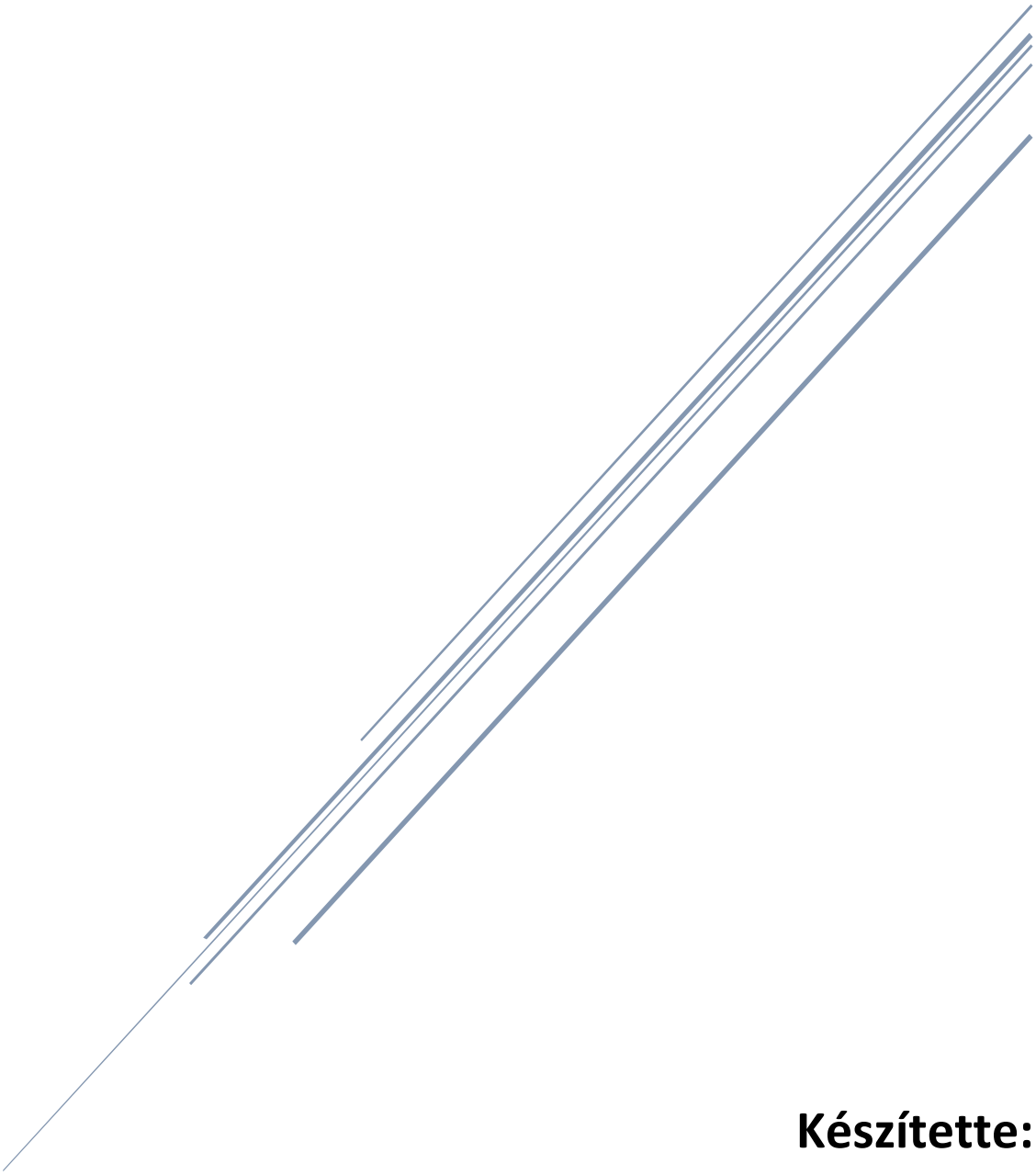
WPA-2 SÉRÜLÉKENYSÉGE

Biztonság és védelem a számítástechnikában



Készítette:

Név: *Szalai Márton*

Neptun kód: *DTKUG0*

Bevezetés

A mai modern világban úgy tűnik, hogy szinte lehetetlen lenne a mindennapjainkat élnünk vezeték nélküli internet elérése nélkül. Az emberek mindenhol a WiFi-re támaszkodnak, a szórakozástól kezdve, a munkán át, egészen a beszélgetésekig. Viszont ez önmagában veszélyt is rejt, ugyanis a hackerek biztonsági réseket, hiányosságokat kihasználva hozzáférhetnek a személyes adatainkhoz.

Amilyen ütemben fejlődik a technika, ahol már akár a hűtőszekrényünk is vezeték nélküli kapcsolattal működik, egyre fontosabbá válik, hogy minél biztonságosabbá tegyük hálózatunkat. Itt jön be a képbe a „Wireless Security”, azaz a vezeték nélküli biztonság.

Vezeték nélküli hálózatok védelme

A hálózatvédelem alatt azt értjük, hogy megvédjük az otthoni eszközeinket attól, hogy idegenek elérhessék azokat, vagyis biztosítja, hogy adataink csak azok számára legyen elérhető, akiknek ehhez előzetesen engedélyt adtunk. Ehhez különböző protokollok léteznek.

Két nagyobb csoport vezeték nélküli biztonsági protokollt különböztetünk meg, úgymint a Wired Equivalent Privacy (WEP), azaz Vezetékessel Egyenértékű (Biztonságú) Hálózat, és a
Wi-Fi Protected Access (WPA) hitelesítési biztonsági protokoll, amelyet a Wi-Fi szövetség alkotott. Ezeken belül négy különböző protokollt különböztetünk meg:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA 2)

- Wi-Fi Protected Access 3(WPA 3)

WPA/WPA2

A WPA-t a Wi-fi Szövetség, egy ipari-kereskedelmi csoport hozta létre, amely a „Wi-Fi” védjegy tulajdonosa és az ilyen védjegyet viselő eszközök hitelesítője.

A WPA az IEEE 802.1x-hitelesített kiszolgálókkal való együttműködésre lett kialakítva, amely különböző kulcsot rendel mindegyik felhasználóhoz, annak ellenére, hogy használható a kevésbé biztonságos "osztott kulcs” – pre-shared key (PSK) – módban is, ahol minden felhasználónak ugyanaz a kulcsa a hálózati hozzáféréshez. A WPA tervezésének alapja az IEEE 802.11i szabvány 3. számú vázlata volt.

