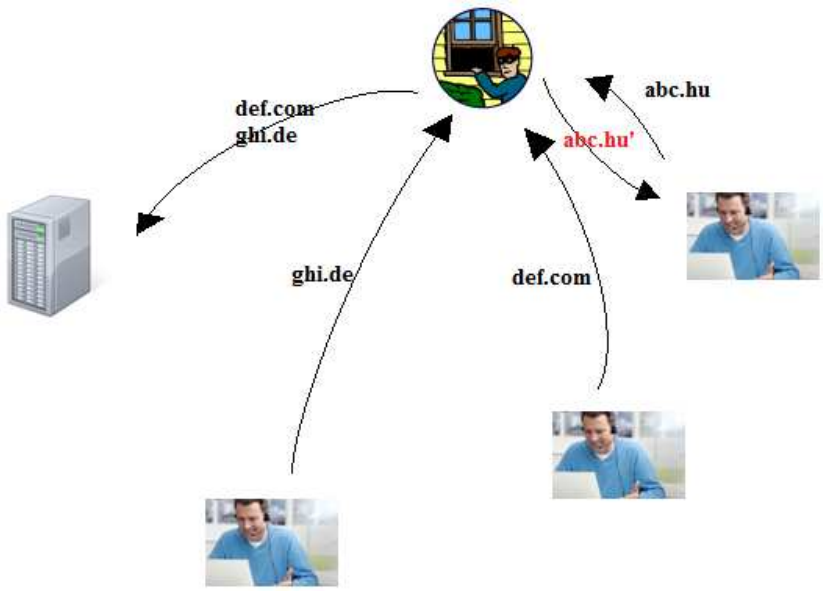
Az ARP Poisoning napjaink talán legnépszerűbb eszköze a MITM jellegű támadások kivitelezésének első lépésére. Ennek fő oka, hogy könnyen megvalósítható. Emellett a mobil eszközökre jelenleg nem igazán van elérhető védelem ilyen támadások ellen, ráadásul a számítógépek is csak korlátozott mértékben képesek észrevenni az ilyen adatlopási próbálkozásokat. A védelem hiánya nagyrészt pont a MITM támadások fő sajátosságából következik. Mivel az emberek nagy része általában otthonról, vagy a munkahelyéről használja a számítógépét, ezért ezeket a támadásokat távolinak érzik. Ugyanakkor az emberek nagy része bár legtöbbször valóban otthonról használja a számítógépét (vagy a munkahelyéről), időnként felkapcsolódik egy-egy nyilvános hálózatra is. Ilyenkor viszont ugyanúgy nincs védve az adatforgalma, hiszen „úgysem pont akkor fognak tőle adatot lopni”. Ez a gondolatmenet természetesen helytelen, hiszen bizonyos információkat elég, ha egyszer megszerez egy rosszindulatú támadó. Így hiába van védve a felhasználó otthoni és munkahelyi internetes kapcsolata, amit az idő 99 százalékában használ. Ugyanis közben a maradék egy százaléknyi időben ugyanúgy elérheti a támadó ezeket az információkat. A támadó szempontjából a helyzet pedig még ennél is jobb. Hiszen neki nem vakon kell találgatnia, hogy mikor történik meg az az egy százaléknyi idő, amikor a felhasználó nem biztonságos kapcsolatot használ. Ő pontosan tudja, hogy az áldozat akkor nincs védve, amikor egy nyilvános hálózatra felcsatlakozik. Így a támadó szempontjából az egyetlen nehézség azt megtalálni, hogy hová érdemes mennie, ahol feltehetőleg több számára érdekes információt fognak forgalmazni. Így például egy olcsóbb hotel hálózatán nem feltétlenül van olyan lehetősége sokat érő bizalmas adatokat szerezni, mint egy felkapott kávézóban. Az ARP Poisoning támadás pont ezt a lehetőséget használja ki. Míg egy sima adatlopás esetén megfelelő védelmet nyújt egy https titkosítás, addig az ARP Poisoning segítségével elindítható egy olyan támadás, aminek során a támadó kikényszeríti, hogy a https forgalom helyett http forgalom történjen a szerver és a felhasználó végberendezése között, vagy akár saját maga is meghamisíthatja az adott weboldalt, így a felhasználó nem a valódi weboldalon írja be a jelszavát, hanem a támadó által előre elkészítetten. Ennek segítségével a támadó meg tudja szerezni a felhasználó bizalmas adatai. Beleértve a bankszámlákhoz tartozó jelszót, vagy az e-mail fiók jelszavát is. A támadás lényege egyszerű. Első lépésben elterjeszti a hálózaton, hogy valójában rajta keresztül folyik az adatforgalom (2. kép).



2. Ábra: ARP válaszok terjesztése a hálózaton

Mivel innentől kezdve az ő címére küldi minden felhasználó az adatot, neki már csak annyi dolga van, hogy a számára nem fontos kéréseket továbbítsa a hálózati eszköz felé, nehogy feltűnjön a többi felhasználónak, hogy a hálózat nem a szokványos módon működik. Amennyiben van annyi számítási kapacitása a támadó eszközének, hogy ezeket a kéréseket továbbítani tudja, akkor feltűnés nélkül képes lehallgatni minden felhasználó kommunikációját. Mivel manapság elég egy modernebb mobiltelefon is egy viszonylag nagy méretű hálózat kezeléséhez, így ez a támadás egyre inkább előtérbe kerül. Természetesen innentől kezdve ha mindenki megbízik a hálózatban és használja azt a támadón keresztül, akkor a támadó a következő lépésben tetszőlegesen manipulálhatja az áldozat adatforgalmát, elhitetve vele, hogy az általa kívánt weboldallal kommunikál. Közben ugyanakkor egy a támadó által előre elkészített oldalt használhat akár (lásd 3. kép). Mivel a támadható weboldalak listáját le lehet korlátozni, ezeknek a másolatait a támadó előre elkészítheti, a saját változtatásaival kiegészítve is. Így például egy általa kiválasztott bank oldalát módosíthatja olyan módon, hogy a jelszó beírása után az elsőként ne a banknak küldje el a titkosított jelszót, hanem előtte a támadó készülékére küldje el a bankszámlaszám, jelszó párost. Ebben az esetben természetesen a későbbiekben bármikor beírhatja ezeket a támadó a tényleges oldalon, ahol így hozzáférést szerezhet az áldozat számlájához. Mint korábban írtam, természetesen ez ellen védelmet jelenthet a sok banknál használt sms jelszó védelem pont úgy, mint a https kapcsolat kikényszerítése a szerver részéről. Ez azt jelenti, hogy a számlához történő hozzáférést csak akkor engedélyezi a bank, ha a felhasználó beír egy számára sms-ben kiküldött kódot is. A telefonszámot legtöbb esetben a bankszámla létrehozásakor kell

megadni, így a felhasználó védve érezheti magát. Ugyanakkor ez a telefonszám telefonon keresztül is módosítható sok bank esetében. Amennyiben a támadó megszerzi a banki jelszó mellett akár csak az e-mail jelszavát is a felhasználónak, hihetetlen mennyiségű adatot tudhat meg az áldozatról anélkül, hogy bárkiből csellel kellene azt kihúznia. A telefonon történő azonosításnál feltett kérdéseket így könnyen meg tudja válaszolni, hogy aztán a telefonszámot személyes találkozás nélkül is meg tudja változtatni. A https hiányosságairól pedig az 5.7 fejezetben írok részletesebben. Bár sokféle támadási módszer létezik, a fenti eset egy meglehetősen egyszerű és könnyen elképzelhető problémát tár fel, amelyben a támadó csupán egy kávézóban üldögélve, majd egy pár órányi kutatómunka után akár egy nagyobb összeget is átutalhat az áldozat számlájáról. Természetesen ezen kívül is van többféle támadás, attól függően, hogy a támadó milyen adatokat akar megszerezni, illetve milyen módon kívánja ezt megtenni.



