ÓBUDAI EGYETEM

Keleti Károly Gazdasági Kar
Vállalkozásfejlesztés és Infokommunikációs Intézet

SZAKDOLGOZAT

ÓE-KGK
2023

Hallgató neve: **Bella Barnabás**
Hallgató törzskönyvi száma: **T007096/FI12904/G**

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Óbudai Egyetem
Keleti Károly Gazdasági Kar
Vállalkozásfejlesztés és Infokommunikációs Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: Bella Barnabás
Szakdolgozat száma: [redacted]
Törzskönyvi száma: T007096/FI12904/G **Neptun kódja:** [redacted]

Szak: Gazdaságinformatikus
Specializáció: Vállalatinformatikai specializáció

A dolgozat címe: Wi-Fi törési lehetőségek és Wi-Fi biztonság
A dolgozat címe angolul: Wi-Fi cracking possibilities and Wi-Fi security
A feladat részletezése:
1. Végezzen irodalmi kutatást a Wi-Fi törés és Wi-Fi biztonság témakörében!
2. Mutasson be legalább egy esettanulmányt!
3. Mutassa be a Wi-Fi törés témakörét!
4. Mutassa be a Wi-Fi biztonság témakörét!

Intézményi konzulens neve: Fehér-Polgár Pál

A kiadott téma elévülési határideje:2024. 12. 15.
Beadási határidő: 2023. 12. 15.

A szakdolgozat: Nem titkos.

Óbudai Egyetem Keleti Károly Gazdasági Kar Vállalkozásfejlesztés és Infokommunikációs Intézet P.H. Budapest

Kiadva: Budapest, 2023. 11. 15. ..... Intézetigazgató

A dolgozatot beadásra alkalmasnak találom:

Fehér-Polgár M. ..... belső konzulens

..... külső konzulens

ÓBUDAI EGYETEM

Keleti Károly Gazdasági Kar

HALLGATÓI NYILATKOZAT

Alulírott Bella Barnabás (Neptunkód: [redacted]) hallgató kijelentem, hogy a szakdolgozat saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja, a titkosításra vonatkozó esetleges megkötések mellett.

Budapest, 2023. december 12.

Bella Barnabás

hallgató aláírása

TARTALOMJEGYZÉK

ÁBRAJEGYZÉK

TÁBLÁZATOK JEGYZÉKE

1. BEVEZETÉS

Napjainkban az informatika már-már elengedhetetlen része a mindennapjainknak, éppen ezért online információink védelmére is kimagasló hangsúlyt kellene fektetnünk. Szakdolgozatomban többek között arra keresem a választ, hogy ez mennyire történik meg az átlag felhasználók körében. A vizsgálatomat a Wi-Fi törés és biztonság témakörében teszem meg. Ez az információ védelem témakörét egy nem szokványos megközelítésbe helyezi, hiszen a sajtóban véleményem szerint nem sok szó esik ezen téma fontosságáról. A dolgozat során végig veszem a Wi-Fi technológia működését, bemutatom a fontosabb Wi-Fi törési módszereket és a védelem szempontjából fontos gyakorlatokat. Végül felmérem a Wi-Fi-k biztonságát két féle módszerrel.

2. WI-FI TECHNOLÓGIA BEMUTATÁSA

2.1. Wi-Fi Alliance

A Wi-Fi kifejezés sokunk számára egy mozaikszónak tűnhet, ennek ellenére ez egy márkanév, amelyet egy marketing cég hozott létre az üzleti tevékenységeikhez. A Wi-Fi CERTIFIED logó, embléma használatához a cégeknek a Wi Fi Alliance tagjának kell lennie és egy tanúsítványt kell szerezniük. (CISCO dn.) (WI-FI ALLIANCE dn.)

1. ábra: A Wi-Fi Alliance logója

Forrás: Wi-Fi 2023

2. ábra: A Wi-Fi CERTIFIED logó

Forrás: Wi-Fi 2023

2.2. IEEE 802.11 standard

A Wi-Fi egy vezeték nélküli technológia, ami lehetővé teszi a különböző Wi-Fi képes eszközök számára, hogy csatlakozzanak az internetre. Ilyen eszközök lehetnek például a számítógépek, okostelefonok és más egyéb IoT (Internet of Things) eszköz, mint például bármely okos eszköz vagy akár egy kamera stb. A csatlakozott eszközök képesek az információ cserére, azaz a kommunikációra, ezáltal egy hálózatot hoznak létre egymással.

