HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

WI-FI HÁLÓZATOK KÉT KIJÁTSZHATÓSÁGI PONTJA: WPA2 ÉS ROGUE AP

TWO ERROR OPTIONS OF WI-FI NETWORKS: WPA2 AND ROGUE AP

KOSKA Melinda Henriett

(ORCID: 0000-0003-2909-8788)

koskameli@gmail.com

Absztrakt

Tavalyi év során fény derült a WPA2 titkosítási protokoll hibájára, mely több milliárd eszközt és gyártót is érint. A hiba kiküszöbölése még folyamatban van és a probléma megoldása a WPA3 lesz majd, illetve egyéb felhasználói ajánlás is megfogalmazásra került.
A Wi-Fi hálózatokhoz kapcsolt másik általam vizsgált támadási forma a rogue ap-ok, melyek engedély nélküli biztonsági rések. Mind a két esetben az adatfolyamok lehallgathatók, manipulálhatók, ezért kell különös figyelmet szentelni e két területnek.
Az Emberi Erőforrások Minisztériuma ÚNKP-17-2-I-NKE-79 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.
Kulcsszavak: *Wi-Fi, WPA2, Rogue AP*

Abstract

Last year, became known, default of WPA2 security protocol. It means billions of devices and companies. The problem solution is still in progress, WPA3 is coming and other user's recommendations have been formulated.
Another form of attack, which connected to Wi-Fi networks is the rogue ap, that has been installed on a secure network without explicit authorization. In both cases, the data stream could be listened and manipulated, that is why the users and companies need to pay attention to these two areas.
Supported by the ÚNKP-17-2-I-NKE-79 new national excellence program of the ministry of human capacities"

Keywords: *Wi-Fi, WPA2, Rogue AP*

A kézirat benyújtásának dátuma (Date of the submission): 2018.04.25.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.10.

BEVEZETÉS

Az információs és kommunikációs technológiák a 21. század egyik legdinamikusabban fejlődő iránya, amely több területre is hatással van. A szerteágazó irányai közül az általam vizsgált terület, a wireless-es technológiák, azaz vezetéknélküli csatlakozás egy része, a Wi-Fi hálózatok biztonsága. Azon belül is a WPA2 protokoll és a Rogue Access Point (továbbiakban AP) használatakor felmerülő biztonsági kérdések.

Informatikai rendszereket majdnem mindenki használ, csak eltérő szinten. Az informatikai infrastruktúra iránt egyik általánosságban elvárt szolgáltatás a vezeték nélküli, teljes lefedettségű, mindenki számára elérhető szélessávú, gyors internet hozzáférés, csökkenő költség hozzájárulással. [1] Mivel egyre többen használják a vezeték nélküli technológiákat, fontos hangsúlyt fektetni a helyes internet, hálózatok használatára és az adatok biztonságos kezelésére.

Az emberi tényező az egyik legkritikusabb az adatszerzések útvesztőjében, azért, mert halmozottan rendelkeznek olyan jellegzetességekkel, amelyek alapján nagyvalószínűséggel potenciális áldozatokká (adatlopás, információszivárogtatás, beszervezés) válnak. Az első lényegi pont, hogy olyan adatok birtokában vannak, amelyek védendőnek számítanak, még akkor is, ha ez számukra nem triviális. A másik oldal pedig a kihasználható emberi tulajdonságra alapoz, mint például a hiszékenység, naivitás, kíváncsiság, gyors információszerzés utáni vágy, avagy a segítőkészség.

A fentebb felsorolt emberi tulajdonságokat a nethez való csatlakozáskor is ki lehet használni. Olyan támadási formákat kivitelezésére alkalmas az internet, mint például, az adathalászat, adatlopás, rosszindulatú alkalmazások elterjesztése, megfigyelés lehetősége, avagy a hálózat üzemeltető részéről olyan adatokhoz való hozzájutás, mint a böngészési információk, jelszavak és a beszélgetések. Így könnyen zsarolhatóvá válik az ember például egy-egy elküldött fénykép, üzenet által. Fokozottan igaz ez, ha a felhasználó egy nem biztonságos Wi-Fi hálózaton keresztül továbbít adatot. Másik lényeges vizsgálandó pont a tudatos és nem tudatos internetfelhasználók köre. Utóbbi kategória fejlesztéséhez szükséges meglátásom szerint, a támadások fajátinak ismerete, védekezési mechanizmusok. A hipotézisem, mely felméréseken és beszélgetéseken alapul a Nemzeti Közszolgálati Egyetem hallgatói köréből, [2] hogy a felhasználók a Wi-Fi hálózatokon keresztül történő adatforgalombiztonsága ismereteinek hiányával küzdenek.

FENYEGETETTSÉG

Egyre többen kapcsolódnak be az információ- és kommunikációtechnológiába. [3] Ennek egyik ága a wireless technológia, mely vezeték nélkül képes áthidalni óriási tereket. Így hatalmasat lendít a mobilitáson. Fizikai jelenlét nem kell ehhez a kapcsolat létrehozásához, azonban a rádiós csatorna jellege miatt, könnyebben hozzáférhető a rendszer, mint a vezetékes internet elérésnél. A vezeték nélküli kapcsolat a leginkább hatékony, rugalmas és költséghatékony megoldás a mindennapi élethez, legyen szó iparról, mezőgazdaságról, szolgáltató szektorról, avagy a privát felhasználói tevékenységekről. Minél több eszköz és ember vesz részt a kiterjesztett világban, annál több dologra kell figyelemmel lenni biztonsági szempontból. [4] Nem csak a védelem informatikai hatékonyságán múlik az adatok és a privátszféra védelme, hanem a biztonságtudatos felhasználókon is. Egy nemzetközi jó gyakorlat Németországból, hogy nem csak a felhasználókat terheli felelősség adatvédelmi szempontból, hanem az internetkapcsolatok üzemeltetői is felelnek a megfelelő biztonságért. Egyedi ügyben olyan