3. Ábra: A támadó csak az általa kiválasztott oldalt hamisítja, a többi üzenetet továbbítja

6.3 DNS Poisoning

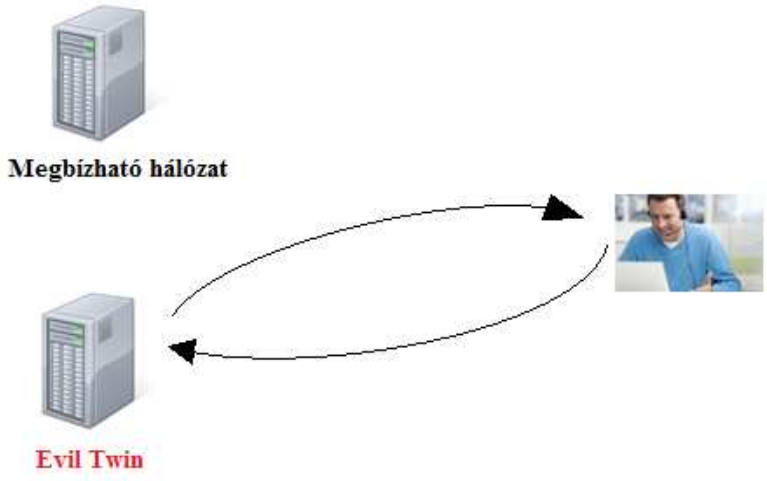
A DNS Poisoning nem olyan népszerű támadási forma, mint az ARP Poisoning. Mindazonáltal működése alapelvében hasonlít a fentiekben részletezett változathoz. A segítségével elérhető eredmények is nagyrészt megegyeznek az ARP-s változatéval. A kettő közti különbség, – ahogy a neve is mutatja – hogy míg az ARP Poisoning esetében az ARP táblákat tölti meg a támadó a hamisított információval, addig DNS Poisoning esetén a DNS listákat írja át. Így például elérhető, hogy egy bank internetes címet beírva az áldozat ne ténylegesen a bank oldalának IP címét kapja meg, hanem a támadóét. Ebben az esetben

természetesen szintén el tudja lopni a számára szükséges adatokat a támadó, akár a fentiekben vázolt ál weboldal elkészítésével is. Az ARP és DNS Poisoning támadások ezzel együtt kimutathatók a hálózati forgalom analizálásának segítségével is. Erről és további védelmi megoldásokról az 5.7 fejezetben lesz szó bővebben.

6.4 Evil Twin

Ennek a támadásnak a neve azt jelenti, „gonosz iker”. Ez a név jól jelzi a támadás lényegét. Evil Twin támadásnál a támadó az igazi hálózati eszköz helyébe igyekszik lépni. Ezt úgy teszi meg, hogy lemásolja annak az azonosítóját. Mivel az áldozat csak annyit lát, hogy annak az eszköznek is ugyanaz a neve, ezért joggal gondolhatja, hogy az eredeti hálózati eszközt látja. Éppen ezért csatlakozik hozzá és innentől kezdve minden adatforgalom a támadó készülékén megy keresztül (lásd 4. kép). És míg egyes esetekben gyanús lehet a felhasználónak, hogy a megszokott egy helyett kettő hálózati eszközhöz csatlakozhat, a probléma azokban az esetekben áll fenn igazán, amikor egyébként is több hálózati eszközhöz lehet csatlakozni. Ez a helyzet áll fenn például az egyetemi hálózat esetében is, ahol majdnem mindenhonnan több hálózati eszközre is rá lehet látni. Ilyen esetben például teljesen észrevehetetlen tud lenni egy Evil Twin támadás, hiszen lehet, hogy néhány centi eltéréssel egyik helyen kettő, másik helyen pedig három hálózati eszközre lehet rálátni. Ugyanakkor ha az SSID-t is lemásolja (azaz tényleg minden paraméterét a hálózatnak), akkor még ennyi sem fog látszani, csupán hogy több csatorna van. Ez azonban nem derül ki, csak ha alaposabban megvizsgálja a felhasználó a kapcsolatot. Ilyen esetben az, hogy a harmadik eszköz adott helyzetben a támadó által kínált csatlakozási lehetőség, vagy egy megbízható, az egyetem által biztosított eszköz, nehezen, vagy egyáltalán nem eldönthető az áldozat szemszögéből. További problémát jelent, hogy még ha észre is veszi a támadást, kénytelen választani a két eszköz közül, ha hozzá akar férni az internethez. Ebben az esetben kénytelen megrizikózni azt, hogy esetleg ellopják az adatait. Hiszen a másik verzió, hogy például nem nézi meg az e-mailjeit. Feltéve hogy célja volt az internetre csatlakozással, nagy az esélye, hogy egy bejelentkezést végrehajt. Ha ez a támadón keresztül történik, akkor a támadó ahhoz a fiókjához már hozzáfér az áldozatnak a későbbiekben. És egy olyan esetben amikor a felhasználó kénytelen megnézni ezt a fiókot, akkor ötven százalék az esélye, hogy a két eszköz közül azt választja ki, amelyik a támadónak küldi az adatokat. A fentieken kívül Evil Twin jellegű támadás az is, amikor a támadó lemásolja egy hálózati eszköz azonosítóját, majd kicsit arrébb viszi a készülékét és ott biztosít internetes hozzáférést a felhasználóknak. Ezekben az esetekben ahol ő szolgáltat internet elérést, ott csak az ő hálózata elérhető. Így azáltal, hogy – például az egyetemi

példánál maradva – egy épülettel arrébb (de még az egyetem területén) biztosít egy BME nevű WiFi hozzáférést, biztosra veheti, hogy aki ott akar felcsatlakozni az internetre, az rajta keresztül fogja ezt megtenni. Természetesen ezt továbbra is ki lehet védeni valamilyen szinten azzal, ha a felhasználó tudja hogy az adott épületben biztosan nincsen internetezésre lehetőség. De ezzel a felhasználók nagy része természetesen nincs tisztában. Sőt, ez történhet úgy is, hogy egy hálózati eléréssel rendelkező épülethez közel szolgáltat internetezési lehetőséget a támadó. Ilyenkor kimondottan hiheti azt az áldozat, hogy csupán néhány méterrel távolabbról még elérhető a hálózat. És nehéz megmondani, hogy milyen távolságról bízhat még meg az egyetemi hálózatban.



4. Ábra: A felhasználó a támadó által kínált hálózatot használja

6.5 Rogue Access Point

Rogue Access Pointnak nevezzük azt a támadási fajtát, amikor a támadó egy internettel nem lefedett helyen kínál lehetőséget hálózatra történő csatlakozásra. Ebben az esetben abban reménykedik, hogy az áldozat az ingyenes internetezési lehetőséget kihasználva onnan nézi meg a postafiókját, vagy ott használ egyéb bejelentkezést igénylő oldalakat. Ilyenkor az Evil Twin-hez hasonlóan, hálózati eszközt személyesít meg a támadó. A két támadás közti egyetlen lényeges különbség, hogy míg az Evil Twin sok esetben észrevehetetlen támadási mód, addig a Rogue Access Point jellegű támadásokat könnyen kivédhetjük, ha csak megbízható helyen kapcsolódunk vezeték nélküli hálózathoz.