A kommunikáció az eszközök között rádióhullámokon keresztül zajlik. (CISCO dn.) (IEEE STANDARDS ASSOCIATION [IEEE SA] 2023)

A Wi-Fi technológia az IEEE 802.11 vezeték nélküli csatlakozási szabványok sorozatán alapul, amelyek forradalmasították a kommunikációt és az információhoz való hozzáférést. Az IEEE 802.11 szabvány meghatározza azokat a protokollokat, standardokat, amelyek lehetővé teszik a kommunikációt a Wi-Fi képes vezeték nélküli eszközökkel. A Wi-Fi képes eszközökbe beleértjük a vezeték nélküli útválasztókat és vezeték nélküli hozzáférési pontokat, melyekről a továbbiakban részletesebben is írni fogok. A vezeték nélküli hozzáférési pontok különböző IEEE 802.11 szabványokat támogatnak. A szabványok különböző frekvenciákon működnek, különböző sávszélességet biztosítanak, és különböző számú csatornát támogatnak. Ezekről a rádióhullám fejezetében részletesebben is írni fogok. (IEEE STANDARDS ASSOCIATION [IEEE SA] 2023) (CISCO dn.)

Az IEEE 802.11 szabvány összes módosítása úgy van megalkotva, hogy a szabványnak megfelelő eszközök visszamenőleg kompatibilisek legyenek a korábbi verziókkal, így bármely újabb IEEE 802.11 szabványú eszköz kommunikálni tud, bármely korábbi szabványt használó termékkel. (IEEE STANDARDS ASSOCIATION [IEEE SA] 2023)

2.2.1. IEEE 802.11

Az IEEE 802.11 1997-ben jelent meg. Ez a szabvány adja a mai napig az újabb IEEE 802.11 módosítások és Wi-Fi hálózatok alapját. Az akkoriban úttörőnek számító 2.4GHz-es frekvenciát használta és 1-2 Mbps-os átviteli sebességre volt képes. ISM sávot (ISM band) használt a kommunikációra. Az ISM, az Industrial Scientific and Medical rövidítése, azaz ipari, tudományos és orvosi használatra szánt sáv. Az ISM sáv olyan rádió frekvenciákat jelent, amiket engedély nélkül lehet használni. (IEEE STANDARDS ASSOCIATION [IEEE SA] 2023) (SIGNALBOOSTERS.COM 2020) (ROUSE 2012)

2.2.2. IEEE 802.11b

Az IEEE 802.11b 1999-ben jelent meg. Szintén 2.4GHz-es frekvenciát használt, de fejlődés is történt, hiszen csökkentették az interferenciát más, nem Wi-Fi-t használó

eszközökkel, mint a mikrohullámsütőkkel, mobiltelefonokkal, babafigyelőkkel és sok egyéb más 2.4GHz-es frekvenciát használó eszközökkel. Ezt egy modulációs séma implementálásával érték el. Az alkalmazott modulációs séma a DSSS/CCK (direct-sequence spread spectrum/complementary code keying - közvetlen sorozatú szórt spektrum/kiegészítő kód billentyűzés) volt. (IEEE STANDARDS ASSOCIATION [IEEE SA] 2023) (S. TANENBAUM – J. WEHTERALL 2013, pp. 323-325.)

„Azt az átalakítási folyamatot, amely a bitek és az azokat ábrázoló jelek közötti átalakítást végzi, digitális modulációnak nevezzük.” (S. TANENBAUM – J. WEHTERALL 2013, p. 147.)

Ennek következtében nem csak az interferencia csökkent, hanem az adatátviteli sebesség is megnőtt. Most már 11 Mbps-os átvitel is lehetséges volt. Beltérben 38 méter, kültéren 140 méter volt körülbelül a rádióhullám hatótávolsága. (IEEE STANDARDS ASSOCIATION [IEEE SA] 2023) (SIGNALBOOSTERS.COM 2020)

2.2.3. IEEE 802.11a

Ez a szabvány módosítás szintén 1999-ben jelent meg. Az IEEE 802.11b-vel ellentétben, amely csak egy-vivős volt, ez már több-vivős modulációs sémát használt, azaz az adatok kódolása több frekvencián történt. Ez által nagyobb adatátvitelre volt képes. Az új modulációs séma az OFDM (Orthogonal Frequency Division Multiplexing - ortogonális frekvenciaosztásos multiplexelés) volt. A 2.4GHz-es frekvencia helyett 5GHz-es működést támogatott, 20MHz-es sávszélességgel/csatornaszélességgel különböző átviteli sebességek mellett. Az OFDM által, akár 54 Mbps-os elméleti átviteli sebességre is képes volt, viszont akkoriban az 5GHz-es frekvenciasávú eszközök drágának számítottak, így nagyrészt cégek használták. (IEEE STANDARDS ASSOCIATION [IEEE SA] 2023) (S. TANENBAUM – J. WEHTERALL 2013, p. 156.) (SIGNALBOOSTERS.COM 2020)