Az IEEE 802.11 egy vezeték nélküli adatátviteli protokoll. Az OSI modell (Nyílt rendszerek összekapcsolása referenciamodellje) két legalsó rétegét, a fizikai és az adatkapcsolati réteget definiálja.

Az IEEE 802.11i szabványt 2004 júniusában fogadták el, amely már külön biztonsági előírásokat tartalmaz. Fő célja az volt, hogy a megjelenésével eltűnjenek a korábbi biztonsági elmaradások. Ez a szabvány adattitkosításra már az AES-t (Advanced Encryprtion Standard) használta. Biztonsági szempontból előírta továbbá a WPA (Wi-Fi Protected Access) protokoll használatát.

A Wi-Fi Szövetség által létrehozott WPA tette lehetővé a biztonságos vezeték nélküli hálózati eszközök fejlesztésének megkezdését, amíg az IEEE 802.11i csoport befejezi a szabvány elkészítését. A Wi-Fi Szövetség ekkora már előkészítette a WPA2 szabványt is, ami már az IEEE 802.11i szabvány végleges vázlatára épült, ezért az alkalmazott jelölések a keret mezőkben (Információ Alapfogalmak vagy IE-k) szándékosan különböznek a 802.11i szabványban alkalmazottaktól, hogy elkerüljék az inkompatibilitásokat az egyesített WPA/WPA2 elkészítésekor.

WPA2-be beépítették a 802.11i. szabvány főbb jellemzőit, főleg a TKIP-t és a Michael algoritmust, továbbá egy új AES-alapú algoritmust, a CCMP-t, mellyel teljesen biztonságossá tették. Így 2006. március 13-ától kezdődően gyártott minden vezetéknélküli eszköz kötelezően a WPA2 szabvány szerint készült, tehát „Wi-Fi”-jelöléssel ellátott.

Összefoglalva a fejlesztéseket az elődjéhez képest:

- TKIP (Temporal Key Integrity Protocol) bevezetése. Ez valósítja meg a dinamikus kulcs cserét, amely biztosítja, hogy minden csomag egy egyedileg titkosított kulccsal legyen elküldve. 2008-ban viszont a hibát találtak benne, 2012-ben pedig a szabványból is kivették.
- Megnövelték az inicializációs vektor méretét azért, hogy ne legyen IV ismétlődés mint ahogy a WEP esetében volt. (24-ről 46 bitre)

- Növelték a minimális kulcs méretet is 40-ről 256 bitre.
- Bevezették az osztott kulcsmódot (PSK) ami lehetővé teszi, hogy jelszót (jelmondatot) használjunk a szabványoknál. Ennek 8-63 darab ASCII karakterből (egy hash-függvény csökkenti le az 504bites(63*8bit/karakter) hosszúságot 256-ra) vagy 64 darab hexadecimális számból kell állnia. (összesen 256 bit)
- Továbbá 2006-ban megjelent még egy új (kiegészítő) szabvány a WPS (Wifi Protected Setup). Az alap koncepció az lett volna hogy az otthoni felhasználóknak nyújtsanak egy egyszerű csatlakozási lehetőséget. Egy 8 számjegyű PIN-t használ, viszont mivel az utolsó számjegy a többinek az ellenőrző összege (checksum-ja) így 7 ismeretlen számjegy van minden PIN-ben. (Ami 10^7-en = 10,000,000 lehetséges kombinációt jelent.)

Titkosítás

A WPA2, bár nem tökéletes, jelenleg a legbiztonságosabb választás. A Temporal Key Integrity Protocol (TKIP) és az Advanced Encryption Standard (AES) a WPA2 által biztosított hálózatokban használt két különböző titkosítási típus. Nézzük meg, hogyan különböznek egymástól és melyik a legjobb.

A TKIP és az AES két különböző típusú titkosítás, amelyeket Wi-Fi hálózat használhat. A TKIP valójában egy régebbi titkosítási protokoll, amelyet a WPA-val vezetett be a nagyon bizonytalan WEP-titkosítás helyett. A TKIP elég hasonló a WEP titkosításhoz. A TKIP már nem tekinthető biztonságosnak, és most már elavult. Más szóval, nem szabad használni.

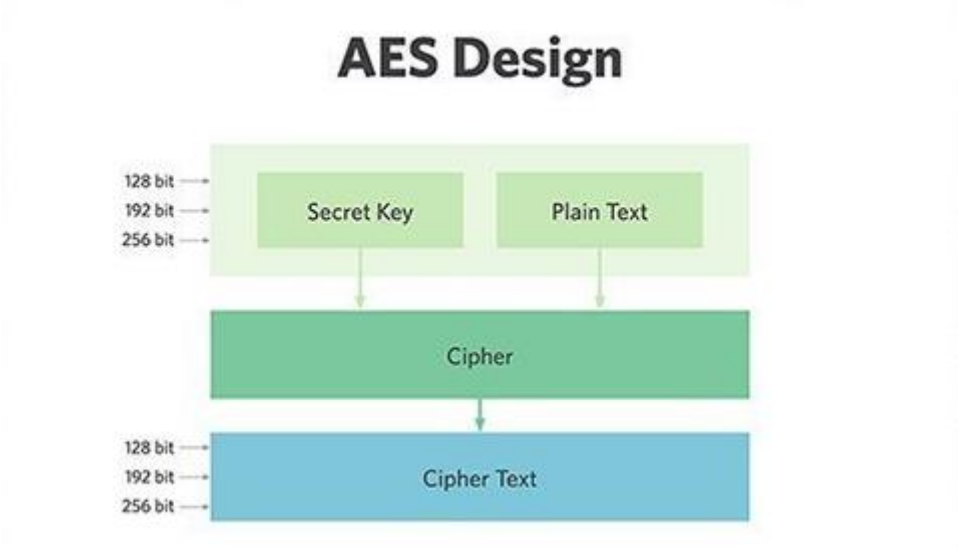
Az AES egy biztonságosabb titkosítási protokoll a WPA2 segítségével. Az AES nem is egy kifejezetten Wi-Fi hálózatokra kifejlesztett szabvány. Ez egy komoly világméretű titkosítási szabvány, amelyet még az amerikai kormány is elfogad. Például, ha a merevlemezt a TrueCrypt segítségével titkosítjuk, akkor az AES titkosítást használhatja. Az AES-t általában nagyon biztonságosnak tartják, és a fő gyengeségek a „brute force” támadások (erős jelszó használatával megakadályozott) és a WPA2 egyéb aspektusainak biztonsági gyengeségei.