6.6 Példák támadási fajtákra

A fenti támadási fajtákat bárki meg tudja valósítani, akinek van némi tapasztalata hálózati kártyák programozásában. E tudás birtokában már okos telefonokra is képes lehet bárki egy

megfelelő szoftver írására, így még egy számítógépet sem kell magával vinnie a megfelelő nyílt hálózat lehallgatásához. Amennyiben megfelelően automatizáltra írja a szoftvert, annak kezelése akár úgy is megoldható, hogy ki se veszi közben a zsebéből. Természetesen ez igényel némi szakértelmet, aminek nem mindenki van birtokában. Ugyanakkor már most léteznek okos telefonokra is olyan alkalmazások, amik megvalósítják ezeket a támadásokat. Ilyen például a Faceniff nevű alkalmazás. Ennek a próbaverziója ingyenesen letölthető az internetről, bárki számára. A kezelése is meglehetősen egyszerű, egyetlen gombnyomással lehet indítani (lásd 5. kép). Maga a program pedig működése során ellopja az áldozat Facebook profiljához tartozó ún. session ID-t ARP Poisoning-on alapuló támadás segítségével. Ennek segítségével a támadó hozzáfér az áldozat Facebook profiljához, amíg az ki nem jelentkezik. Tovább súlyosbítja a problémát, hogy sok esetben a felhasználók nem jelentkeznek ki a fiókjukból. Ez kifejezetten érvényes arra, amikor saját készülékükről interneteznek, hiszen ilyenkor nem tartanak attól, hogy később valaki más is ugyanonnan próbálna meg bejelentkezni. Mivel ilyenkor kijelentkezés híján nem szűnik meg egyből a session ID, a támadó ezt kihasználva még sokáig hozzáférhet az adott profilhoz. Ezalatt bármilyen módosítást végrehajthat az adott profilon belül. Bár ez a program csak a közösségi oldal profiljaihoz enged hozzáférést, de mégis jól mutatja az ARP Poisoning alapú támadásokban rejlő lehetőségeket a támadó szemszögéből. A Cain & Abel nevű alkalmazás régóta ismert szoftver, ami szintén a MITM támadásokra specializálódott. Ez eredetileg a vezetékes hálózatok korában lett fejlesztve a hub-ok által kínált támadási lehetőségek kihasználására, de azóta főleg a vezeték nélküli hálózatok lehallgatására lett használható, hiszen hub-okat egyre kevesebb helyen használnak, amióta a switch-ek ennyire olcsók. Ez ugyan okos telefonra még nem letölthető, de notebook-ok, vagy táblagépek esetén már természetesen elérhető. A Cain & Abel sokszínűségét bizonyítja, hogy a lehallgatáson kívül a megszerzett jelszó hash-eket képes feltörni, különböző protokollok esetén is. Ugyanígy képes gyakorlatilag bármilyen hálózati kommunikáció lehallgatására, így például a nyomtatóra küldött adatokat is le tudja hallgatni, vagy a felhasználók egymás közti kommunikációját.

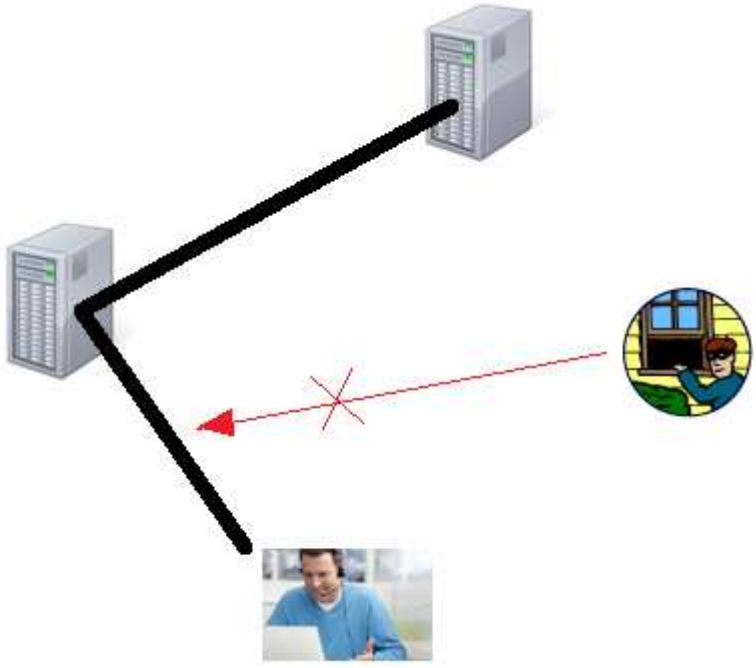
5. Ábra: A FaceNiff alkalmazás elindítás utáni képernyője

6.7 Védelmi megoldások

Természetesen léteznek különböző védekező alkalmazások is a meglévő támadások ellen. Ugyanakkor ezek egyrészt nem minden típusú MITM támadás ellen hatásosak, másrészt sokszor nem is ingyenesek, így kicsi a valószínűsége annak, hogy valaki így védekezzen a támadások ellen. Jó példa a fentiekre a Wifi Protector alkalmazás. Ez az ARP Poisoning támadások esetén jelez, de például az Evil Twin támadásokat már nem jelzi ki. Ennek ellenére fizetős alkalmazásként érhető csak el okos telefonokra. Működés közben a bal felső sarokban látható az ikonja, ami alapesetben egy kék színű pajzs, jelezve hogy a mobiltelefon használója biztonságosan internetezhet. Amennyiben ARP Poisoning támadást érzékel a hálózaton, az ikonja helyén piros színnel jelzi, hogy a hálózat támadás alatt áll. Az alkalmazás kapcsán meg kell viszont jegyezni, hogy sok hiányossága van annak ellenére, hogy nem ingyenes a letöltése. Az alkalmazás ismertetőjében külön említik például a FaceNiff alkalmazást is, mint ami ellen hatékony védelmet nyújt. Ezen kívül írják a Cain & Abel-t, a DroidSheep-et és több más alkalmazást is, aminek a támadását képes jelezni. Ugyanakkor kipróbálás után kiderült, hogy egyrészről csak jelzi a támadást, meggátolni nem tudja azt. Másrészt sokszor jelzett olyankor is támadást, amikor valójában nem futott az adott hálózaton egyetlen ilyen támadó célú szoftver sem. Éppen emiatt a használatának létjogosultsága erősen megkérdőjelezhető. Hiszen a sok fals pozitív eredmény hatására a felhasználó először elveszíti a bizalmát a szoftver iránt – hiszen addigra többször hamisnak bizonyult a jelzés. Majd amikor egy valós támadást jelez az alkalmazás, a felhasználó már nem is figyel a figyelmeztetésre. Mivel a szoftver nem tesz semmit a támadás kivédésére, csak jelzi, így gyakorlatilag használhatatlanná válik az alkalmazás onnantól kezdve, hogy a jelzést figyelmen kívül hagyja a felhasználó. Ezen felül