2.2.4. IEEE 802.11g

2003-ban jelent meg az IEEE 802.11g. Ez a szabványmódosítás képes volt a 802.11a szabvány által támogatott 54 Mbps-os adatátvitelre, viszont 5GHz helyett 2.4GHz-es frekvencián. Ezt szintén az OFDM modulációs sémával volt képes kivitelezni, mellette

tartalmazott még más fejlesztéseket is. Ahogy említettem, ez a szabvány 2.4GHz-es frekvenciát használt, így olcsóbbak voltak ezek az eszközök és már nem csak cégeknek volt ekkora adatátvitelre képes eszköze. (IEEE STANDARDS ASSOCIATION [IEEE SA] 2023)

2.2.5. IEEE 802.11n

2009-ben jelent meg és egyszerre támogatta a 2.4GHz-es és 5GHz-es frekvenciasávokat. Az átviteli sebesség akár a 600 Mbps -ot is elérhette. Több csatorna támogatására is képes volt az egyes frekvenciasávokban. A két frekvenciasáv támogatásának köszönhetően visszafelé kompatibilis volt az összes eddigi szabványmódosítással (a/b/g), ezáltal az ezeket a szabványokat használó eszközökkel is. Az elméleti hatótávolsága 70 méter beltéren. (IEEE STANDARDS ASSOCIATION [IEEE SA] 2023) (SIGNALBOOSTERS.COM 2020)

2.2.6. IEEE 802.11ac

2013-ban jelent meg ez a szabványmódosítás. 3,5 Gbps-os adatátvitelre is képes volt. Az adatátvitel során nagyobb sávszélességet támogatott, több csatornával rendelkezett az egyes frekvenciasávokban. A fejlesztések kiterjedtek a modulációra is. Ez a standard támogatta a MIMO (Multiple Input/Multiple Output – több bemenet/több kimenet) technológiát, ami lehetővé tette, hogy egyszerre több antennát is tudjanak az egyes eszközök használni küldésre és fogadásra. Tehát egy időben, akár több eszközzel is kommunikálni tudtak. Ez a technológia növelte a sebességet, a késést pedig csökkentette. Mellette előny még, hogy kevesebb hiba történik a kommunikáció során. A 2.4GHz-es frekvenciasávon az adatátvitel elérhette akár a 450 Mbps-ot, míg 5GHz-en a 1300 Mbps-ot. (IEEE STANDARDS ASSOCIATION [IEEE SA] 2023) (SIGNALBOOSTERS.COM 2020)

2.2.7. IEEE 802.11ax

A jelenleg legfrissebbnek tekintett szabványmódosítás 2021-ben jelent meg. Az elméleti adatátviteli sebessége elérheti a maximum 9,6 Gbps-ot. Habár a módosítás célja inkább a megbízhatóság növelésére irányult, mivel a Wi-Fi technológia manapság annyira

elterjedt, hogy rengeteg interferenciával kell számolni és az egyidejűleg kommunikáló eszközök száma is jelentősen megnőtt az IoT eszközöknek köszönhetően. A standardhoz hozzáadásra kerültek olyan mechanizmusok is, amelyek a kültéri működés hatótávolságát növelte. A következő frekvenciasávokon képes működni: 2.4GHz, 5GHz. (IEEE STANDARDS ASSOCIATION [IEEE SA] 2023) (SIGNALBOOSTERS.COM 2020)

2.2.8. Wi-Fi Alliance általi elnevezések

A Wi-Fi Alliance elnevezési megállapodást dolgozott ki az átlag felhasználóknak, hogy segítse a különböző IEEE 802.11 implementációk megkülönböztetését és a verziók között való könnyebb eligazodást egy egyszerűbb elnevezéssel. (IEEE STANDARDS ASSOCIATION [IEEE SA] 2023)

A továbbiakban felsorolom az IEEE 802.11 standardokat megjelenési év szerint sorba rendezve és a hozzátartozó Wi-Fi Alliance által létrehozott elnevezéseket:

- 1997: IEEE 802.11,
- 1999: IEEE 802.11b, megfelelője a Wi-Fi 1,
- 1999: IEEE 802.11a, megfelelője a Wi-Fi 2,
- 2003: IEEE 802.11g, megfelelője a Wi-Fi 3,
- 2009: IEEE 802.11n, megfelelője a Wi-Fi 4,
- 2013: IEEE 802.11ac, megfelelője a Wi-Fi 5,
- 2021: IEEE 802.11ax, megfelelője a Wi-Fi 6. (IEEE STANDARDS ASSOCIATION [IEEE SA] 2023)

2.3. Wi-Fi útválasztó

Amikor Wi-Fi elérésről beszélünk, akkor a Wi-Fi képes eszköz, egy úgynevezett vezeték nélküli útválasztón (wireless router) keresztül csatlakozik az internetre. Egyes esetekben vezeték nélküli helyi hálózati, angolul wireless local area network (röviden WLAN) eszköznek is nevezik a vezeték nélküli útválasztót. A vezeték nélküli útválasztókat általában az internetszolgáltatók biztosítják az előfizetőknek, így nagyrészt otthonokban találhatóak. Ennek a hardvernek a segítségével csatlakoznak az előfizetők a szolgáltató hálózatára és ezáltal lesz internetelérésük. A vezeték nélküli útválasztó, más néven Wi-

Fi útválasztó, egyesíti a vezeték nélküli hozzáférési pont (wireless access point) és az útválasztó hálózati funkcióit. Beláthatjuk tehát, hogy különbözik egy egyszerű útválasztótól. (CISCO dn.)

2.3.1. Az útválasztó és az adatcsomag

Az útválasztó képes helyi hálózatokat (local network), más helyi hálózatokkal vagy akár az internettel is összekötni. Az útválasztó különféle információkat tartalmazó adatcsomagok (data packets) irányítását végzi. Egy adatcsomagnak számos rétege, vagy szakasza van, melyek közül az egyik tartalmazza az azonosítási információkat. Ilyen például a küldő adata, az adat típusa, mérete és a legfontosabb a cél IP (internet protocol) címe. Az útválasztó beolvassa ezt a réteget, priorizálja az adatokat, és minden átvitelhez kiválasztja a legjobb útvonalat. Összességében egy optimális sorrendet állít össze és optimális útvonalat keres az adott adatcsomaghoz. (CISCO dn.)

2.3.2. Vezeték nélküli hozzáférési pont

A vezeték nélküli hozzáférési pont, a vezeték nélküli kapcsolatra képes készülékeket rá tudja csatlakoztatni egy helyi, vezetékes hálózatra. Ezt úgy képes kivitelezni, hogy egy új vezeték nélküli hálózatot hoz létre a meglévő, vezetékes hálózaton belül. Ez a vezeték nélküli helyi hálózat, azaz WLAN. (CISCO dn.) (LINKSYS dn.)

2.4. SSID

Az SSID (Service Set Identifier – szolgáltatáskészlet azonosító) a vezeték nélküli hálózatokat különbözteti meg. Erre azért van szükség, mert a jelek szórással terjednek és egy-egy hálózat fedheti a másikat, tehát szükséges az azonosításuk a kapcsolódás szempontjából. A Wi-Fi képes eszközök az SSID-vel határozzák meg, hogy melyik hálózati eszköznek sugározzák a jeleket. Hosszúsága 32 karakter lehet. Tartalmazhat betűket, számokat és néhány speciális karaktert is. Az azonosítóban meg vannak különböztetve a kis és nagy betűk. A Wi-Fi útválasztók beállításaiban van lehetőség arra, hogy kikapcsoljuk az SSID sugárzását és arra is, hogy megváltoztassuk az alapértelmezett, gyártó által generált értékről. A kommunikáció során az adatcsomagok

tartalmazzák az SSID-t a csomag fejlécében. (DROTÁR – KOVÁCS 2013, p. 6.) (MITCHELL 2021)

Az SSID nevében felfedezhettük a szolgáltatáskészlet kifejezést. A szolgáltatáskészletek meghatározzák a vezeték nélküli hálózatok topológiáját, azaz, hogy hogyan kapcsolódnak a hálózaton belüli eszközök. Beszélhetünk BSS-ről (Basic Service Set – alap szolgáltatáskészlet) és ESS-ről (Extended Service Set – kiterjesztett szolgáltatáskészlet). (WIFI PROFESSIONALS 2019) (DROTÁR – KOVÁCS 2013, pp. 5-6.)