A rövid változat az, hogy a TKIP egy régebbi titkosítási szabvány, amelyet a WPA szabvány használ. Az AES egy újabb Wi-Fi titkosítási megoldás, amelyet az új és biztonságos WPA2 szabvány használ. Elméletileg ez a vége. Az útválasztótól függően előfordulhat, hogy a WPA2 kiválasztása nem elég jó.

Míg a WPA2-nak az AES-t használnia kell az optimális biztonság érdekében, a TKIP-et is használhatja, ahol a régi eszközökkel való kompatibilitás szükséges. Ilyen állapotban a WPA2-t támogató eszközök csatlakoznak a WPA2-hez, és a WPA-t támogató eszközök csatlakoznak a WPA-hoz. Tehát a „WPA2” nem mindig jelenti a WPA2-AES-t. Azonban a látható „TKIP” vagy „AES” opció nélküli eszközöknél a WPA2 általában a WPA2-AES-szel azonos.

AES (Advanced Encryption Standard)

Az AES a Rijndael kódolás olyan változata, ahol a blokkméret szigorúan 128 bit, a kulcs pedig 128, 192 vagy 256 bit. Összehasonlításként a Rijndael kódolásban a blokkméret és a kulcsméret is lehet 32 bit tetszőleges többszöröse azzal a kikötéssel, hogy mind a kulcs, mind a blokkméret minimum 128 és maximum 256 bit lehet.



Az AES 4x4-es mátrixokat használ a titkosítás során, habár más blokkméret esetén más a mátrix mérete is.

A kulcsméret meghatározza, hogy a bemeneti információt hány átalakítási ciklus éri, míg eléri a „végleges” titkosított állapotát. A titkosítási ciklusok száma a következőképpen alakul:

- 10 ciklus 128 bites kulcs esetén.
- 12 ciklus 192 bites kulcs esetén.
- 14 ciklus 256 bites kulcs esetén.

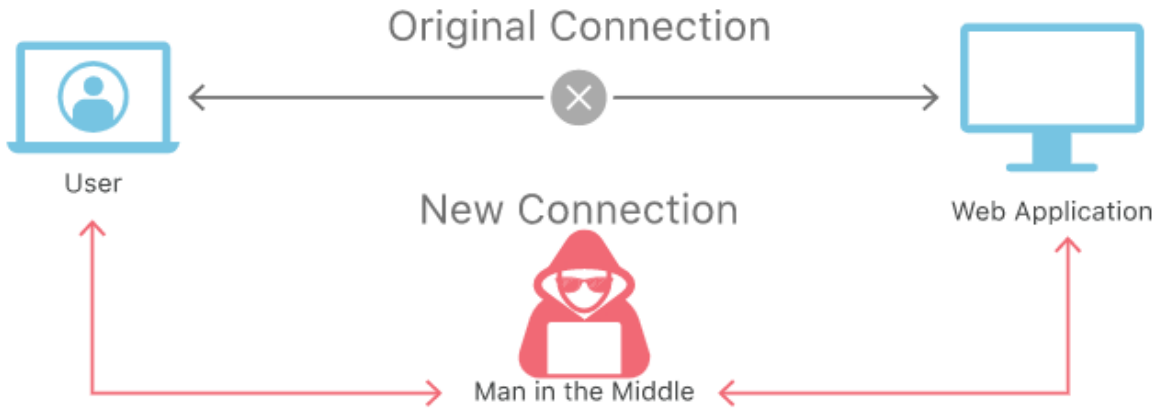
Minden ciklus számos lépést foglal magába, ezek között van az a lépés is, ami kulcs alapján módosítja a mátrixot. A visszaalakítás során ugyanennyi ellentétes ciklust hajtanak végre a kulcs segítségével.

Biztonságossága:

2009 májusáig az egyetlen sikeres publikált támadás a teljes AES ellen egy specifikus támadás bizonyos implementációk ellen. Az NSA átnézte az AES összes végső jelöltjét, beleértve a Rijndael titkosítást és úgy találta, hogy mindegyik megfelelő az USA kormánynak a nem-titkosított (jogi értelemben) adatok titkosítására. 2003 júniusában az USA kormánya is bejelentette, hogy az AES használható a titkosított információk (jogi értelemben vett) védelme érdekében is

WPA2 sebezhetősége

A WPA2 egy évtizeden át ellenállt a rajta biztonsági gyengeségeket kereső vizsgálatoknak. Az egyetlen problémát a gyenge jelszó használata okozhatta, de ez ellen sajnos nem nagyon lehet védekezni. Azonban 2017. októberében 2 belga kutató, Mathy Vanhoef és Frank Piessen bejelentette, súlyos hibát találtak a protokollban. A problémát nem egy gyártói implementációs hiba okozta, a baj magával a protokollal volt. A Key Reinstallation Attack (KRACK) egy közbeékelődéses támadás (man-in-the-middle attack - MitM), amely a különböző kézfogásokat támadja, és közben azt a tényt használja ki, hogy bár ezek a kézfogások és az AES-CCMP külön-külön formálisan bizonyíthatóan biztonságosak, a kettő ötvözése mégis lehetőséget ad hibákra.



A támadási működése:

A Krack támadás a WPA2 protokoll négyutas folyamatára irányul, amely akkor fordul elő, amikor az ügyfél csatlakozni kíván egy védett Wi-Fi hálózathoz, és annak megerősítésére szolgál, hogy mind az ügyfél, mind a hozzáférési pont helyes hitelesítő adatokkal rendelkezik.