további hibája, hogy hamis biztonságtudatot kelt a felhasználóban. Mivel az alkalmazás biztonságosnak értékeli a hálózatot, a laikus felhasználó megnyugszik és bátran megnyit olyan oldalakat is, amiket egy nyílt hálózaton esetleg nem nyitna meg. Ugyanakkor sok támadási fajta áll még az ARP Poisoning-on kívül is a támadó rendelkezésére, ahogy a fenti fejezetekben is láthattuk. Így elég csak egy másik módszert választania és máris könnyedén megszerezheti az áldozat jelszavait. Ezeken kívül magasabb szinten lehet még kialakítani biztonságos kapcsolatot. Erre lehetőséget ad a korábban már említett https protokoll. Egy biztonságos kapcsolatot alakít ki a felhasználóval, így ennek használata megoldást jelenthetne a korábban vázolt problémák nagy részére. Ugyanakkor sok probléma is van ennek a protokollnak a használata kapcsán. Ez ugyanis azon alapul, hogy a megtekinteni kívánt weboldal egy tanúsítvánnyal bizonyítja, hogy ez ténylegesen ő. Ez megfelelő megoldás lehet, hiszen innentől a támadó nem tudja magát beékelni a két fél közé. Ennek oka, hogy ő az adott tanúsítvánnyal nem rendelkezik, így a kapcsolat létrehozásakor látszik, hogy a kapcsolat nem megbízható. Ugyanakkor ezzel még nincs megoldva a probléma, hiszen ebben két nagy hiba is van a gyakorlatban. Egyik ilyen, hogy a felhasználók a legtöbb esetben nem tekintik meg a tanúsítványt, hanem automatikusan csak elfogadják azt. Így ha esetleg gyanús is lehetne hogy az adott oldal nem az eredetileg megtekinteni kívánt, hanem annak csak egy másolata, ezzel akkor sem törődnek a felhasználók. Másik ilyen probléma, hogy a biztonságos https kapcsolat a legtöbb esetben nem azt jelenti, hogy a teljes weboldal https protokollon keresztül töltődik le. Ezzel szemben az oldalnak csak egy része megy titkosított csatornán, a többi nem. Még ez is elég lehetne, de semmi garancia nincs arra, hogy ha https kapcsolatot is kér a felhasználó, hogy tényleg https-sel lesz védve a kapcsolata a weboldallal. Éppen emiatt bár a https jó megoldás lehetne weboldalak esetén, a kapcsolat mégsem lesz megbízható feltétlenül, így nem lehet erre alapozni az adatok biztonságát. Arról nem is beszélve, hogy ha nem weboldalak biztonságáról beszélünk, akkor ezt a megoldást nem lehet használni. Tehát például egy VoIP kapcsolat létrehozásakor a https nem tud segítséget nyújtani abban, hogy a beszélgetést ne lehessen lehallgatni. És bár ezt lehetne külön problémaként is kezelni, az optimális megoldás mégis az lenne, ha a megfelelő védelmet már egy alsóbb szinten is ki lehetne alakítani, hogy a felsőbb szinteken a kevésbé, vagy egyáltalán nem védett protokollok segítségével is lehessen biztonságosan adatot továbbítani. A másik magasabb szinten lévő védelem a VPN kapcsolat kialakítása. Ennél nem áll fenn a https protokoll kapcsán tárgyalt két probléma, helyettük viszont itt további gondok adódnak. A megoldás lényege itt az, hogy egy biztonságos kapcsolatot alakít ki a felhasználó egy távoli állomással. Ilyenkor a másik állomás forgalmát lehet csak lehallgatni (lásd 6. kép), a felhasználó által kommunikált adatok

rejtve maradnak. Ennek a megoldásnak nagy előnye, hogy a képen látható lehallgatás sokkal nehezebb, hiszen ha több VPN kiszolgáló is lenne, amit el tudnak érni a felhasználók, akkor csak a VPN kiszolgálók által forgalmazott adatokat kellene védeni. Ez könnyebben megoldható, mint minden felhasználó esetén megvédeni az adatforgalmat, pláne amikor a felhasználók vezeték nélküli közegen kommunikálnak. Itt ugyanis a fő probléma az, hogy a vezeték nélküli forgalomhoz mindenki hozzáfér, így bármit megtehet egy rosszindulatú támadó a hálózattal. Bár ez a megoldás optimális védelmet nyújthatna a VPN kiszolgálók által forgalmazott adatok megfelelő védelme esetén, több probléma is akad ezzel a megoldással is. Első és legfontosabb, hogy a felhasználók hogyan találjanak egy megfelelően védett VPN kiszolgálót, ami biztosan megbízható. Mivel ilyen kiszolgálót általában csak cégek munkavállalói ismernek (a saját cégük VPN kapcsolatát tudják használni, amennyiben az rendelkezik ilyennel), így a többieket kizárja ez a megoldás. Az ingyenesen elérhető VPN szolgáltatásokról megint csak nem lehet tudni, hogy mennyire megbízhatóak. Ugyanakkor a legnagyobb hiba mindennel együtt leginkább az, hogy a felhasználók egyszerűen nem használják a VPN szolgáltatást, hiszen az átlagos felhasználó elvárása az, hogy amikor megnyitja a böngészőt, az egyből biztonságos kapcsolattal szolgáljon, további beállítások és kapcsolat létrehozása nélkül.



6. Ábra: A felhasználó VPN-t használ, így a támadó nem tudja lehallgatni az adatforgalmat

7. WPS hátrányai, használhatósága

7.1 WPA PSK használata

A WPS egy protokoll, amit a könnyebb és biztonságosabb csatlakozás elősegítésére hoztak létre az otthoni felhasználók számára. Ennek segítségével a jelszó beírása helyett elég a felhasználónak az eszközét egy NFC kártyához való hozzáérintéssel, vagy a hálózati eszközön egy gomb megnyomásával felcsatlakoztatnia. Ugyanakkor az így létrehozott hálózat továbbra is WPA PSK alapon működik, hiszen ez a szolgáltatás az otthoni hálózatokra lett kitalálva. Így a WPA PSK esetén felsorolt hibák itt is élnek, leszámítva a jelszó hosszát. Ezt természetesen orvosolja a WPS, hiszen a hálózat így tetszőleges jelszót használhat, tetszőleges hosszúsággal, hiszen a felhasználónak ezt nem kell megjegyeznie és beírnia minden alkalommal. Viszont az a probléma továbbra is fennáll, hogy a hálózat résztvevői látják egymás forgalmát. Míg ez otthoni hálózatok esetén nem jelent problémát, addig egy nyilvános helyen pont ez az egyik támadási felület, amit meg szeretnénk szüntetni a már korábban leírtak miatt.

7.2 WPA PSK használatának okai

A WPS megalkotásakor a cél az volt, hogy az otthoni felhasználók igényeit kielégítsék a könnyű kezelhetőségével. Ennek megfelelően a protokollt is az otthoni felhasználók igényeinek megfelelően találták ki. Ehhez nyilvánvalóan sokkal jobban passzolt a PSK védelem, mint az Enterprise megoldás. Viszont éppen emiatt a WPS használata a nyilvános hálózatok szintjén továbbra sem nyújt megoldást. A PSK-ra vonatkozó hibákon kívül sem felel meg a WPS az elvárásoknak, ennek további okairól a következő fejezetben írok bővebben.

7.3 Könnyen feltörhető PIN

A WPS legfőbb problémája mégsem az, hogy a PSK protokollt használja. 2011 decemberében Stefan Viehböck hozott nyilvánosságra egy hiányosságot, ami alapján a WPS-sel rendelkező eszközök könnyedén feltörhetők. Ennek elkerülésére jelenleg az egyetlen megoldás, ha a WPS funkciót kikapcsolja a hálózati eszköz üzemeltetője. A hiányosság lényege, hogy a WPS protokoll által használt PIN kód egy 8 számjegyből álló kód. Ez összesen 100 000 000 lehetséges kombinációt jelent. Ugyanakkor az utolsó számjegy egy ellenőrző összeg, ami a másik 7 számjegyből visszafejthető. Éppen ezért a végigpróbálandó lehetőségek száma csak

10 000 000. Ennek brute force módszerrel történő feltörése rövid idő alatt megoldható és ezután a támadó hozzáfér a hálózathoz. Így a biztonságos kapcsolat létrehozása érdekében kitalált WPS végül egy komoly lehetőséget adott a támadóknak a hálózat feltörésére. Jelenleg a sok gyártó ad ajánlást arra, hogy lehet kikapcsolni az eszközeikben a WPS funkciót. Ugyanakkor léteznek olyan hálózati eszköz gyártók is, amiknek az eszközeiben nem lehet kikapcsolni sem ezt, így ezekben az esetekben kényszerűen marad egy biztonsági hiányosság az adott eszközökben. A WPS hiányosságai és főleg a benne rejlő biztonsági kockázat miatt éppen ezért nem foglalkozok vele a dolgozat további részében. Az eddigiek alapján tehát összefoglalható, hogy a nyilvános hálózatok védelme nem megoldott. Ezekben az esetekben az adja a problémát, hogy míg az Enterprise megoldás elvárja, hogy a felhasználók kézzel beírjanak egy jelszót, vagy a rendszergazda kézzel felvegye őket, addig a felhasználóktól ez nem várható el, hiszen ők minden beállítás nélkül szeretnék egyszerűen használni a végberendezésüket. A másik megoldás esetén viszont – A PSK beállításakor – a hálózat biztonsága egyáltalán nem garantálható. Ebben az esetben a felhasználók látják az egymás által generált forgalmat és így nem védhetők ki a MITM jellegű támadások. A feladat tehát egy olyan megoldás elkészítése lenne, amivel könnyen fel tudnának csatlakozni egy Enterprise jellegű hálózatra a felhasználók anélkül, hogy bármit be kellene állítaniuk. A következőkben egy ilyen megoldást fogok leírni az alapötlettől kezdve a megvalósításig.