BSS-nél egy hozzáférési pont van és egy vagy több kliens csatlakozik hozzá. A kliensek közötti kommunikáció a hozzáférési ponton keresztül zajlik, tehát az információcsere nem direkt módon zajlik, hanem egy köztes pont közbeiktatásával, ami a hozzáférési pont. A BSSID (Basic service Set Identifier – alap szolgáltatáskészlet azonosító) a BSS hálózat azonosítására szolgál, ami a hálózat hozzáférési pontjának a MAC címe. Erre azért van szükség, ha két hálózatnak azonos SSID-je lenne. (WIFI PROFESSIONALS 2019) (DROTÁR – KOVÁCS 2013, p. 6.)

ESS-nél kettő vagy több összekapcsolt BSS-ről beszélünk, amelyet a DS (Distributed System – elosztó hálózat) kapcsol össze. A DS-hez több hozzáférési pont kapcsolódhat, tulajdonképpen egy gerinchálózatnak felel meg. A ESSID az ESS hálózat azonosítására szolgál, viszont szokták szimplán SSID-nek is nevezni. (WIFI PROFESSIONALS 2019) (DROTÁR – KOVÁCS 2013, pp. 5-6.)

2.5. MAC

Amikor MAC-ről (Media Access Control – közeg hozzáférés szabályozás) beszélünk két témát érinthetünk. Az első a legtöbbünk által is ismert MAC cím és a MAC réteg. A dolgozatom szempontjából a MAC címet fogom részletesebben bemutatni. (SAM 2023)

Az OSI modell része a MAC réteg. Az OSI (Open System Interconnections) egy rétegzett hálózati keretrendszer, amit azért hoztak létre, hogy áttekinthetőbb legyen a rendszer működése. A MAC réteg a 2. OSI rétegben található, ami egy hardverközeli rétegnek számít. (TUCKER 2020)

A MAC cím a hálózati kártyákhoz lett készítve a gyártás során és teljesen egyedi az értéke. Nem lehet megváltoztatni az értékét, mivel bele van égetve a hálózati interfész kártyába (NIC – Network Interface Card). Fizikai címként is szokás a MAC címre hivatkozni. Ennek ellenére van lehetőség szoftveres módszerekkel megváltoztatni az értékét, de a hardverben a régi, eredeti MAC cím marad. Hat hexadecimális számból áll, amit kettősponttal vagy kötőjellel szokás elválasztani, de előfordulhat olyan is, hogy nincs elválasztva. Az első három hexadecimális szám azonosítja a hálózati kártya gyártóját. Az ezt követő három hexadecimális szám, pedig a hálózati interfész kontrollert (Network Interface Controller). A MAC cím elsődleges célja az eszközök azonosítása, hogy a kommunikáció során a megfelelő eszközhöz érjen célba az információ. Emellett az információ küldőjét is szintén azonosítja. (SAM 2023) (GEEKSFORGEEKS 2023)

2.6. Titkosítási protokollok

A vezeték nélküli kommunikáció lényegesen különbözik a vezetékestől a biztonság szempontjából, ugyanis bármely vezeték nélküli eszköz, amely azonos frekvencián működik képes belehallgatni a kommunikációba. A lehallgatott adatok olvasásának a sikere attól függ, hogy van-e titkosítás a kommunikáció során, ezért kifejezetten fontos a vezeték nélküli kapcsolatok biztonságossá tétele. Ezt kétféleképpen tehetjük meg: hitelesítéssel és titkosítással. (JOHNSON 2020)

Hitelesítés alatt azt értjük, hogy csak a hozzáféréshez engedélyt kapott személy tudjon csatlakozni a hálózathoz. Ez általában a hálózat jelszavának beírásával történik. Titkosításnál, csak a megfelelő kulccsal rendelkező eszköz legyen jogosult az adatok olvasására. (NETSPOT, dn.)

A WPA rendelkezik személyes és vállalati használatra szánt verzióval. A legfrissebb vállalati verzió, a WPA-EAP szigorú 802.11X standardot használ a hitelesítésekhez. A vállalati módnak a hitelesítéshez egy hitelesítési szerverre van szüksége, amellyel a kliensek már a bejelentkezési adatok elküldése előtt kommunikációt folytatnak. A dolgozatom témája szempontjából, a továbbiakban a személyes használatra szánt verziókat fogom részletezni. (S. GILLIS 2022)