állásfoglalást hozott a bíróság, hogy a WLAN hálózatot nem lehet nyíltan hagyni, jelszóval kell védeni, azonban a nemzetközi joggyakorlat nem követi ezt a példát. [5]

INTERNET OF THINGS (IOT)

Az internet forradalma eddig az embereket kapcsolta össze, a következő lépés azonban a tárgyak összeköttetése (lesz), ami az Internet of Things (dolgok internete, továbbiakban IoT), mely képes a netet használva egyszerre érzékelni és kommunikálni több eszközzel. [6] Az Internet of things kifejezés már az 1900-as évek végétől használatos. A Wi-Fi és a 4G-LTE vezeték nélküli internet elérésének növekvő térnyerése, és a mindenhol jelentkező információ és kommunikáció felé vezető irány már teljesen nyilvánvaló. Mindennapos használati tárgyként már beleivódott a köztudatba a laptop, tablet, okostelefonok, okos televíziók, videójáték konzolok, de már a hűtőszekrények [7] és a légkondicionálók is. Ezen technikai eszközök teljes mértékben az emberektől függenek, olyan értelemben, hogy a tárgyak az adatokat, információkat az embertől érzékelik, vagy vele kerül kölcsönhatásba legtöbbször. Azonban az IoT sikeres elterjedéséhez szükség van számítástechnikai paradigmaváltásra, és tovább kell lépnie a hagyományos mobil eszközökön, és a mindennapos használati tárgyaknak kell összekapcsolódniuk, amelyek körülveszik az embert. A cél ezen eszközök autonóm, emberi beavatkozás nélküli, és okos viselkedése, ami egy teljes világot átfogó integrált jövő internethez vezet, s ehhez három alappillérnek kell teljesülnie; a felhasználók és a készülékeik közötti feltételnek, amelyek feldolgozzák és közvetítik az információkat, ahol releváns, és ezeket vegyítve, elemzést kell végrehajtaniuk. A három pillérhez három paradigma is tartozik, ami az internetorientáltságot, a szenzorokat, és a tudást foglalja magában.

Az IoT-ot heterogén technológiák jellemzik, amely jellegéből adódóan folyamatosan újul, időről-időre új megoldások kerülnek felszínre. Különböző biztonsági és adatvédelmi követelmények problémák látnak napvilágot, melyek megoldásra várnak. Ilyen követelmények többek között, az adatok, adatátvitelek titkosítása, engedélyezése és hitelesítése, a rendszerhez való hozzáférés szabályozás, visszautasítása rendszertől. Ez alatt az érthető, hogy nem csatlakozhat a kliens a hálózathoz. További elvárás a felhasználó és az eszköze közötti bizalom kiépítése. A hagyományos biztonsági eljárások már meghaladottak, illetve a felhasználók a már meglévő technikai megoldásokat sem használják ki kellőképpen. A felhasználók bizalmának foka, megléte határozza meg, hogy milyen eszközöket használnak a mindennapok során, illetve a támadások egyik kulcs kérdése is, hogy a célpont az érkező támadóval, vagy támadással szemben bizalommal kezeltetik-e, vagy fenntartásokkal.

Az eszköz-eszközzel való kapcsolatok rohamos növekedése nem csak az adat mennyiségét és forgalmát növelik, hanem egyéb számítógépes fenyegetések számát is. A machine to machine (azaz eszköz és eszköz közti kommunikáció, továbbiakban M2M) jelen állapot szerint nem védettek, illetve nem eléggé védettek a kibertámadásokkal szemben.

2011-ben az összekapcsolt eszközök száma elérte a Föld lakosságának teljes számát. Több milliárd új eszköz részvételét eredményezi ez a folyamat. 2013-ban a 2020-ra várható összekapcsolt tárgyak számát 24 milliárd eszközre saccolták [6, p.1645-1646], addig ugyanerre az évre vonatkozólag 2016-ban már ötven milliárd objektumra számítanak az előrejelzés szerint. [8] [9] [10]

Ebből is látszik, hogy ez az új tendencia korai szakaszában van még, de rohamos fejlődésen fog keresztül menni, [11] [12] sőt az élet területének szinte minden részét érinteni fogja, különösképpen az egészségügyet, [13] [14] [15] az ipart, a katasztrófa előrejelzést, [16] az autóipart, logisztikát, közlekedést, tehát összességében jobb életkörülményekkel kecsegtet mindenki számára. Ezért elkerülhetetlen, hogy az IoT-nak megfelelőnek kell lennie ahhoz, hogy az adatokat, amelyeket összegyűjt és továbbít, biztonságosan tárolja és továbbítsa. Az IoT sikeressége érdekében kulcsfontosságú a dolgok egyedi azonosítása. Ez teszi lehetővé, hogy az

adott eszközt egyedülállóan azonosítanak és távoli eszközöket az interneten keresztül vezérelni lehessen.

A képi világa az IoT-on alapuló alkalmazásoknak létfontosságúak, mivel ez hozza létre a felhasználó és a környezet közös pontját. A fejlesztések az érintőképernyős technológiákat részesítették előnyben és igen elterjedté tette az okostelefonokat és a tableteket. A laikus személy számára, hogy teljes mértékben részesévé tudjon válni az IoT forradalmának, vonzó, interaktív és könnyen érzékelhető vizualizációt kell létrehozni. Példaként említhető e képi megjelenési formára a 2D-ről a 3D-re váltás. Az adatokat, információkat gyorsan tudássá kell alakítaniuk az eszközöknek, ami egy kritikus pontja többek között a gyors döntéshozatalnak is. [6, p. 1649]