8. Saját megoldás

8.1 Alapötlet

A meglévő védelmi megoldások áttekintése után egyértelműnek tűnt, hogy melyik terület biztonságát lehetne továbbfejleszteni. Mivel az otthoni és vállalati környezetben is megfelelőnek lehet nevezni a jelenlegi védelmi megoldásokat és azokon fejleszteni már csak komoly fejlesztések árán lehetne, így az általam megvalósított megoldás a nyilvános helyeken elérhető hálózatok biztonságát célozta meg. Ennek segítségével meg lehetne oldani azt a helyzetet, hogy ismeretlen felhasználók csatlakozhassanak egy adott hálózathoz és mindegyikük biztonsága garantált legyen anélkül, hogy további dolgokat kellene beállítaniuk a csatlakozás érdekében. A felhasználóknak egyetlen dolguk lesz a kész megoldás után, hogy egy ingyenes alkalmazást letöltsenek az okos telefonjukra, vagy táblagépükre. Ha ez a szoftver telepítve van a felhasználó végberendezésére, akkor az alkalmazás elindításával automatikusan lehet csatlakozni a hálózathoz. A biztonságos kapcsolódás elősegítésére a tervezés fázisában megvizsgáltam, hogy lehetséges-e egy tanúsítvány átvitelével kialakítani egy biztonságos kapcsolatot, vagy szükséges a megfelelő felhasználónév-jelszó párost átadni. Előbbi előnye az, hogy a szükséges adatot egy QR kóddal, vagy NFC kártyával is át lehet vinni. Ez egy olcsóbb megoldás ahhoz képest, hogy a felhasználónév-jelszó páros esetén egy smart card szükséges ahhoz, hogy mindenki egy véletlen generált felhasználónevet és jelszót kapjon. Ezzel szemben a felhasználó név és jelszó átvitele kérdés, hogy jelent-e plusz védelmet a felhasználók számára a tanúsítványos megoldáshoz képest. Ennek vizsgálata egy későbbi fejezetben látható.

8.2 Ötletből adódó korlátok

Ahogy az az alapötletből is látszik, ez a vezeték nélküli hálózatok biztonságának csupán egy töredékét fedi le. Emellett a megoldás erősen épít a már meglévő technológiákra is, azokat inkább csak kiegészíti, mintsem alternatív megoldást nyújtana. Ennek megfelelően a saját megoldásom szintén WPA Enterprise alapú, hiszen ennek segítségével minden jelenleg elérhető Enterprise megoldás kiegészíthető lesz ezzel a funkcióval. Ez előnyösebb sok szempontból, mint egy teljesen új megoldás elkészítése, hiszen sok helyen már létező biztonsági megoldások vannak. Ezeknek teljes lecserélése nyilván csak nehezen és költségesen megoldható. Éppen ezért a megoldásom elkészítésénél szempont volt, hogy a meglévő Enterprise megoldásokhoz hozzáépíthető legyen, valamint ezt olyan módon lehessen

megtenni, hogy a meglévő beállításokat csak a legszükségesebb pontokon kelljen megváltoztatni, amennyiben valaki ezt a kiegészítést szeretné alkalmazni. Mint ahogyan korábban is írtam, az Enterprise hálózatok biztonsága terén az IPS mechanizmusok fejlesztése jelenleg is folyamatosan kihívásokat jelent. Ennek megfelelően mivel az én megoldásom is épít az Enterprise hálózatok struktúrájára, ezeket a jelen megvalósítás sem teszi elhanyagolhatóvá. Továbbá a megvalósítás nem használható otthoni hálózatokban a bonyolult kiépítés és drága berendezések használata miatt. Ugyanígy a megoldás nem felel meg a vállalati követelményeknek sem, így a céges hálózatok kiépítése során nem lehet beleépíteni a meglévő megoldásokba. Ennek oka pont a céges és nyilvános vezeték nélküli hálózatok közt lévő különbség, miszerint a cégek esetén a felhasználóknak feladatuk bizonyítani, hogy jogosultak az internet használatára. Mivel ennek legbiztosabb módja továbbra is az, ha az ezért felelős személy a cégnél felveszi az illetőt a hálózatra jogosultak listájára, így az automatikus regisztrálás ezen a védelmen nyilvánvalóan gyengítene csak. Ugyanígy, vállalati környezetben nincs szükség az Evil Twin jellegű támadások kiszűrésére, hiszen ott ez megoldható máshogyan. A korábban leírt módszer, miszerint a felépített hálózat szól minden felhasználónak, aki a másik hálózatra akar csatlakozni, itt tökéletesen működik. Ugyanis ha itt próbálja meg a támadó hiteltelennek beállítani az eredeti hálózatot, akkor a helyi hálózat üzemeltetője meg tudja nézni, hogy ki lehet a másik hálózat forrása. Ebben az esetben korlátozott a lehetséges támadók száma, hiszen a támadónak ott kell lennie a helyszínen.

8.3 Előnyök

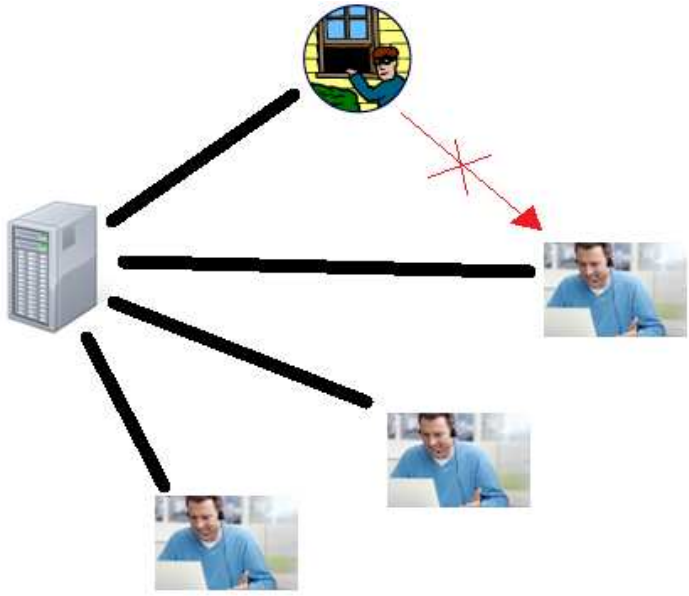
A megvalósításból adódó korlátok ellenére komoly előnye is van a megoldás bevezetésének nyilvános hálózatokon. Míg jelenleg ezen a szinten az Evil Twin támadások ellen nincs kimondottan hatékony védelmi módszer, addig ez egy biztos megoldást ad. A QR kód esetén csupán arra kell figyelni, nehogy valaki leragassza egy másik kóddal az eredetit – Ennek fizikai védelme könnyebb feladat, mint a hálózaton zajló gyanús eseményeket kiszűrni és megfelelően reagálni rájuk. Emellett a biztonságos kapcsolat kialakításához szükség van arra, hogy a felhasználó valami alapján biztosan tudja azonosítani az adott hálózatot. Erre remek lehetőséget nyújt ez a megoldás, hiszen ha ez a QR kód nincs leragasztva egy másikkal, akkor biztosan ugyanazt az adatot kapja meg a felhasználó, ami alapján azonosítani tudja a hálózatot. NFC kártya esetén ugyanez a folyamat játszódik le. Az egyetlen különbség ebben az esetben a technológiai megvalósítás, miszerint nem a QR kódról olvassa le egy okos telefon a kódot, hanem egy NFC chip segítségével csak hozzá kell érintenie a felhasználónak a végberendezését a kihelyezett NFC kártyához. Ennek előnye, hogy kényelmesebb