2.6.1. WEP

A WEP (Wired Equivalent Privacy – vezetékessel egyenértékű védelem) 1999-ben jelent meg és ahogy a neve is sugallja, azzal a reménnyel jött létre, hogy a vezetékes hálózatokhoz hasonló biztonságot fog tudni biztosítani. Az RC4 (Rivest Cipher 4) titkosítást használt, ami egy fix, statikus kulccsal titkosította és fejtette vissza az adatokat. A kommunikáció során tehát a kulcs sosem változik, ezáltal könnyű volt a feltörése. Az üzenet hitelességének vizsgálatára CRC-32 ellenőrző összeget használt. Kétféle hitelesítés létezett a WEP hálózatnál: OSA (Open System Authentication) és SKA (Shared Key Authentication). OSA-nál WEP kulcs nélkül lehetett csatlakozni a hálózathoz, tulajdonképpen nyitott hálózat volt. SKA-nál ismerni kellett a WEP kulcsot a csatlakozáshoz. A hitelesítéshez egy szöveget kellett a kliensnek titkosítania és visszaküldeni az útválasztó felé. (NETSPOT dn.) (JOHNSON 2020) (RANA – ARUN 2021) (SALTER 2019) (S. GILLIS 2022)

2.6.2. WPA

2003-ban jelent meg. Az első Wi-Fi Alliance által készült protokoll, ami az elődjén, a WEP-en alapult. A csatlakozáshoz ismerni kell a PSK-t (Pre-Shared Key – előre megosztott kulcs), azaz a jelszót. A WEP sebezhetőségére, a statikus kulcs használatára, létrehoztak egy új titkosítási módot a TKIP-t (Temporal Key Integrity Protocol). Ez a kommunikáció során minden egyes adatcserénél új kulcsot hozott létre, ezáltal növelve a biztonságot. Emellett a csatlakozott eszközök, így már nem képesek más kliensek kommunikációjába belehallgatni. Ugyanis minden csatlakozott eszköz visszatudta fejteni más, szintén a hálózathoz csatlakozott klienstől megszerzett adatcsomagokat a statikus kulccsal. A kommunikáció így már privátnak tekinthető. Az üzenet validációjára MIC-et (Message Integrity Code) használt, amit nehezebb megkerülnie a támadónak. (JOHNSON 2020) (SALTER 2019) (RANA – ARUN 2021)

2.6.3. WPA2

2004-ben jelent meg. A TKIP sebezhetősége miatt jött létre. Az új titkosítási mód, az AES-CCMP volt (Advanced Encryption Standard - Counter Mode Cipher Block Chaining Message Authentication Code Protocol). WPA2 nem tiltotta meg a TKIP

használatát, ezáltal évikig használta még sok felhasználó. Legnagyobb sebezhetősége a KRACK támadás, amiről a későbbiekben részletesebben is írni fogok. (JOHNSON 2020) (SALTER 2019) (RANA – ARUN 2021)