A felhasználó olyan módon is részt vesz ebben a körforgásban, hogy az adatok egy részét ők maguk viszik fel a rendszerbe. Példaképpen Gmail fiók létrehozásánál szükség van a teljes névre, születési dátumra, nemi hovatartozás megadására, opcionálisan mobiltelefonszám beütésére, jelenlegi e-mail címre és tartózkodási helyre, amit beállításoktól függően már előre is kitölt a rendszer. Azt ígéri a Gmail, hogy csak néhány személyes adatra van szükség az új e-mail cím létrehozásához, amelyekkel segítenek megőrizni a fiók biztonságát, és még hasznosabbá teszik a különböző szolgáltatásokat. [17] Ezeknek az adatoknak a hitelessége azonban megkérdőjelezhető, tehát a kiindulási információk nem feltétlen pontosak. Nem tudatos adatmódosításról, adat beviteli hiányról van szó, hanem az emberi mivoltnak a determináltságáról, ami időhiányban, figyelmetlenségi és pontossági problémákban nyilvánul meg. A hálózati rendszerek az emberek által bevitt adatokból indulnak ki, és onnan végzik a feladatukat, amelyek azonban mivel az alapfeltételezés nem mindig helyes, költség- idő hatékonysági szempontból kár keletkezhet. Ha a tárgyak saját maguk vehetnék fel az információkat a külvilágból emberi segítség nélkül, akkor az emberek részére olyan adat és információ halmazok állnának, melyek nagymértékben csökkentenék a veszteségeket, melyeket ma még realizálni sem lehet. [18]

Minden okos, intelligens rendszer rendelkezik hibával. Egyik vicces rendellenességet az Amazon hangvezérlésű intelligens asszisztense, Alexa, prezentálja legszemléletesebben véleményem szerint. Alexa hang alapon rendel, keres a neten, és végrehajt, azonban nem csak az adott felhasználótól érkező parancsot teljesít (akár a TV-ből hallott információt is). A „hölgy” bankkártyához van kötve, amely segítségével tud vásárolni, azonban így nem behatárolt támadási vektor tud lenni akkor, ha nincs egy megerősítő közbeékelődő folyamat beinterpretálva a megrendelés és a fizetés között, akkor ez bankkártyával való visszaélésnek is minősülhet. Illetve egy bohémebb példa az okos eszközök hibáira, szintén Alexától, hogy kineveti a felhasználót, ami inkább bosszantó, mintsem támadás, vagy rés lenne. [19]

WI-FI hálózatok

A Wi-Fi (wireless fidelity) vezetékes kapcsolat nélküli kommunikációt, hálózati technológiát jelent, amivel rádióhullámokon keresztül a vezetékes hálózathoz lehet csatlakozni. Minden vezetékes vagy vezeték nélküli hálózatnak meghatározott protokoll szerint kell működnie. Ebben a jelentésben a protokoll arra vonatkozik, hogy az adatok hogyan cserélnek gazdát. A Wi-Fi Alliance céghálózathoz tartozik a Wi-Fi termékek tanúsítása, s meghatározzák, hogy milyen szabvány alapján nevezhető egy termék Wi-Fi-nek. Ez a szabvány most az IEEE 802.11, ami adatkapcsolat és adattitkosítási metódus. [20] Több fajtája ismeretes, privát, nyilvános (közösségi tereken használt, kávézókban, könyvtárakban), nyílt (csatlakozásához nem kell jelszó) és zárt (jelszóval védett). Az adattitkosítási részében biztonságos hálózatnak hívják azt, amit titkosítási algoritmusok védenek, amelyek a WEP, WPA, WPA2. A WEP a legkorszerűtlenebb algoritmus, mely kevesebb, mint egy perc alatt feltörhető, így a használata nem javasolt.

A Wi-Fi hálózat főbb komponensei a következőkből állnak

- hozzáférési pontból, azaz Wireless Access Pointból, mely a Wi-Fi és a kábeles hálózatot összekötő útválasztó, így használhatóvá válik a vezeték nélküli hálózat.
- Kliens, ami lehet számítógép vagy program, ami hozzáfér egy szolgáltatáshoz, amelyet egy számítógép hálózathoz tartozó másik számítógép nyújt. [21] [22]

Az AP hozzáférési pontot jelent, melyen keresztül tud a Wi-Fi-t használó eszköz csatlakozni a vezetékes hálózathoz. Ez több eszköz számára elérhetőséget biztosít a hálózathoz, az IEEE 802.11-es vezeték nélküli adatátviteli protokollban, ez a szám maximum 25 lehet. Azonban, ha nagy területet kell lefedni, akkor a vezetékes hálózathoz több Access Point is tartozhat, így kiküszöbölve a maximális felhasználói csatlakozó számot és a nagy terület lefedettségét.
WLAN hálózatokban több hozzáférési pont található, emiatt szükséges egy azonosítás, mely pontosan meghatározza, hogy mely hozzáférési pont mely felhasználóhoz tartozik. Az azonosításhoz a MAC címet használja. [23] A MAC cím az egyedi hardver azonosító az eszközhöz. Neve egy rövidítésből fakad, a Media Access Controlból. Célja, hogy minden azonosító egy adott eszközt azonosítson. A probléma a beazonosítással, hogy csak a következő útválasztóig lehet visszakövetni az adott eszközt, miután elérte az útválasztót, azután már az útválasztó MAC címén keresztül folynak tovább az adatok. Másik probléma a visszakövethetőségével, hogy viszonylag könnyen megváltoztatható. Az egyén oldaláról közelítve pedig, egyértelműen azonosítja a felhasználóra vonatkozó APt, hogy melyikhez autentikáljon, azaz kapcsolódjon. Helyváltoztatással másik routerhez (útválasztóhoz) csatlakoznak, ahol adatkapcsolati rétegen használt azonosítót (basic service set identifier továbbiakban BSSID) kapnak. Az eszközök és a felhasználók (kliensek) hitelesítése az egyik legfontosabb a vezeték nélküli rendszerek működésében, ezért fontos a MAC és a BSSID.