Ezzel a négyirányú eljárással új titkosítási kulcs kerül tárgyalásra, amelyet az összes későbbi forgalom titkosítására használnak. Jelenleg minden modern Wi-Fi-vel védett hálózat használja a négyirányú összeköttetési protokollt, ami azt jelenti, hogy ezeket a hálózatokat a Krack támadás vagy annak valamilyen változata befolyásolja. Például a támadás személyes és üzleti Wi-Fi hálózatokkal, az előző WPA és a legújabb WPA2 szabvány ellen, és még olyan hálózatok ellen is működik, amelyek csak AES titkosítást használnak. A WPA2 elleni támadások újszerű technikát használnak, az úgynevezett kulcs újratelepítési támadásnak (KRACK), amely a következő lépésekből áll:

- Kulcsfontosságú újratelepítési támadások: magas szintű leírás

Kulcs-újratelepítési támadás esetén a támadó becsapja az áldozatot egy már használt kulcs újratelepítésébe. Ezt kriptográfiai üdvözlő üzenetek manipulálásával és reprodukálásával érik el. Amikor az áldozat újratelepíti a kulcsot, a hozzá tartozó paraméterek, például az átadott csomag száma és a vételi csomagszám visszaállnak a kezdeti értékükre. Alapvetően a biztonság érdekében a kulcsot csak egyszer kell telepíteni és használni. Sajnos a WPA2 protokoll nem garantálja ezt a gyakorlatot.

- Legfontosabb újratelepítési támadások: konkrét példa a WPA2 négyirányú folyamata ellen

Amikor az ügyfél csatlakozik egy Wi-Fi hálózathoz, futtatja a négyirányú linket egy új titkosítási kulcs megtárgyalására. Ezt a kulcsot telepíti, miután megkapta a 3. üzenetet a négyirányú linktől, és miután a kulcs telepítve lett, a normál adatkeretek titkosításához fogja használni egy titkosítási protokollt.

Mivel azonban az üzenetek elveszhetnek vagy elvethetők, az Access Point (AP) továbbítja a 3. üzenetet, ha nem kapott megfelelő választ, mint kézhezvétel visszaigazolást. Ennek eredményeként az ügyfél többször is fogadhatja a 3. üzenetet, és minden alkalommal, amikor megkapja ezt az üzenetet, újratelepíti ugyanazt a titkosítási kulcsot, és ezért alaphelyzetbe állítja a növekményes átviteli csomag számát, és megkapja a lejátszó által használt lejátszószámlálót. titkosítási protokoll

Ennek eredményeként az átviteli csomag újbóli felhasználásának kényszerítésével és ily módon a titkosítási protokoll megtámadható, például a csomagok visszajátszhatók, visszafejthetők és / vagy hamisíthatók. Ugyanez a

technika használható a csoportkulcs, a PeerKey, a TDLS és a gyors BSS átmeneti kapcsolat megtámadására.

A csomagok visszafejtése lehetséges, mert a kulcs újratelepítési támadása miatt az átviteli számok (más néven csomagszámok vagy inicializálási vektorok) nullára állnak. Ennek eredményeként ugyanaz a titkosítási kulcs kerül felhasználásra az átviteli csomagok értékeivel, amelyeket a múltban már használtak. Ennek következtében az összes WPA2 titkosítási protokoll újrafelhasználja a kulcsáramlást, amikor a csomagok titkosítása lehetővé teszi a Krack támadás megkönnyítését.

A csomagok visszafejtésének képessége felhasználható a TCP SYN csomagok dekódolásához, ezáltal lehetővé téve az ellenfélnek, hogy megkapja a kapcsolatok TCP sorszámát, és eltérítse a TCP kapcsolatokat. Ennek eredményeként, még ha a WPA2 is védett minket, az ellenfél a leggyakoribb támadásokat kezdeményezheti a nyílt Wi-Fi hálózatok ellen: rosszindulatú adatokat fejthet be a titkosítatlan HTTP kapcsolatokba. A támadó például kihasználhatja ezt a helyzetet, hogy ransomware vagy rosszindulatú szoftvert juttathat az áldozatok által meglátogatott és nem titkosított webhelyekre.
Ha az áldozat az AES-CCMP helyett a WPA-TKIP vagy a GCMP titkosítási protokollt használja, a hatás kritikusabb.

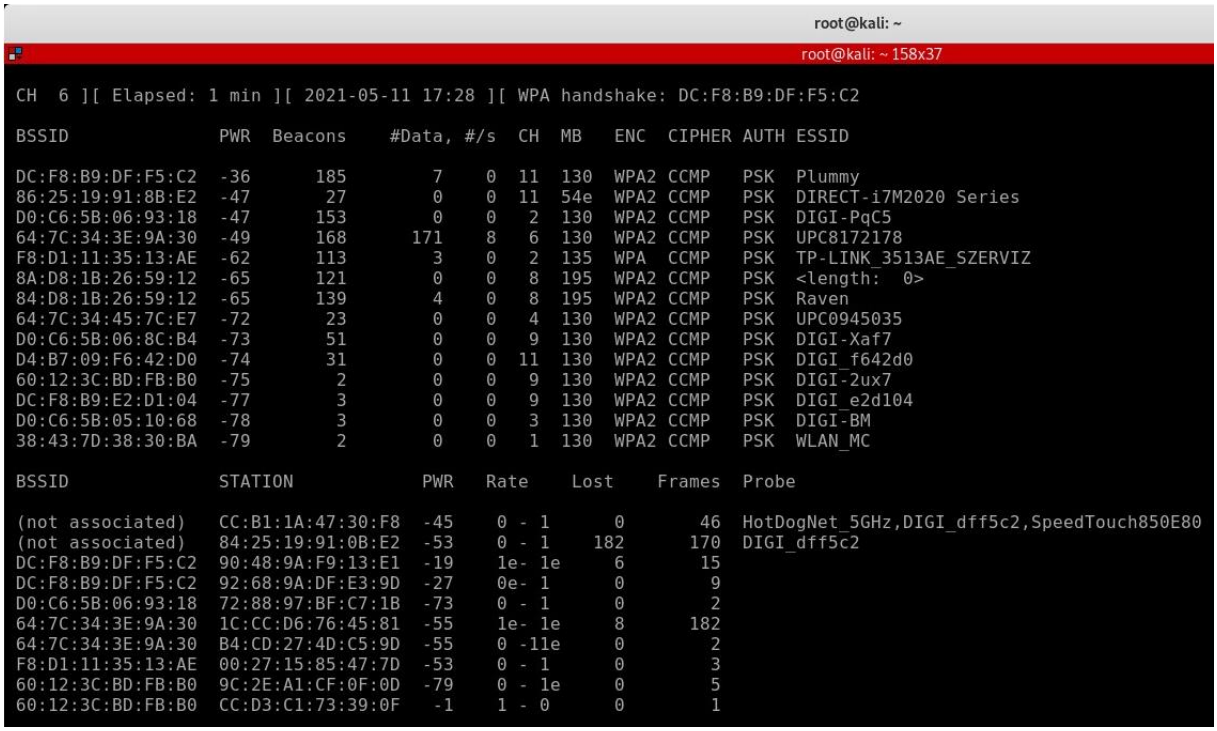
A támadás létezése meghökkentő volt. Mathy Vanhoef saját elmondása szerint a publikálás előtt egy évvel, a PhD dolgozatának megvédésekor még magabiztosan állította, hogy a WPA2 sebezhetetlen. Az ott kapott kérdés sarkallta arra, hogy alaposabban is megvizsgálja a protokollt. Miután a gyengeséget felfedezte, először természetesen az illetékes szervezeteket értesítette: a Wi-Fi Alliance-t, illetve a gyártókat. Ennek megfelelően mire megtörtént a publikáció, az eszközök egy része már megkapta a megfelelő biztonsági frissítéseket. Sajnos azonban megeshet, és ez az okostelefonok piacára különösen jellemző, hogy a gyártók hátrahagyják a készülékeket, és ezek a megjelenésüktől számítva egy, legfeljebb két évig kapnak csak biztonsági frissítéseket. Így könnyen előfordulhat, hogy egy-egy három évnél idősebb eszköz a mai napig sebezhető.