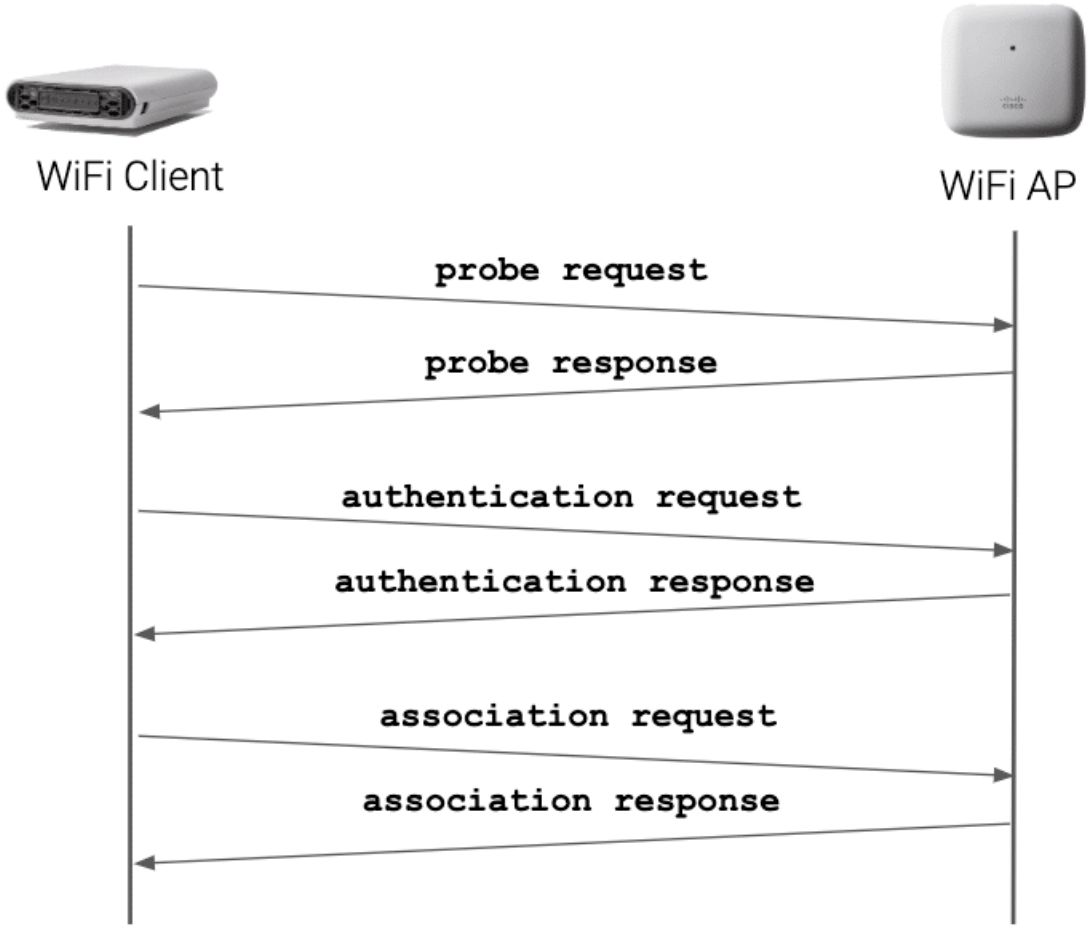
2.6.4. WPA3

A KRACK támadás elkerülésére jött létre 2018-ban. A PSK-t az eszközök nem osztják meg egymással, helyette SAE-val (Simultaneous Authentication of Equals) történik a hitelesítés, így már nem lehet véghez vinni a KRACK támadást. A SAE képes megvédeni a rövid jelszavas hálózatokat, mivel ugyanolyan nehézzé teszi a feltörését, mintha egy hosszabb jelszavas hálózat lenne. A titkosítás módja a AES-GCMP (Advanced Encryption Standard - Galois/Counter Mode Protocol), ami elődjénél (CCMP) biztonságosabb titkosítást biztosít. A titkosítás során pedig PFS-t (Perfect Forward Secrecy) használ, ami meggátolja a lehallgatott adatcsomagok későbbi visszafejtését. Ez a gyakorlatban úgy nézne ki, hogy a támadó lehallgatna rengeteg adatcsomagot és ha a hálózat jelszava kiszivárog vagy sikerül megfejteni, akkor ezt követően képes lesz az adatok olvasására. Az elavult titkosítási protokollok használatát ellehetetlenítik a WPA3 használata során, növelve ezáltal a biztonságot. WPS (Wi-Fi Protected Setup) helyett egy új módszert dolgoztak ki, a Wi-Fi Easy Connect-tet, amelynél az eszközökön (útválasztó, kliens) található QR kód, okostelefonnal történő beolvasásával hozzuk létre a kapcsolatot. (SALTER 2019) (JOHNSON 2020) (NETSPOT dn.)

2.7. Kapcsolódás menete

A hálózathoz való csatlakozás menete a következőképpen zajlik. A kliens körbe szkenneli a környező SSID-kat, a kliens hálózati kártyájának megfelelő frekvenciasávokban. Ezt követően vizsgáló kéréseket küld (probe request) a kliens. Ezek a vizsgáló kérések tartalmazzák a kliens IEEE 802.11 standardját és támogatott adatátviteli sebességét. Erre a hozzáférési pontok válaszolnak, SSID-t és BSSID-t tartalmazó válaszüzenettel. Ha a kliens a specifikációjának megfelelő SSID-t talál, akkor hitelesítést indít. A hitelesítés fázisában egy négy irányú kézfogás történik (4-way handshake) ami, ha sikerrel végződik, akkor a kliens hozzá tud kapcsolódni a hozzáférési ponthoz, más szóval hozzárendeli magát (association) a hozzáférési ponthoz. A sikeres hitelesítési

folyamathoz a kliensnek rendelkeznie kell a megfelelő PSK-val, azaz a hálózat jelszavával. Erre abban az esetben van szükség, ha titkosított a hálózat. A hitelesítés fázisában a kliens a MAC címét is elküldi, ha esetleg a hozzáférési pontnál MAC szűrő van beállítva. (GRIDELLI 2019) (UY 2020) (TUTORIALSPOINT dn.)