Hálózati protokollok

Az azonosítás és a biztonság megőrzéséhez elengedhetetlen ismerni a nyílt rendszerek összekapcsolásának referenciamodelljét, az Open Systems Interconnection Reference Modelt (továbbiakban OSI). Rétegelt felépítésű, mely a hálózati protokoll meghatározásában játszik szerepet. Alulról építkezik, és csak azokkal az adatokkal tud dolgozni, melyeket az alsóbb rétegből kap, felfelé pedig csak egy lépcsőt ugorhat. Az OSI referenciamodellje meghatározza két számítógép közti kommunikáció feltételét. Vetélytársa a TCP/IP lett, így mára ennek a modellnek csak egy részét alkalmazzák.

- Legalsó rétege a fizikai réteg, ahol a bitek kijutnak a kommunikációs csatornára.
- Második szintje a modellnek az adatkapcsolati réteg, ahol létrejön a két hálózati elem között az adatok továbbítása. Azonosításra visszautalva, a MAC címek találhatóak itt.
- Hálózati réteg követi az adatkapcsolati réteget, ahol adatátvitelhez szükséges eljárások találhatóak, mint például útválasztó választás. Itt az egyik legjellemzőbb protokoll maga az IP.
- Amennyiben az adat elindul a kommunikációs csatornára, már rendelkezik adatkapcsolattal. A két végpont és az útválasztó megválasztása is már lezajlott, akkor a szállítás lesz a következő lépcsőfok.
- Ezután a csomópontok kommunikációján múlik az adatok áramlása, ami a viszony réteg.
- Ha az adat végig haladt ezen a folyamaton, akkor alkalmasnak kell lennie, hogy a végfelhasználó számára megfelelő formában álljon rendelkezésre, ez lesz a megjelenítési réteg.
- A hetedik réteg dolga a bejövő adatok értelmezése. [24]

A hálózati protokollok, amely leírja, hogy az eszközök milyen módon tudnak egymással kommunikálni, a fentebb felsorolt szintekhez kapcsolódva többféle csoportosításban jelennek meg. A lentebb kiemelt területek a laikusok számára általam legtöbbször előforduló elemek. Az OSI modell legalsó szintjén, az L1-es szinthez tartozik az Ethernet (amely a legelterjedtebb hálózati megoldás, nagy sebességgel), USB, Wi-Fi és Bluetooth.

A kommunikáció akkor jön létre, ha jelen van egy adatkapcsolati réteg, amelyen keresztül zajlik az adatok hibamentes, biztonságos szállítása a hálózati csomópontok között. Az információkat keretbe rendezik, szükség szerint tördelik és ellátja kiegészítő címekkel, plusz egyéb ellenőrző információval. Az L2-es szinthez az ARP tartozik, (angolul Address Resolution Protocol), és az IP címet és a MAC címet rendeli egymáshoz. Az ICMP (Internet Control Message Protocol) tartozik még ide, amelyet az interneten használnak, s legtöbbet a hibák meghatározásánál felfedezhető. Adatcsomagokat figyeli, hogy hibásan érkezett vagy nem, hányszor érkezett meg, vagy elveszett a hálózatban, illetve az egymás után küldött csomagok sorrendjét is figyelemmel kíséri. [25] [26] A DHCP egy dinamikus állomáskonfiguráló (Dynamic Host Configuration Protocol) kliens-szerver protokoll, (amely tartozhat az L3-as szinthez is, ekkor relay-nek nevezik) amelytől a hálózati állomások az IP, illetve egyéb protokollokkal kapcsolatos információkhoz hozzájutnak a rendszergazda közvetlen beavatkozása nélkül, így időt, pénzt és energiát spórolnak meg. Feladata, hogy egy IP címet egyszer osszon ki.

A harmadik szinten található az IPv4, IPv6, mely a hálózati protokollok csoportjába tartozik, tartalmazza a címzett és a küldő címet, valamint a portjait. A routerek ezek alapján döntenek a csomagok továbbításról.

Az L4-ik szintjén a TCP van, ami egy kommunikációs protokoll, mely mostanra az egyik legelterjedtebb lett a gondos kidolgozása miatt. Folyamatosan ellenőrzi adatfolyamatot, így megbízhatósága is kitűnő. [27] Magasabb szintű szervíz protokollok csoportjába tartozik a Hypertext Transfer Protocol (kérdés-válasz protokoll, továbbiakban HTTP), ami az egyéni felhasználók szempontjából a legtöbbször előbukkan, mivel az URL címben legtöbbször HTTP-s címekkel találkozhatnak. Ugyanezen szervíz protokollhoz tartozik, az Interactive Mail Access Protocol (levelezési protokoll, továbbiakban IMAP), mely segítségével kezelhetők, illetve távoli elérésre alkalmasak a leveleket. Először csak a fejlécet küldi el, ami alapján lehet dönteni egyes levelek külön letöltéséről, azonban nagyobb tárhelyet is igényel, ezért nem terjedt el. [28] A POP3, mely a levelezési protokollok csoportjába tartozik, amellyel letölthetők a levelek. [29] Az SMTP is idetartozik, amely szintén levelezési protokoll. [30]

A szintek legfelső fokához a DNS (Domain Name System) tartománynévrendszer tartozik, mely alkalmazási protokoll, mint a DHCP. A tartományneveket kezeli, szükség szerint átalakítja numerikus azonosítókká. Ez segít abban, hogy különböző területről, különböző eszközökkel ugyanaz az oldal jelenjen meg a világhálón, habár változtak a körülmények. A felhasználók számára egyszerűsít, mivel csak számokból álló kombinációkat nehezen jegyeznek meg, azonban egy domén nevet (mint például https://akk.uni-nke.hu/), azt sokkal könnyebben, viszont ez a könnyítés nem használható a hálózaton belüli kommunikációban, s a DNS ezt hivatott átkonvertálni numerikus leírássá. Az internet struktúrájában kettő névtér létezik, az általam itt taglaltat és az IP-címteret. A Domain Name System felelős az első szegmensért, és fordítási szolgáltatást nyújt az IP-címterek és a DNS nevek között.