használatot tesz lehetővé. Ugyanakkor hátránya a QR kódos megoldáshoz képest, hogy a mobil végberendezések kevesebb része rendelkezik NFC chippel, mint amennyi képes értelmezni egy QR kódot. Így ez a megoldás sok felhasználó számára elérhetetlenné tenné az adott hálózatot. A további különbségeket a 7.5 fejezetben fejtem ki bővebben. A jelenlegi megoldások lefedik a vezeték nélküli hálózatok védelmének fontosabb feladataira a megoldásokat. Mint korábban is írtam, a jelenlegi megoldások közül két dolog maradt ki eddig. Egyrészt az IPS jellegű védelmek. Ezekről korábban leírtam, miért nem ezen az úton indultam el. Másrészről viszont egy alapvető támadási fajta, az Evil Twin elleni védelem nincs jelenleg megoldva, illetve az erre használt megoldás nem teljes értékű nyílt hálózatok esetén. Ez azt jelenti, hogy az eredeti hálózat egy olyan üzenetet küld el mindenkinek, ami azt jelzi a felhasználók felé, hogy a másik hálózat nem megbízható. Könnyen belátható, hogy egy esetleges rosszindulatú támadó innentől könnyen lebéníthatja az eredeti hálózatot ugyanilyen üzenetekkel. Éppen ezért a cél az lenne, hogy ezekre az üzenetekre ne legyen szükség, így a végberendezéseknek nem kellene ezeket úgy értelmezniük, mint figyelmeztetéseket és akkor a támadók hamis jelzéseit is figyelmen kívül hagyhatnák. Mivel a felhasználó szemszögéből a támadó és az eredeti hálózati kiszolgáló teljesen egyenértékű hálózatként jelenik meg, ezért a cél az lenne, hogy valamilyen módon az eredeti kiszolgáló megkülönböztethetővé tegye magát a támadótól. A levegőben elektromos hullámok segítségével ez lehetetlen, hiszen nehéz megmondani, honnan jön egy üzenet. Arról nem is beszélve, hogy még ha tudja is a felhasználó melyik irányból jön egy üzenet, nem tudja megállapítani azt, hogy milyen távolságról küldték. Ennek oka az, hogy a jel erősségét tetszőlegesen beállíthatja a támadó. Éppen ezért ha a támadó fizikailag a hálózati berendezés és az áldozat között helyezkedik el, akkor még ilyen módon sem lehet megállapítani, hogy honnan kapja a hálózati hozzáférést a felhasználó. Ugyanakkor a helyzet még rosszabb, hiszen a felhasználói végberendezések nem tudják jelenleg megállapítani, milyen irányból kapják a jelet, amit feldolgoznak. Tehát most akárhonnan próbálhat a támadó közbeékelődni az áldozat és a hálózati eszköz közé, az áldozat eszköze mindig el fogja fogadni a támadót, mint hiteles hálózati szolgáltatót. A cél tehát az lenne, hogy egy olyan átviteli közeget válasszunk, ami garantálja, hogy a támadó és a hiteles hálózat elkülöníthető legyen. Erre tökéletes lehetőséget biztosít az általam biztosított megoldás, hiszen ez csak azt határozza meg, milyen módon juttatja a felhasználó tudomására a szükséges információt a hálózat üzemeltetője. Ennek az adatnak az elhelyezése minden esetben a hálózat üzemeltetőjétől függ, tehát csak azt kell biztosítania, hogy a vendégek ne tudják kicserélni az általa kihelyezet kódot. Ha ezt biztosítani tudja, akkor az általam leírt megoldás garantálja, hogy a támadó nem

tud Evil Twin alapú támadást végrehajtani. Emellett az Enterprise megoldásra épülése biztosítja, hogy a többi MITM támadás ellen is a lehető legmaximálisabban védve legyen.

8.4 Man In The Middle támadások lehetősége

A korábban végigvett támadások esetén nyilván védelmet kell nyújtania egy ilyen megvalósításnak. Így a fentieket végigvéve a következőt láthatjuk az egyes támadások esetén.
A sima **adatlopás** nem megvalósítható, hiszen a felhasználók nem látják egymás forgalmát. Ezt az Enterprise megoldás biztosítja azzal, hogy az egyes felhasználók forgalmát elrejti a többiek elől a hálózaton. Ahogy a 7. képen is látszik, ebben az esetben a támadó ha fel is tud csatlakozni a hálózatra, el van különítve a felhasználótól. Éppen ezért nem látja az általa lebonyolított kommunikációt.

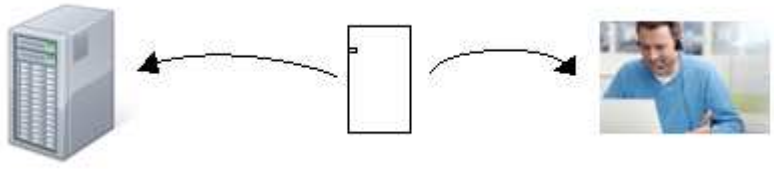


7. Ábra: A felhasználók külön vannak választva, nem látják egymás forgalmát

Az **ARP Poisoning** alapú támadásokat el sem tudja kezdeni a támadó. Ehhez ugyanis szintén az áldozattal egy hálózaton kell lennie, képesnek kell lennie közvetlenül kommunikálni vele. Enélkül nem tudja eljuttatni az áldozathoz a hamis ARP üzeneteket. A hálózati eszköz pedig természetesen tisztában van vele, hogy a forgalom rajta keresztül folyik. Így a 7. képen is látható helyzet fog előállni. Jól látható, hogy a támadó a hálózat kulcsa nélkül nem tud üzenetet küldeni az áldozatnak. Így a felhasználó csak a hálózati eszköz felől érkező ARP üzeneteket kapja meg, ennek megfelelően csak arra fogja küldeni az adatokat.
DNS Poisoning alapú támadás esetén a támadó megpróbálja elhitetni a felhasználókkal, hogy egy adott weboldal az ő IP címén található. A 7. képen látszik, hogy ebben az esetben is – akárcsak az ARP Poisoning esetén – mivel a támadó nem tud közvetlenül az áldozatnak

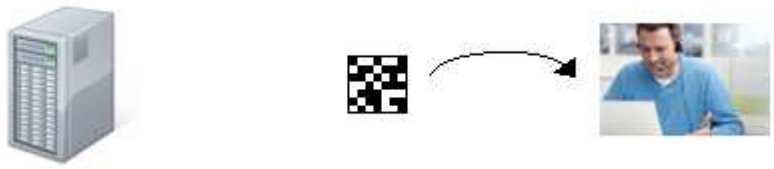
küldeni üzenetet, ezért csak az access point felé küldheti ezeket a csomagokat. Az access point oldaláról viszont ezeket a támadásokat könnyű kivédeni, hiszen egyrészt sok esetben csak egy fix DNS kiszolgálótól fogad el névfeloldásra vonatkozó üzeneteket, másrészt a támadó által küldött üzenetekről könnyen megállapítható, hogy egy a hálózati hierarchiában alatta álló berendezéstől jött az üzenet. Ez semmilyen esetben nem lehet elfogadható, így ezekkel a csomagokkal az access pointnak nem szabad törődnie, mint ahogy nem is teszi.