Feltörés a gyakorlatban

Ahogy azt az előző bekezdésekben is említettem, a legnagyobb problémát a gyenge jelszó jelentheti egy-egy vezeték nélküli hálózat védelménél. Úgy gondolom jó ellenpéldát mutathat az, ha a gyakorlatban is bemutatom, menyiből tart egy ilyen hálózat feltörése. Ehhez mindösszesen elég egy USB Wi-Fi sticket vásárolnunk, valamit a Kali Linuxot feltelepíteni a számítógépünkre.

Ezen Linux disztribúció számos olyan extra programot tartalmaz, amely a hálózatok teszteléséhez, megfigyeléséhez hasznos lehet.

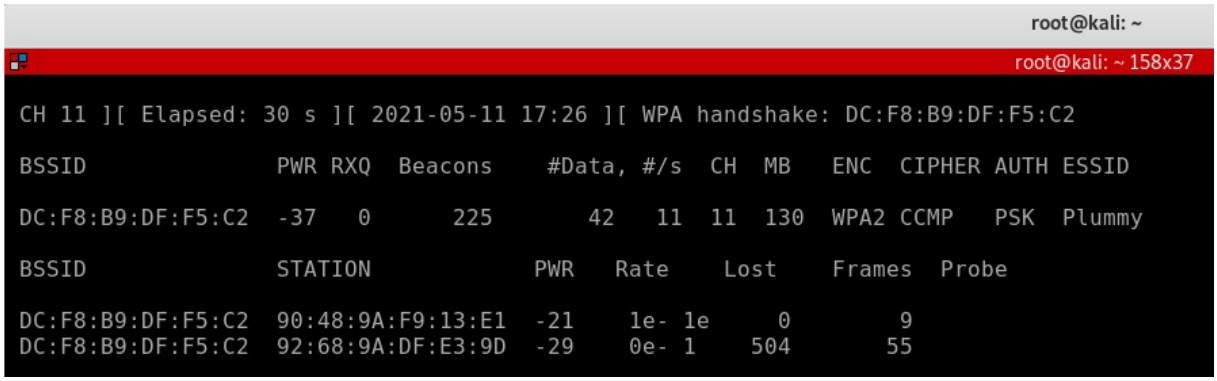
Első lépésként listázzuk az elérhető hálózatokat:



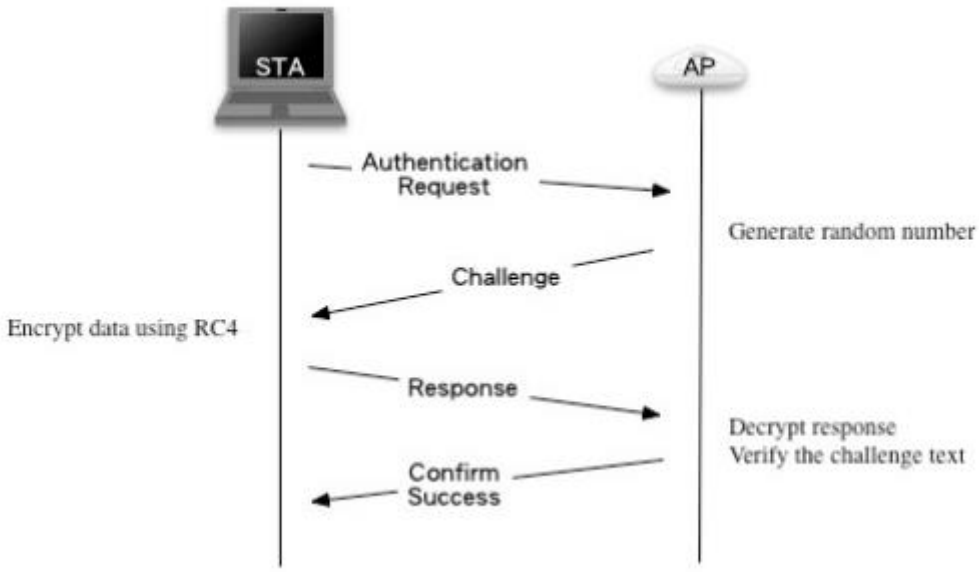
Ahogy az a képen is látható, számos hálózat található hatótávolságon belül, különböző információkkal. Ami számunkra a legfontosabb itt, az a BSSID, azaz Basic Service Set Identification, ez a WAP MAC-címe.

Az ESSID (Extended Service Set Identification) a vezetéknélküli hálózat neve, illetve a CH, ami a csatornát jelenti.