WPA2 titkosítási protokoll

A Wi-Fi Protected Access 2 (továbbiakban WPA2) a vezeték nélküli rendszerek protokollja immáron 15 éve, amelyet a titkosítás érdekében, azaz adatok megőrzése céljából fejlesztettek ki. 2017 októberében Mathy Vanhoef rátalált egy olyan hibára, amely szerint a protokoll, vagyis a titkosítási folyamatot leíró szabvány a hibás, nem pedig az egyes rendszereket létrehozó termékek vagy kivitelezésük. [31] Ez azt jelenti, hogy a teljes átmenő adatforgalom

megfigyelhető, illetve bármi elhelyezhető az adott eszközön, akár további megfigyelés céljából is.

Amikor vezeték nélküli csatlakozás létrejön, akkor a hálózati vezérlővel megegyezik a kliens a titkosítási kulcsról. Telepítés után ezen keresztül fognak az adatcsomagok vándorolni a titkosítási protokollt (jobb esetben a WPA2-őt) használva. Azonban, amikor megérkezik ez a titkosítási kulcs, előfordulhat, hogy többször küldi el, mert a rendszer számol a térben elvesző adatokkal, így pedig a számlálót (nonce), ami az adatcsomagok forgalmát nézi, lenullázza. Erről az anomáliáról (Key Reinstallation AttaCKs) kapta a nevét a felfedezés, a KRACKs. A titkosításnak az lenne a kiindulópontja, hogy nem ismétlődhet meg a titkosítási kulcs lekérése-elküldése, főleg úgy, hogy lenullázza a számlálót, mintha addig semmi sem történt volna. Ez azonban nem valósul meg. A támadó a titkosítási kulcs lekérésénél kapcsolódhat be, lenullázhatja a számlálót, innen a WPA2-be is bele lehet nyúlni, és a hálózati csomagokkal minden megtehető, amire a támadónak szüksége lehet, mint például bankkártya adatok megszerzése, jelszavak visszafejtése, chatelések elérése, e-mailekhez és képekhez való hozzáférés. A támadást több féle módon is el lehet követni, egyik példája az elvileg mindig eredményes brute-force, ami egy számítógépes program, és az összes lehetséges jelszókombinációt kipróbálja, hogy megszerezze a titkosítást biztosító kulcsot és bejusson a rendszerbe. [32] Minél hosszabb a jelszó, és minél összetettebb, szótár alapon nem kitalálható, annál időigényesebb feltörni, illetve bizonyos rendszerek, mint a Gmail, pár próbálkozás után letiltja bejelentkezést. A hálózati konfigurációtól függően nem csak adatok megszerzésére irányulhat ez a folyamat, hanem adatok bevitelére és manipulálására is. A támadás az összes Wi-Fi hálózat ellen hatásos, és bármilyen okoseszköz áldozatul eshet, de érdemes megemlíteni a kevésbé védett Androidos rendszereket, melyeken az adat visszafejtés egyszerűbb és gyorsabb is. Az Android operációs rendszer Linux-alapú és körülbelül évente kétszer új verzió kerül a piacra. A WPA2-es hibák a 6.0-és újabb verziókat érintik, amely azt jelenti, hogy 800 millió okostelefont és tabletet. Az alapvető probléma ebben az esetben, hogy a kliens az all-zero titkosítási kulcsot telepíti az eredeti kulcs helyett. [31] Magát a WPA2 titkosítást milliárdnyi vezeték nélküli eszközön használnak.

A CERT (Computer Emergency Response Team), egy szakértői csoport, akik a megfelelő eljárások alkalmazásában segíti a szervezeteket, ügyfeleket, kormányokat, a számítógépes hálózati incidenseknél, mint ahogy ezt az esetet is. [33] Az amerikai CERT figyelmeztetést adott ki a hibáról: „*az US-CERT tudomást szerzett a hibáról a WPA2 biztonsági protokoll négyirányú kézfogásakor észlelt problémáról. A szabvány minden típusa érintett*.” [34] Készítettek egy listát, hogy mely gyártók érintettek, idetartoznak többek között az Android Open Source Project, az Apple, a Microsoft Corporation, a Samsung Mobile, a Sony Corporation, melyek mobilkészülék gyártók, illetve okos eszközökre fejlesztenek ki operációs rendszereket. A Microsoft Corporation volt az első, aki reagált a problémára és elsőként dobott piacra frissítést ennek a hibának a kiküszöbölésére. Továbbá ide sorolható a Cisco Systems, Juniper Networks, Fortinet, Ubiquity és a D-Link System, a Netgear, a TP-LINK, melyekkel általában routerek és modemeknél lehet találkozni. A Dell, a Toshiba Electronic Devices & Storage Corporation és a Lenovo cég is érintettek, akik laptop gyártó cégek. A Google sem képzett kivételt. [35]

A támadások megelőzésére többféle módszer is lehetséges. Amennyiben és amikor az új termékek frissítése megjelenik, élni kell a lehetőséggel. A szakértők javasolják a router firmware-jének (mikroprogramjának) a módosítását. A Wi-Fi hálózat jelszó frissítése, mint megoldás, nem eredményez megoldást. Olyan hálózatokon, ahol ismeretlen eszközökhöz csatlakozik a kliens, nem bízhat meg az adatok biztonságát védő, illetve nem védő rendszerekben, mert nem ismertek a körülmények, a technikák, ilyen esetben a felhasználónak saját magának kell megteremteni azt a közeget, ahol az adatai biztonságban vannak. 2018 januárjában már fejlesztés alatt áll a Wi-Fi Protected Access 3, azaz a WPA3. Ez már védelmet

nyújt a brute-force jellegű szótársa támadásoktól is és a magasabb szintű biztonságot igénylő cégek, szervezetek, kormányok magasabb bit számú biztonsági réteggel dolgozhatnak. [36]

Rogue AP

A Wi-Fi hálózat egy osztott közeg, s a biztonságra, védelemre meglátásom szerint Magyarországon a kevesebb pénzből kivitelezett megoldások nyertek teret, ami által nem lesznek védve az adatok.