Az eddigi védelmeket mindeddig az a tény garantálta, hogy WPA Enterprise megoldás esetén a hálózat résztvevői nem látják egymás forgalmát. Éppen ezért mivel ezt egy már meglévő megoldás garantálja, nem ezekre koncentráltam a megoldásom összeállításánál. Ugyanakkor egy ugyanilyen komoly problémát jelent a következő támadási fajta is. Ez az Evil Twin, aminek lényege, hogy a felhasználó nem tudja megkülönböztetni a hiteles és a támadó céllal létrehozott hálózatot. Mivel a levegős közeghez minden eszköz egyformán hozzáfér, így a támadó pontosan ugyanolyan eséllyel tudja meggyőzni a saját valódiságáról a felhasználót, mint az eredeti hálózat. Erre megoldást az jelent, hogy a felhasználó egy előre megadott helyen elhelyezett adatra építi a biztonságos kapcsolat létrehozását. Ezt így a támadó nem tudja lemásolni, hiszen ehhez tisztában kéne lennie olyan információkkal, amikről csak az eredeti hálózat tud. Ezen belül a 8. és 9. képen látszik a két lehetséges megoldás közti különbség. A 8. képen látható megoldásnál az előre kihelyezett eszköz minden esetben egy véletlen jelszót és felhasználónevet generál. Ezt továbbítja a vele kapcsolatba kerülő eszköznek, valamint a felhasználók azonosításáért és hitelesítéséért felelős radius szervernek is. Miután mind a kettőnek továbbította a szükséges információkat, természetesen a következő berendezésnek már más felhasználó nevet és jelszót küld át. Ez egyszerű implementálása egy hagyományos Enterprise megoldásnak annyi különbséggel, hogy itt a felhasználók beregisztrálását egy eszköz végzi automatikusan anélkül, hogy akár a felhasználónak, akár a hálózat üzemeltetőjének bármit be kellene írnia. Ez nem sokban különbözik attól a megoldástól, amikor a blokkra nyomtat egy kódot a pénztárgép és az továbbítja a RADIUS szerver felé a kiadott kódot.



8. Ábra: A kihelyezett eszköz mindkét félnek továbbítja a bejelentkezéshez szükséges adatokat

Ugyanakkor a 9. képen látható megoldás egy ettől eltérő változatot mutat be. Itt a hitelesítés egy aszimmetrikus titkosításon alapul. Ez hagyományosan úgy történik, hogy egy előre definiált nyilvános kulcs segítségével kommunikál a két fél. Mind a két oldal használ ugyanakkor egy saját privát kulcsot is. Ennek segítségével úgy tudják az adatokat titkosítva küldeni, hogy egyik fél sem ismeri a másik által használt titkos kulcsot. A kommunikáció akkor feltörhető, ha a támadó a két fél közé tud ékelődni és el tudja hitetni a felhasználóval, hogy az ő privát kulcsához tartozó publikus kulccsal kommunikáljanak. (Tehát egy olyan publikus-privát kulcspárral, amiben ismeri a privát kulcsot). Mivel itt a felhasználók védelme a fő cél, elég ebbe az irányba garantálni, hogy a kommunikációhoz szükséges kulcs sértetlenül eljut a felhasználóhoz. Ezt úgy lehet például garantálni, hogy egy QR kód segítségével nyilvánosságra hozza a szükséges publikus-privát kulcspárt a hálózat üzemeltetője. Így a felhasználó biztos lehet benne, hogy ha a QR kód hiteles, akkor a támadó nem tudja magát a hálózat üzemeltetőjeként beállítani.



9. Ábra: Egy statikus adatot kap meg a felhasználó

A rogue access point alapú támadások ellen természetesen a fenti megoldás sem biztosít védelmet. Ugyanakkor ezeket azzal tudja az ember könnyen kivédeni, hogy csak olyan vezeték nélküli hálózathoz csatlakozik, ahol garantálva van a biztonsága. Tehát tudatosítani kell az átlagos felhasználókban, hogy egy ismeretlen vezeték nélküli hálózatra csatlakozás komoly veszélyeket rejt magában.

8.5 Megvalósítás

Az általam kitalált megoldás tehát kétféleképpen is megoldható. Elsőként bemutatom részletesen a felhasználói nevet és jelszót dinamikusan generáló megoldást, amikor egy smart card minden felhasználónak más hitelesítési információkat továbbít. A későbbiekben bemutatom a másik változatot is, rávilágítva a lényegesebb különbségekre és a megoldások jellegéből akadó eltérésekre mind gazdaságilag, mind technikailag.

8.5.1 Dinamikus adatok átvitele

Az első gondolatom a hitelesítés fizikai úton történő kiválasztására az volt, hogy az eddig előre beírandó jelszavakat és felhasználói neveket egy automatizmus útján kellene bevinni a rendszerbe. Ezzel megoldható lenne a könnyű használat, mivel felhasználó biztos lehet benne, hogy véletlen generált hitelesítési adatokat kap, amiket mások nem tudnak meg. Erre megoldás lehetne egy NFC kártya, de ennek programozása csak nehezen megoldható, arról nem is beszélve, hogy ezt nem véletlen kódok generálására találták ki. Ennek ellenére létezik másik megoldás is. Smart cardok esetén nincs probléma azzal, hogy hogyan lehetne felprogramozni ezeket, hiszen ezeket egyedileg lehet akár összeállítani, valamint könnyen programozhatók. Ebben az esetben megoldható könnyedén, hogy a kártyák automatikusan állítsák elő a hitelesítéshez szükséges adatokat, valamint ezeket továbbítsák is a felhasználónak és a hálózati eszköznek. A megoldás arra épít, hogy a fizikai közelség és a gyors információcsere miatt a kommunikáció lehallgatása gyakorlatilag lehetetlen. A kapcsolódáskor pedig könnyen ellenőrizheti a felhasználó, hogy az eredeti hálózathoz csatlakozik-e. Egyrészt azt kell megvizsgálnia, hogy a saját jelszavával beengedi-e a rendszer, másrészt azt, hogy másik véletlen generált jelszóval nem. Tehát véletlen számú rossz bejelentkezési kísérlet után egy helyes kísérlet garantálja, hogy a megfelelő hálózathoz kapcsolódik.

8.5.2 Statikus adatok átvitele

A másik megoldás elsőre azért merült fel, mert olcsóbb megvalósítást tenne lehetővé. Ha QR kóddal történik az információ átvitel, akkor nincs szükség drága smart card használatára, elég egy megfelelően nyomtatott matrica is (lásd 10. kép). Így nyilván nem oldható meg, hogy minden felhasználó különböző jelszót kapjon. QR kóddal akkor lenne ez megvalósítható, ha minden blokkra külön rányomtatnának egy különbözőt. Ez viszont megint nem különbözik a blokkra kódot nyomtató változattól. Amennyiben a cél az, hogy egy előre kinyomtatott QR kódot használhasson mindenki, akkor más megoldást kell rá találni. Itt merült fel az aszimmetrikus titkosítás gondolata. A WPA Enterprise ismét kínál egy ehhez jól illeszkedő megoldást. Ez az EAP TLS, ami tanúsítvány alapon oldja meg a titkosítást. Ennek megfelelően itt nincs szükség jelszó átvitelére, mindenki a saját tanúsítványával kommunikál. Bár a szabványt alapvetően arra találták ki, hogy a kliensek hitelesítsék magukat tanúsítvány által, ugyanígy a hálózati eszköz is képes erre. Ennek megfelelően az Enterprise ezt a változatát elég csupán „lebutítani”, hiszen itt bármilyen tanúsítvánnyal elfogadhatja a