A következő lépésben klienseket keresünk, és a köztük és a router közötti összes kommunikációt egy .cap fájlba mentjük. A WPA handshake-et (WPA kézfogás) akarjuk ezzel megszerezni. Ehhez természetesen a saját hálózatomat vettem célba.



A WPA handshake akkor történik meg, amikor egy kliens csatlakozni akar egy védett Wi-Fi hálózathoz. Ennek során egyezik meg a kliens a hálózati vezérlővel az új titkosítási kulcsról. Amikor a kliens megkapja a kulcsot, telepíti, és azzal titkosítja az adatcsomagokat.



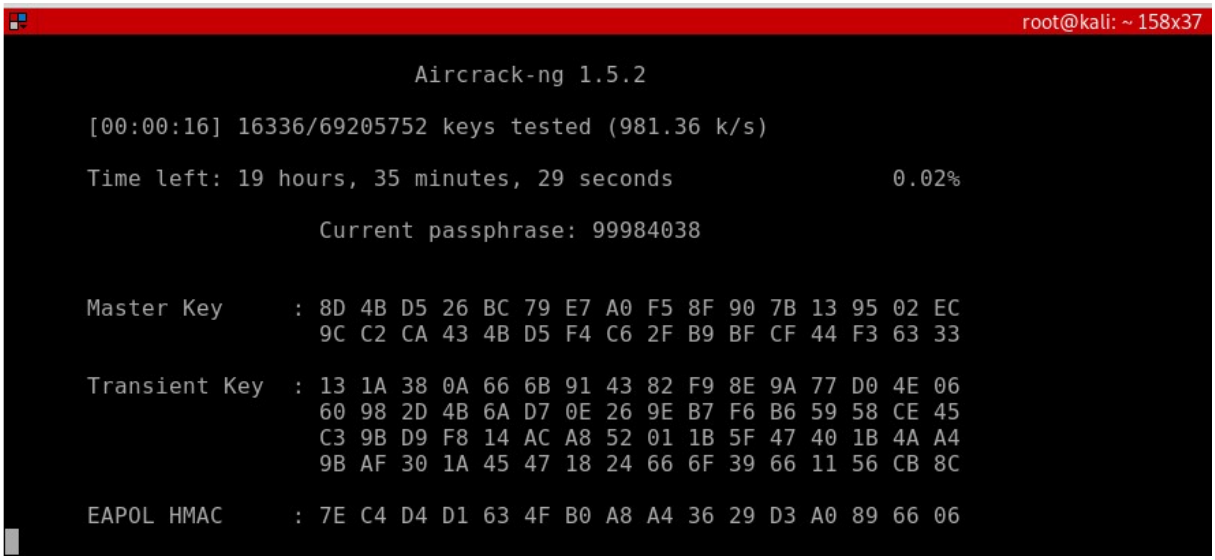
Maga a WPA handshake nem tartalmaz adatot, amivel elő lehet állítani a jelszót, csak abban segít, hogy megvizsgáljunk egy kulcsot, hogy az megfelelő-e, vagy sem.

Utolsó lépésként a .cap fájlunk segítségével fogjuk megkeresni a helyes jelszót egy szótárfájl segítségével. A szótárfájlt mi magunk hozunk létre, amely a lehetséges jelszavak tartalmazza.

```
root@kali:~# crunch 6 8 0123456789 -o codes.txt
Crunch will now generate the following amount of data: 987000000 bytes
941 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 111000000

crunch:  38% completed generating output

crunch:  63% completed generating output

crunch:  97% completed generating output

crunch: 100% completed generating output
root@kali:~#
```

A könnyebb bemutatás érdekében a hálózat jelszavát előzetesen „12345678”-ra állítottam be. A crunch paranccsal 6-8 hosszúságú szavakat hoztam létre, amely csak számokat tartalmaz, de már ez is 111 millió különböző sort jelent, amely 941 MB-nyi helyet igényel.

Innentől kezdve már csak annyi dolgunk van, hogy futtassuk azt a programot, amely minden egyes lehetséges jelszót megvizsgál a .cap fájl segítségével, és megkeresi a jelszót.



Fontos megjegyezni, hogy ez egy speciális eset, mivel csak a legminimálisabb követelményeknek tesz eleget a jelszó. Amennyiben csak betűkből álló jelszavunk van, már más a helyzet:

```
root@kali:~# crunch 6 8 qwertyuiopasdfghjklzxcvbnm -o test.txt
Crunch will now generate the following amount of data: 1945860473024 bytes
1855717 MB
1812 GB
1 TB
0 PB
Crunch will now generate the following number of lines: 217167790528
```