A Rogue AP, magyarul csaló hozzáférési pont, ami a Wi-Fi hálózatnál jelent kockázatot. A Wi-Fi kiépítésénél többféle biztonsági funkciót iktatnak be, hogy a támadásokat kivédjék. A rogue AP támadások ezekben a WLAN hálózatokban hoznak létre engedély nélkül biztonsági réseket vagy puha hozzáférési pontot, és a Wi-Fi teljesítményét csökkenthetik is. [37] Több megoldási kivitelezése lehet, melyeknél a fizikai ott létnek nem minden esetben kell már teljesülnie. Legegyszerűbben az aircrack-ng program tesztelésével mutatható be a vezeték nélküli hálózat AP kihasználhatósága. Ez egy wireless-es auditing tool, mely nem csak tesztelésre használható, hanem akár a hálózat feltörésére is és teljesen egyszerűen letölthető a netről. Windows operációs rendszerre telepíteni sem kell, mivel egy .zip fájl töltődik le és azt kell kicsomagolni. Az Airdump.ng-vel meghatározhatók a hálózatok információi (mint például a BSSID, és a Wi-Fi router MAC címe) és a felcsatlakozott klienseké is, a jelerősséggel, az elveszett csomagok számával, csak néhányat kiemelve. A jelerősség azért élvez kiemelt fontosságot, mert az okos eszközök a legerősebb jel keresésre vannak beprogramozva, így, ha a támadó erősebb jelet tud kibocsátani, mint a meglévő hálózat, amellyel kommunikál, akkor a felhasználó miután deautentikálták az alaprendszerből a támadó eszközére fog felcsatlakozni. Mivel az átmenő adatforgalom a résnek köszönhetően lehallgatható, a kliens és a szerver közti hitelesítési adatok, titkosítási kulcsok egy az egyben megszerezhetők. E rétegek után lehetőség van az Airplay-ng-vel a kliens és az AP közötti kapcsolat megszakítására. Ez egyfajta szolgáltatásmegtagadás, a Wi-Fi deauthentication, azaz hitelesítési támadás. A klienseket mivel a szerver már nem hitelesítettnek érzékeli, lecsatlakoztatja a hálózatról, így rákényszeríti a program a felhasználó eszközét, hogy a nem megfelelő csatlakozási pontot használja.

A rogue AP-ok elkerülése érdekében vezeték nélküli behatolás-megelőző rendszereket telepítenek, amelyek figyelik a nem ismert, jogosulatlan rádiófrekvenciákat. A rogue pontot a felhasználó maga is létrehozhatja abban az esetben, ha meg kívánja osztani a számítógépes vezetékes hálózati hozzáférését vezeték nélküli ügyfelekkel. Gyakori hiba, hogy a routert, amelynek a feladata, hogy a különböző vezetékes hálózatokat összekapcsolja, kiterjessze és a közöttük lezajló adatforgalmat lebonyolítsa, nem titkosítják le, nem építenek bele védelmi eszközöket, így a védett rendszerhez szinte zöld utat ad a felhasználó annak, aki jogosulatlanul szeretne hozzáférni. Ennek elkerülése a forgalommonitorozásban rejlik, mint például a rogue AP detection. Ez a kereső azonosítja a biztonságos hálózathoz csatlakozni kívánt nem engedélyezett eszközt, személyt, és elszigeteli. Ez a technika nem ütközik jogi problémákba, azonban az elhatárolása már felvet különböző jogi aggályokat. A vezeték nélküli környezetbe belépő ilyen jellegű támadások felfedezése költséges lehet, és külön figyelmet kell rá fordítani. A rogue AP detection megszünteti a szolgáltatást és „hallgatja” a jeleket, többféle megoldása létezik a megfigyelésre, egyik, hogy automatikusan vizsgálja csatornákat például 50 msként vagy kézi vezérléssel. Ezután azonosítja, hogy mely Access Point-ok rogue-ak és melyek érvényesek és része a hálózatnak. A vezérlőnek küldi el a következő összegyűjtött adatokat; a jogosulatlan felhasználó csatlakozó pontjának MAC címét, a jogosulatlan felhasználó csatlakozó pontjának a nevét, a jogosulatlan felhasználó csatlakoztatott kliensek (ami a számítógép, vagy azon futó program, mely hozzáfér a hálózathoz) MAC címét. Továbbá milyen vezeték nélküli rendszerhez kapcsolt protokollal rendelkezik az eszköz (WEP, WPA, WPA2), preamblet, amely a kezdeti szinkronizációra használt 64 bit, a jel-zaj viszonyt (signal- to-noise ratio), mely a hasznos és zavaró jel arányát fejezi ki dB-ben kifejezve, illetve a vevő-jelerősség

mutatót (RSSI). Egy riasztást generál, amely a hálózati rendszergazdához fut be. Tehát hiába ismeri fel a rendszer a behatolót, előbukkan az emberi tényező, hogy foglalkozik-e vele és milyen lépéseket tesz ez ellen, ha egyáltalán a rogue AP detectiont alkalmazzák a hálózaton. [38] Ez a gyakorlatban úgy képzelhető el, hogy egy meglévő vezetékes hálózathoz tartozik egy vezeték nélküli rendszer, mint például egyetemeknél. Fizikálisan a vezetékes végpontnál létre lehet hozni Wi-Fi magán hálózatot, melynek az SSID-je ugyanolyan nevű lesz, mint az adott, már meglévő vezeték nélküli hálózaté. Amennyiben nem érzékeli, nem készít log elemzést a Wi-Fi rendszerről, illetve monitorozás nem történik az incidensről, az idők végezetéig ki lehet használni ezt a rést, s a privát hálózaton keresztül átmenő teljes adatforgalom ellenőrizhető és irányítható.