kapcsolódási kísérletet a RADIUS szerver. Aszimmetrikus titkosítás esetén a biztonságos kommunikációhoz csupán az szükséges, hogy a két fél megbízhasson abban, hogy az általa látható publikus és privát kulcspár a másik féltől származik és nem egy közbeékelődő támadótól. Mivel itt a QR kód integritásának biztosítása mellett garantálható, hogy a felhasználó a hálózat által kínált kulcspárt látja, ezért itt ez a hitelesítés megfelelő. Sőt, amíg az előző megoldás arra épített, hogy a kommunikáció nem lehallgatható, itt csak arra épít a hitelesítés, hogy a kommunikáció első üzenete sértetlenül megérkezik a felhasználóhoz. Ennek biztosítása már egy könnyebb dolog, hiszen egyszerű esetben akár egy átlátszó, kulccsal zárható dobozba is elég betenni a QR kódot. A végberendezések a QR kódot ugyanúgy felismerik, de így a QR kód leragasztása sem válik lehetővé, hiszen látszik, hogy az új kód a dobozon kívül van felragasztva. Ugyanígy védelmet jelenthet, ha a kódot nagy méretben nyomtatja ki a vendéglátó egység és a pult mögött helyezi el a felhasználók számára jól látható helyen. Így megint csak fizikailag van védve a kód, hiszen ott csak a személyzet tartózkodhat. Ennek tehát hátránya az előző megoldáshoz képest, hogy kényelmetlenebb a felhasználók szemszögéből olyan szempontból, hogy egy QR kód olvasóval le kell olvasniuk a kitett kódot, míg a másik megoldás esetén elég volt hozzáérinteni a készüléket a kihelyezett eszközhöz. Ugyanakkor ez könnyen orvosolható, hiszen egy NFC kártya is képes arra, amit egy QR kód megvalósít. Ebben az esetben a smart card-hoz hasonló megoldást kapunk annyi különbséggel, hogy a titkosítás aszimetrikusan történik. Ugyanakkor ez előnyt jelent, hiszen a jelszó átvitelénél két megoldás közül lehet választani. Egyrészt át lehet küldeni a nyers adatokat, ebben az esetben elég, ha le tudja hallgatni a támadó a kommunikációt. Ez így nyilván nem lehet jó megoldás, hiszen ezzel annyit értünk el, hogy a támadó által lehallgatandó hálózatot minimális méretűre csökkentettük. A másik megoldás esetén titkosítva küldjük át az adatot. Ekkor viszont megint csak tovább eszkaláltuk a problémát, hiszen az eredeti hálózatban megoldandó problémát áthelyeztük egy fizikailag kisebb hatósugarú kommunikációra. Lehet megoldás itt is az itteni kommunikáció aszimmetrikus titkosítása, de ezzel visszatértünk a QR kód által kínált megoldáshoz, fölösleges későbbi adatcserével. Továbbá nem szabad elfelejteni, hogy a smart card, illetve NFC kártya által kínált megoldások továbbra is a levegőt használják, mint átviteli közeget. Éppen ezért itt továbbra is érvényes, hogy a támadó ugyanúgy hozzáfér az átviteli közeghez, mint az eredeti hálózat. Úgyhogy bár egyelőre ez megfelelő védelmet nyújthatna, hosszabb távon csak a technikai megvalósítás hiányzik ahhoz, hogy ez a kommunikáció is lehallgatható, változtatható legyen. Biztonság szempontjából tehát a lehető legtökéletesebb megoldást a QR kód jelenti, amennyiben annak fizikai védelmét meg tudja oldani a hálózat üzemeltetője.

Ugyanakkor ez egy kényelmetlenebb megoldás, mint a másik kettő, hiszen ott elég a készüléket hozzáérinteni egy kihelyezett egységhez, nem kell vele leolvasni egy kódot. Ennek megfelelően az NFC chipekkel rendelkező készülékek esetén lehetőség van a megoldás NFC kártyával történő elkészítésére is. Ebben az esetben a biztonsági kockázat nagyobb, hiszen az átvitt adat végső soron kompromittálható. Anyagilag bizonyos helyeken azonban jobban megéri esetlegesen egy NFC kártyára épülő megoldás. Azokon a helyeken, ahol nem cél a felhasználók kizárása időről időre, a QR kód ugyanúgy egy egyszeri költséget jelent, mint az NFC kártya. Azonban ha valahol cél, hogy a vendégek ne használhassák a hálózatot órákon, vagy napokon keresztül, ott időről időre ki kell cserélni a kitett kódot. Ebben az esetben az NFC kártya átprogramozása nem kerül semmibe, bármennyiszer meg lehet ezt tenni. QR kódnál viszont minden esetben új nyomtatással kell számolni. Hosszútávon tehát ezeken a helyeken elképzelhető, hogy megtérül az NFC kártya megvásárlása anyagilag.

10. Ábra: Tanúsítványt tartalmazó QR kód

9. Összegzés

Dolgozatomban megvizsgáltam a jelenleg elérhető hálózati védelmi megoldásokat. Ezek közt külön tárgyaltam a nyílt hálózatokat, illetve amelyeket captive portal véd. Megvizsgáltam a különböző hálózati titkosításokat. Ezen belül a WPA két változatának hasznosságát és hátrányait fejtettem ki különböző környezetekben. Ennek megfelelően említettem otthoni, nyílt és vállalati környezetben is a WPA otthoni, illetve vállalatokra fejlesztett változatát. Megvizsgáltam, melyiknek milyen hátrányai vannak és milyen előnyei. Arra a következtetésre jutottam, hogy a WPA-n belül is az Enterprise megoldás nyújt igazán komoly védelmet a felhasználók számára. A PSK ezzel szemben annyi előnnyel rendelkezik, hogy olcsóbb és könnyebb a beüzemelése, mint a vállalati változatnak. Ennek megfelelően ez ideális otthoni kis hálózatokra, ahol nem kell tartani az esetleges hálózaton belüli adatlopásoktól, lehallgatásoktól, hiszen a hálózat használói egymás rokonai. Minden más helyzetben viszont szükségesnek találtam a WPA Enterprise megoldás bevezetését, hiszen ez garantálja a megfelelő védelmet mind a hálózat üzemeltetője, mind a hálózat használói számára. Láthattuk tehát, hogy a jelenlegi biztonsági megoldások Enterprise megoldás esetén kielégítőek a legtöbb esetben. Ez alól kivételt jelent nyílt hálózatok esetén, hogy az Evil Twin támadások elleni megoldás nem ideális. Míg a többi támadási módszer ellen képes védekezni a vállalatok számára kifejlesztett WPA Enterprise akkor is, ha nyílt hálózatokról van szó, addig az Evil Twin támadások ezen már kívül esnek. Ennek megfelelően bár létezik rá megoldás, az nem nyújt teljes védelmet a hálózat és résztvevői számára. Erre nyújt megoldást az általam elkészített változat, ahol egy QR kód segítségével hitelesítheti magát a hálózatot a felhasználó. Így biztos lehet benne, hogy mindig a megfelelő hálózatra csatlakozik. Ennek okait kifejtettem. A megoldás lényege pedig az, hogy a hálózati biztonság át van helyezve fizikai síkra. Azaz a hálózat szolgáltatójának csak annyit kell biztosítania, hogy az átküldendő adat hordozójához (jelen helyzetben QR kód) ne férjen hozzá fizikailag a támadó, ne tudja azt kicserélni. Ennek egyéb változatai közt meg lett említve, hogy a hitelesítéshez szükséges adatokat esetleg át lehetne vinni úgy, hogy minden felhasználó más hitelesítési adatokat kapjon meg, azonban ez egyrészt drágább megoldást jelent, másrészt nem is megfelelő az általa kínált biztonság. Ugyanígy alternatív megoldást jelenthet egy NFC kártya kihelyezése a QR kód helyett. Ez a felhasználóknak kényelmesebb és esetekben olcsóbb megoldás a hálózat üzemeltetőjének, mint a QR kódos változat. Ugyanakkor elméleti szinten a QR kód biztosabb megoldást jelent még akkor is, ha az NFC kártyák által átvitt adat jelenleg megfelelő biztonságot nyújt a felhasználóknak.

10. Irodalomjegyzék

Cím	Szerző	Évszám
[1] http://www.academia.edu/1501652/GPU_-_accelerated_WPA_PSK_cracking_solutions	Khai Tran Viet	2010
[2] http://mokk.bme.hu/munkatarsak/	Média Oktató és Kutató Központ	2012
[3] http://faceniff.ponury.net/	-	-
[4] http://www.oxid.it/cain.html	-	-
[5] https://www.wifiprotector.com/	-	-
[6] http://droidsheep.de	-	-