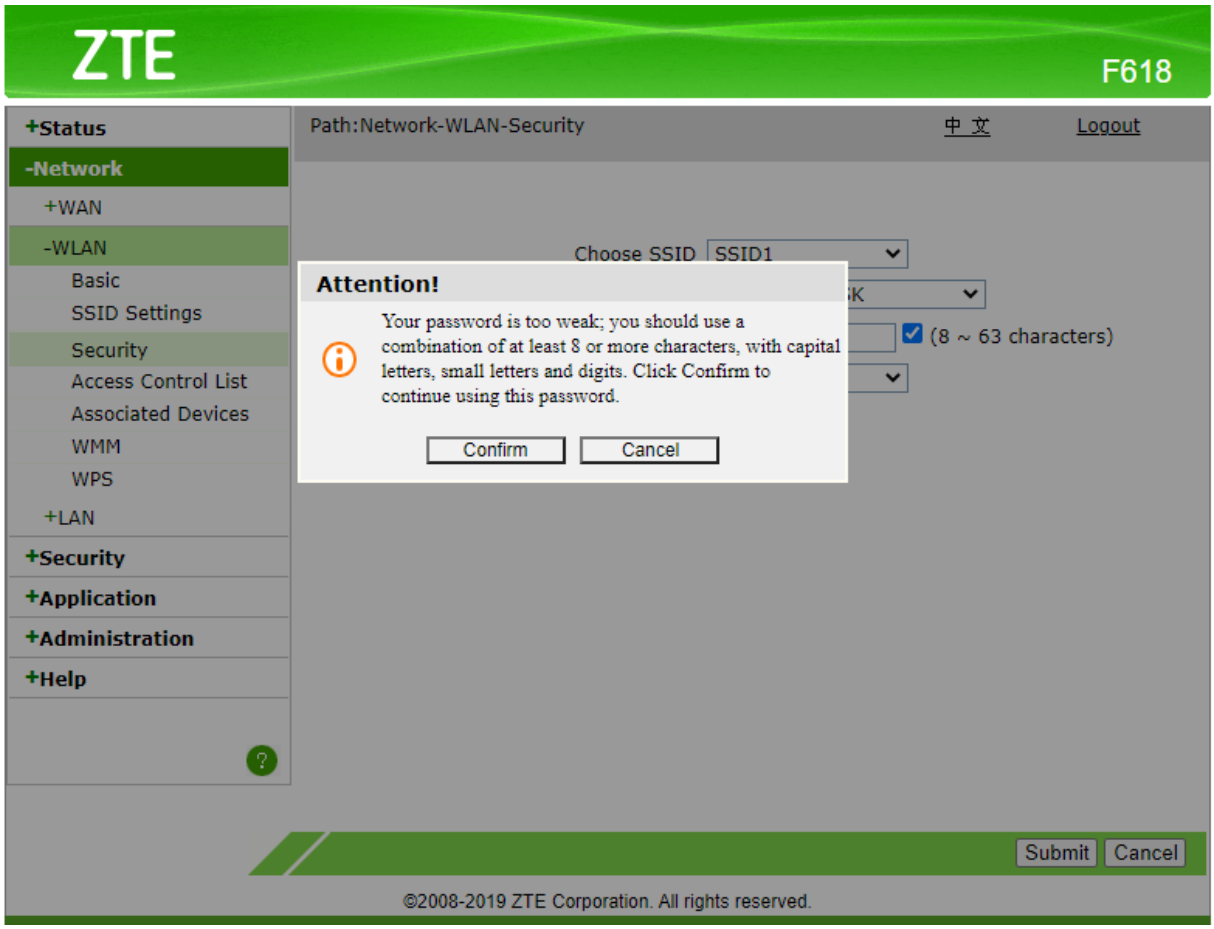
Itt már 6 és 8 karakter hosszúságú szavakat generáltam az angol abc betűiből, és látható, hogy ez már jelentős helyet igényel. A biztonságosságtól még ez is távol áll, hiszen a jelszó megkereséséhez már nem kell a hálózat közelében lennünk, megfelelően erős hardver és elegendő tárhellyel csak idő kérdése a kulcs megtalálása.

Érdekességképpen megvizsgáltam, hogy egy kellően erős jelszóhoz, ami 16 karakterből áll, tartalmaz kis és nagybetűket, valamint egy speciális karakter, mekkora szótárfájlra lenne szükség:

```
root@kali:~# crunch 16 16 qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM! -o plummypwd.txt
Crunch will now generate the following amount of data: 8952128115722681041 bytes
8537414661142 MB
8337319005 GB
8141913 TB
7951 PB
Crunch will now generate the following number of lines: 4867006141797699265
```

Ahogy az a mellékelt ábrán is látható, a rendszer egy több mint 8 millió terabájtos fájlt hozott volna létre, amely teljesen életszerűtlen.

A mai modern routerek már eleve legalább 8 karakter hosszúságú jelszót fogadnak csak el, és ellenőrzik is a jelszó erősségét, így amennyiben nem elég bonyolult karakter sorozatot adtunk meg, erre figyelmeztet is:



Védekezés

A biztonságot tovább lehet javítani azzal, hogy a végfelhasználói funkciók helyett a nagyvállalatoknak szánt opciókat aktiváljuk. Az átlagos felhasználói WLAN-hálózatoknál (WPA2-Personal) egyetlen jelszó létezik, ezt kapja meg minden kliens, és ezzel lehet kapcsolódni a teljes hálózathoz. Ez azonban rizikós, elég, ha valaki megtudja a Wi-Fi-jelszót, vagy egy hacker valamilyen eszközhibát kihasználva egy klienstől ellopja azt, és máris illetéktelenek hatolnak be hálózatodra.

A WPA2-Personal beállítások mellett létezik egy WPA2-Enterprise titkosítási módszer is: egy úgynevezett RADIUS szervert (Remote Authentication Dial-In User Service) kell bevetni a további hitelesítés érdekében. Ilyen funkciót néhány drágább router is kínál, de például a modern NAS-okban is megtalálható, vagy

külön a szerver-PC-t beállítva is aktiválható. A technológia lényege, hogy a Wi-Fi-re kapcsolódáshoz nem elegendő egyetlen jelszó minden kliensnek, helyette a felhasználóknak egyedi felhasználónév-jelszó párosra van szükségük a kapcsolódáshoz. A RADIUS-szerveren lehet felvenni az új felhasználókat és eszközöket, így mindenki a saját jelszavával kapcsolódhat a hálózathoz. Amennyiben valakitől meg szeretnénk vonni az elérést, nem kell mindenkit értesítenünk a jelszóváltoztatásról, elegendő törölni őt a felhasználók sorából. Támadás ellen is véd a RADIUS, hiszen ha egy hacker megfejti egy felhasználó titkosításhoz használt jelszavát, csak ezt az egy adatfolyamot kapja el, a többi továbbra is elérhetetlen lesz számára.

Hasznos trükkök:

- Router jelszavának megváltoztatása és a beállításokban a beállítómenü letiltása Wi-Fi-n keresztül, így kizárólag az tudja konfigurálni a netet, aki kábelen csatlakozik a routerhez
- A WPS-funkciót érdemes kikapcsolni: ez egy gombnyomásos, azonnali, jelszó nélküli Wi-Fi-kapcsolatot kínál, de könnyen feltörhető, és rontja a biztonságot.
- A MAC-cím-szűrést viszont nem ajánlatos használni, mert ennek megkerülését már megoldották a hackerek, így nem nyújt túl nagy védelmet, csak a kényelmetlenséget növeli.
- A legtöbb útválasztóban tűzfal is lapul, ezt mindenképpen érdemes aktiválni, illetve a túlterhelés elleni védelmet is használjuk ki (DDoS), hogy helyi hálózatunkat ne tudják lelökni az internetről.
- A modern routerek emellett vendég-Wi-Fi-hálózatot is kínálnak, ami nagyon hasznos funkció. Ezzel a fő otthoni hálózattól elszeparált eszközök kapcsolódhatnak az internetre, így a többi helyi hálózati erőforrást nem látják, de a netelérésük biztosított. Általában az is beállítható, hogy a teljes sávszélességből mennyit használhatnak a vendégeszközök.