AJÁNLÁSOK

- A VPN, virtuális magánhálózatok, használata mindig erősen ajánlott, mert ezzel a kiépített hálózattal az eredeti hálózaton keresztülmenő adatforgalom nem látható, mivel titkosítva van. Ez a megoldás nem csak titkosításra ad lehetőséget, hanem adatfolyamok elkülönítésére is. [39]
- Javasolt adatvédelmi beállításként a MAC-cím (hálózati kártya számsorozata, amely a hálózat azonosítására szolgál) szűrést érdemes használni, így csak azok a gépek tudnak csatlakozni a hálózathoz, amelyek a MAC címük alapján engedélyezve vannak. Távoli hozzáférést magánszemélyeknél kellően fontos megváltoztatni tiltás módra, ez alól kivétel, ha olyan a munkahely, ahonnan összeköttetést kell a céges és a magángépek között létrehozni. Előbb említett lehetőség a Windows 7,8 és a 8.1-es verzióján alapbeállítás volt. A távoli hozzáférés tiltását akár mobileszközről is véghez lehet vinni, ezért kell fontolóra venni, hogy szabad megváltoztathatóságot meghagyják-e a drótnélküli adminisztrációnak. Ezáltal csak az tud változtatni a router beállításain, aki közvetlenül csatlakozik hozzá. [40]
- Megfelelő biztonsági intézkedések a különböző vezeték nélküli eszközök világában (1. számú táblázat)

	Titkosítás	**Hitelesítés**	**VPN**	**Zárolás és távoli hozzáférés**	**Hozzáférés szabályozás**
Viselhető intelligens eszközök (szemüveg, okos órák)	X	X			
Otthoni okos eszközök (riasztó rendszer)	X		X		
Applikációk	X				X
Felhő alapú eszközvezérlés (okostelefon, tablet)				X	

[41]

1. számú táblázat: Megfelelő biztonsági intézkedések a különböző vezeték nélküli eszközök világában, (saját szerkesztés)

- Hotspoton keresztül történő adatforgalomra érdemes a client isolation biztonsági funkciót használni. Ez megakadályozza a vezeték nélküli ügyfelek kommunikálást egymással. [42]

KÖVETKEZTETÉSEK

Az információs és kommunikációs technológiák komplexen érintenek mindenkit és a terjedő wireless-es technológiák új típusú biztonsági felkészültséget kívánnak, mely hiányzik a felhasználók oldaláról is. A kiberbűnözés célpontjainak jelentős részét az egyének adják, mint például a hallgatók. Ez a korosztály legtöbbet pubokban, gyorséttermekben, publikus nyílt Wi-Fi hálózattal rendelkező helyeken, hotspotok mentén fordulnak meg és csatlakoznak fel a Wi-Fi-re. A felhasználók legtöbbször nincsenek tisztában azzal, hogy milyen hálózatra lépnek fel. A hipotézisem, hogy a felhasználok a Wi-Fi hálózatokon keresztül történő adatforgalombiztonsága ismereteinek hiányával küzdenek, ami valós probléma. Az általam vizsgált két pont, a WPA2 hiányossága és a Rogue AP-ok, a kliensek által igen nehezen észrevehető veszélyforrások, ezért fontos ismerniük. A problémák legtöbbször három esetben jelentkeznek, amikor nincs teljes lefedettségű Wi-Fi hálózat, illetve a jelerősség nem megfelelő, és ezt használja ki a támadó, egy erősebb jelerősségű eszközzel, vagy a hálózaton nincsen detektálás, illetve, ha van detektálás, azonban emberi mulasztás miatt nem valósul meg a védelem. A Rogue AP-ok engedély nélküli biztonsági rések, ahol a felcsatlakozott eszközök adataihoz könnyen hozzá lehet férni, majd a kapcsolatot a kliens és a szerver között a támadó megszakítja (Wi-Fi deauthentication), majd a felhasználó eszközét kényszeríti a csaló hozzáférési ponthoz való csatlakozásra. Ez ellen a szervezet és az egyén is védekezhet. A szervezet felől az úgynevezett Rogue AP detection, behatolás-megelőző rendszerrel lehet kiváló védelmet biztosítani, avagy hozzáférés szabályozást alkalmazni, amellyel a nem rendszergazdai szintű hozzáférők nem oszthatják meg a hálózatot külső személlyel, eszközzel. Privát oldalról a többfaktoros hitelesítést és titkosítást sem szabad figyelmen kívül hagyni. Bármilyen hálózat használat esetén a VPN hálózat használata, MAC szűrés, avagy client isolation technikák jó megoldások lehetnek bárki számára, azonban, hogy figyelmet fordítson a felhasználó adatai biztonságba helyezésére, ahhoz először meg kell győzni, hogy fontos adatok birtokában van, és védeni kell ezeket.

FELHASZNÁLT IRODALOM

[1] WANT, R.- DUSTDAR, S.: *Activating the internet of things [guest editors'introduction*],” Computer, vol. 48, no. 9, pp. 16–20, 2015.

[2] KOSKA Melinda: Wi-Fi hálózatok biztonsági kockázata, NKE, 2018

[3] International Telecommunication Union: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, (letöltve: 2018.02.20)

[4] KIFÜ: Közérthetően az IT biztonságról http://kifu.gov.hu/sites/default/files/IT_brosura_v7.pdf, 7, (letöltve: 2018.02.20.)

[5] Origo: Bírság járhat a nyitott wifiért Németországban. http://www.origo.hu/techbazis/internet/20100514-birsag-jarhat-a-nyitott-wifiert-nemetorszagban.html, (letöltve: 2018.02.20.)

[6] GUBBI, J. et.al*: Internet of things (iot): A vision, architectural elements, and future directions*, Future Generation Computer Systems, vol. 29, no. 7. 1645–1660, 2013.

[7] ALKAR, A.- BUHUR, U.: *An Internet based wireless home automation system for multifunctional devices*, IEEE Transactions on Consumer Electronics 51 1169–1174, 2005.

[8] DARIANIAN, M.- MICHAEL, M.P.: *Smart home mobile RFID-based Internet-ofThings systems and services*, in: 2008 International Conference on Advanced Computer Theory and Engineering, 2008, 116–120.

[9] AIREHROUR, D. et. al.: S*ecure routing for internet of things: A survey*, Journal of Network and Computer Applications, vol. 66, 198–213, 2016

[10] EMMERSON B.: *M2M: the Internet of 50 billion devices*, Huawei Win-Win Magazine Journal (4) (2010) 19–22.

[11] MIORANDI, D. et. al.: *Internet of things: Vision, applications and research* challenges, Ad Hoc Networks, vol. 10, no. 7,1497–1516, 2012.

[12] DA XU, L.: *Enterprise systems: state-of-the-art and future trends*, IEEE Transactions on Industrial Informatics, vol. 7, no. 4, 630–640, 2011.

[13] PANG, Z. et.al.: *Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things*, in Advanced Communication Technology (ICACT), 2013 15th International Conference on. IEEE, 2013, 529– 534.

[14] MISRA, S. et. al.: Security challenges and approaches in internet of things,2016

[15] DOMINGO, M. C.: *An overview of the internet of things for people with disabilities*, Journal of Network and Computer Applications, vol. 35, no. 2, 584–596, 2012.

[16] ZHOU, H. et. al.: *Design and research of urban intelligent transportation system based on the internet of things*, in Internet of Things. Springer, 2012, 572–580.

[17] Google-fiók Súgó: https://support.google.com/accounts/answer/1733224?hl=hu, (letöltve: 2018.02.20.)

[18] ASHTON, K.: *That ''Internet of Things'' thing*, RFiD Journal, 2009.

[19] ABC News: Amazon says it's working to fix Alexa's laughing problem http://abcnews.go.com/GMA/News/amazon-working-fix-alexas-laughing-problem/story?id=53594464, (letöltve: 2018. 04. 10.)

[20] Wi-Fi Alliance: https://www.wi-fi.org/who-we-are, (letöltve: 2018.03.30.)

[21] ILLÉSI Zsolt: *Wifi hálózatok igazságügyi szakértői elemzése: Wifi hálózatok felderítése*. In Hadmérnök, 2009. szeptember 3. http://hadmernok.hu/2009_3_illesi.pdf, (letöltve: 2018. 03.15.)

[22] SADOSKI, D.: *Client/Server Software Architectures – An Overview*, Software Technology Roadmap, 1997-08-02.

[23] JUNIPER Networks: Tech Library https://www.juniper.net/documentation/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-ssid-bssid-essid.html#jd0e46, (letöltve: 2018.03.30.)

[24] SZABÓ Bálint- MÁRFÖLDI Endre: *Számítógépes hálózatok*. http://www.tankonyvtar.hu/hu/tartalom/tamop425/0005_24_szamitogepes_halozatok_scorm_03/333_az_osi_modell.html, (letöltve: 2018.03.30.)

[25] HupWiki: Információs háttértár https://wiki.hup.hu/index.php/Datagram-orient%C3%A1lt_kommunik%C3%A1ci%C3%B3s_protokoll

[26] HupWiki: Információs háttértár https://wiki.hup.hu/index.php/ICMP, (letöltve: 2018.03.30.)

[27] HupWiki: Információs háttértár https://wiki.hup.hu/index.php/TCP, (letöltve: 2018.03.30.)

[28] HupWiki: Információs háttértár
https://wiki.hup.hu/index.php/IMAP,(letöltve: 2018.03.30.)

[29] HupWiki: Információs háttértár
https://wiki.hup.hu/index.php/POP3,(letöltve: 2018.03.30.)

[30] HupWiki: Információs háttértár
https://wiki.hup.hu/index.php/SMTP, (letöltve: 2018.03.30.)

[31] VANHOEF, M.- PIESSENS, F.: *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2*. In Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS). ACM 2017

[32] PC WORLD: *Így törhető fel bármelyik titkosítás*
https://pcworld.hu/szoftver/igy-torheto-fel-barmelyik-titkositas-138341.html, (letöltve: 2018.03.30.)

[33] HEGYESHALMI Richárd: *Óriási gond van a wifi biztonsággal*
https://index.hu/tech/2017/10/16/oriasi_gond_van_a_wifi_biztonsagaval/, (letöltve: 2018.03.30.)

[34] BBC News: *Wi-fi security flaw 'puts device at risk of hacks'*
http://www.bbc.com/news/technology-41635516, (letöltve: 2018.03.30.)

[35] CERT Software Engineering Institue: *Vendor Information for VU#228519*
https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4, (letöltve: 2018.03.30.)

[36] Gdata: *Biztonságosabb lesz a vezeték nélküli internet*
https://virusirto.hu/blogbejegyzesek/2018/01/12/biztonsagosabb-lesz-a-vezetek-nelkuli-internet/, (letöltve: 2018.03.30.)

[37] MARECO, D.: Rogue AP Detection: What Is It & Why Your WLAN Design Needs It
https://www.securedgenetworks.com/blog/rogue-ap-detection-what-is-it-why-your-wlan-design-needs-it, (letöltve: 2018.02.20.)

[38] CISCO: Rogue Detection under Unified Wireless Networks
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70987-rogue-detect.html, (letöltve: 2018.02.20.)

[39] SZIGETVÁRI Zoltán: *A VPN-ről*
https://www.itkommando.hu/site/a-vpn-rol/ (letöltve: 2018.03.30.)

[40] GData: *Hogyan védjük meg a wifi hálózatunkat?*
https://virusirto.hu/blogbejegyzesek/2015/04/26/hogyan-vedjuk-meg-a-wifi-halozatunkat/ (letöltve: 2018.03.30.)

[41] CTIA: *The Wireless Association*. Mobile Cybersecurity and the Internet of Things Empowering M2M Communication. (2014, December 2, 2014).
http://www.ctia.org/docs/default-source/default-document-library/ctia-iot-white-paper.pdf (letöltve: 2018.03.30.)

[42] CISCO: *Wireless Client Isolation*
https://documentation.meraki.com/MR/Firewall_and_Traffic_Shaping/Wireless_Client_Isolation (letöltve: 2018.04.15.)