Kitekintés, későbbi verzió

A Wi-Fi Alliance 2018 januárjában jelentette be, hamarosan új adattitkosítási protokollal bővül a WiFi eszköztára, ugyanis a 14 éves WPA2 helyét átveszi a sokkal modernebb WPA3, ami a vezeték nélküli hálózatok elleni támadások ellen is bevet egy-két trükköt.

A WPA3 működése felhasználói szinten ugyanolyannak tűnik majd, mint a korábbi szabványoké: a vezeték nélküli hálózathoz jelszó megadása után csatlakozhatunk – azonban továbbra is érdemes biztonságos, kellően bonyolult karaktersort választani.

A támadók helyzete ezzel együtt nehezebbé válik majd, ugyanis a WiFi hálózat lehallgatásával és az offline kódtöréssel már nem lehet úgy próbálkozni, mint a WPA2 esetében, ahol a lementett adatfolyamot szótár alapú töréssel meg lehetett fejteni. És így a korábban lementett adatfolyamok tartalmát is el lehetett olvasni.

A WPA3 esetében ehhez a támadónak folyamatos kapcsolatban kell lennie az adott hálózattal ahhoz, hogy találgathasson, offline módon ugyanis csak egyetlen próbát tehet a törésre. Mivel a próbálgatást az adott eszköz támadásként is érzékelheti, ismét csak nehezedik a kódtörés. És ha a támadó véletlenül sikeresen fel is töri a jelszót, a régi, lementett adatfolyamot akkor sem tudja feltörni, csak az aktuális adatfolyamhoz férhet hozzá. Viszont a Counter Hack szakemberei szerint erre nincs igazán esély, ha kellően erős, 16-30 karakterből álló WiFi jelszót hozunk létre – a felhasználók többsége azonban sajnos nem fog ezzel bajlódni. Márpedig minden védelem olyan erős, mint a leggyengébb láncszeme.

A WPA3 az IoT eszközök kiszolgálását is egyszerűbbé teszi, erre ugyanis a 2004-ben megjelent WPA2 még nem volt felkészítve. A kijelző nélküli eszközök a Wi-Fi Easy Connect funkció segítségével csatlakozhatnak az adott hálózathoz, ehhez pedig QR kód alapú azonosítást használhatnak. A router QR kódját be kell olvasni az adott okostelefonnal, majd a csatlakoztatni kívánt eszköz QR kódját ugyancsak be kell olvasni, így az eszközök összeköttetésbe kerülnek. Ez az azonosítás publikus-kulcs alapú titkosítással működik.

A WPA3 esetében további újítás, hogy a publikus hálózati kapcsolat az első másodperctől kezdve alapértelmezetten adattitkosítás mellett zajlik. Tehát míg a WPA2 esetében az azonos publikus hálózaton lévő eszközök esetében lehetőség volt az aktivitás megfigyelésére és közbeékelődéses támadások vagy adatforgalom lehallgatásra, addig a WPA3 ezek ellen már védelmet nyújt, hála az Opportunistic Wireless Encryption funkciónak. Ez nagy előrelépés, ugyanakkor egyes szakértők szerint csak félmegoldás, hiszen a támadó ál-hozzáférési-pont létrehozásával kikapcsolhatja a funkciót, ha akarja, tehát elővigyázatosságra továbbra is szükség lesz. Az üzleti felhasználók számára 192-bites adattitkosítás is érkezik, ami igazodik a CNSA (Commercial National Security Algorithm) sajátosságaihoz – ezt a CNSS (Committee on National Security Systems) fejlesztette ki, méghozzá azért, hogy kellő védelmet kaphassanak a kormányzati, védelmi és ipari szektorok WiFi hálózatai.

Attack	Solved by WPA3
Deauthentication	Yes
Handshake Capture Dictionary Attack	Yes
PMKID Hash Dictionary Attack	Yes
Handshake Capture Encrypt/Decrypt	Yes
KRACK Exploit	Yes
Airport Hackability!	YES!!!

A WPA2 protokoll továbbra is használatban maradhat, de egyre nagyobb teret kap majd a WPA3, főleg, ha a 802.11ax eszközök is elkezdenek terjedni. A WPA2 fejlesztése egyébként az elmúlt évek során sem állt le, folyamatosan frissítette a Wi-Fi Alliance. A legutóbbi nagy frissítés a KRACK névre keresztelt támadásforma felfedezésénél történt, amikor kiderült, hogy a támadók akár jelszó nélkül is lehallgathatják az internetes adatforgalmat, ha a helyi vezeték nélküli hálózathoz közel indítanak támadást. A problémára érkeztek frissítések a különböző gyártóktól, valamint a Wi-Fi Alliance is szigorított a routerek hitelesítési eljárásán, így a tesztek alkalmával már a KRACK elleni védettséget is ellenőrizték.

A tanúsítványok kiosztása tehát már zajlik, így egyebek mellett a Qualcomm és a Cisco is készül már WPA3 kompatibilis termékekkel, utóbbi még a régebbi eszközökhöz is kiad frissítéseket, hogy azok WPA3 kompatibilisek lehessenek. Ez, vagyis az utólagos WPA3 támogatás az adott gyártón múlik majd: lesznek, akik frissítik régebbi eszközeiket, de olyanok is, akik csak az új termékeketlátják el WPA3 támogatással.

Felhasznált irodalom:

https://bitport.hu/nagy-gaz-van-a-wi-fi-halozatokkal.html

https://hu.wikipedia.org/wiki/WPA

https://www.securew2.com/blog/complete-guide-wi-fi-security

https://dea.lib.unideb.hu/dea/bitstream/handle/2437/85333/Szakdolgozat_Borics_Akos.pdf;jsessionid=D0B5C5F680E2B037383CF15F00A10D74?sequence=1

https://en.wikipedia.org/wiki/IEEE_802.11i-2004

https://pcworld.hu/pcwpro/igy-lesz-biztonsagos-a-wifid-248017.html

https://hu.digitalentertainmentnews.com/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-589153

https://ipon.hu/magazin/cikk/kezd-teret-hoditani-a-wifi-uj-vedelme-a-wpa3