3. ábra: kapcsolódás menete

Forrás: GRIDELLI 2019

2.8. Rádióhullámok

Ahogy korábban említettem a kommunikáció a vezeték nélküli eszközök és a Wi-Fi útválasztó között rádióhullámokon keresztül zajlik. A Wi-Fi-k által használt rádióhullám hasonlít a mobil telefonok, televíziók által használt rádióhullámokhoz. A különbség a Wi-

Fi hálózatoknál abban rejlik, hogy magasabb frekvencián zajlik a kommunikáció, mint az előbb említett eszközöknél. (BRAIN – HOMER 2021)

A rádióhullámok míg elérik a célpontot különféle akadályokkal találkozhatnak és ezek az akadályok befolyásolják a hatótávolságát és teljesítményét. A rádióhullámok használata során meg kell felelni különböző szabályoknak, törvényeknek, tehát nem lehet bármilyen rádióhullámot szabadon használni. Ez azért van így, mert lehetséges olyan rádióhullám kibocsátása, ami blokkolja a telefonok és a rádiók működését. A rádióhullámok az elektromágneses jelek közé sorolhatóak és arra tervezték őket, hogy információkat szállítsanak a levegőben. (CISCO PRESS 2017) (NETSPOT dn.)

A rádióhullámokat sokszor rádiófrekvenciás jeleknek is szokták emlegetni és nagyon magas frekvencián rezegnek. Ez lehetővé teszi a jeleknek, hogy az óceán hullámaihoz hasonlóan haladjanak át a levegőben. Évek óta használjuk őket hang és videó anyag szállítására, sugározására. A hangot például rádiókhoz, a videókat pedig televíziókhoz sugározták. Elmondhatjuk tehát, hogy rádióhullámokat használunk a vezeték nélküli kommunikációnk többségében. (CISCO PRESS 2017)

A rádióhullámoknak különböző attribútumai vannak:

2.8.1. amplitúdó

Az amplitúdó fejezi ki a rádióhullám erősségét, melyet erőben mérünk. Az erő az elektromágneses jeleknél, azt az energia mennyiséget fejezi ki, amely a jelek egy megadott távolságig történő sugárzásáig szükségesek. A könnyebb megértést segíti a következő hasonlat: az az erőfeszítés, amelyet a biciklisnek kerékpározás közben ki kell fejtenie, egy adott távolság megtételéhez. Ahogy növeljük az erőt, úgy növekszik az elért távolság is, azaz egyenes arányosság van az erő és a távolság között. (CISCO PRESS 2017)

Az erő mértékegysége a watt. Esetünkben ez kifejezi a jel erősségét. A milliwattot (mW) kifejezhetjük decibelben is (dBm). A decibelt úgy feleltetjük meg milliwattnak, hogy egy milliwatthoz hasonlítjuk, mérjük. Egy milliwatt nulla decibelnek felel meg. Értelemszerűen pozitív decibel értékekről beszélhetünk egynél nagyobb milliwattnál és

negatívról egy milliwattnál kisebb értékeknél. Rádióhullámoknál előnyösebb a decibel mértékegységet használni. (CISCO PRESS 2017)

2.8.2. frekvencia

A rádióhullámoknál a frekvencia azt jelenti, hogy a jel másodpercenként hányszor ismétli önmagát. A fizikában, a frekvencia azoknak a hullámoknak a száma, amelyek egységnyi idő alatt áthaladnak egy fix ponton. A frekvencia mértékegysége a Hertz (Hz). A Herz a másodpercenként előforduló ciklusok száma. A Wi-Fi-k 2.4GHz, 5GHz és 6 GHz-es frekvencián működnek. A 2.4GHz megfelel 2,400,000,000 ciklusnak, az 5GHz 5,000,000,000 ciklusnak és így tovább. Ezek a frekvenciák túl magasak az emberek számára, hogy hallhatóak legyenek, és túl alacsonyak ahhoz, hogy képesek legyenek látni. Ezáltal nem észrevehetőek a mindennapi életben. (CISCO PRESS 2017) (BRITANNICA, THE EDITORS OF ENCYCLOPAEDIA 2023)

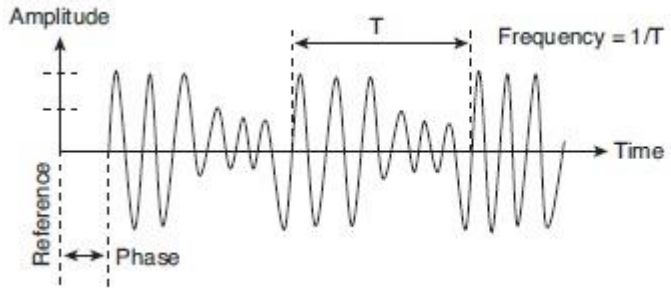
A frekvencia a rádióhullámok terjedésében játszik szerepet. A magasabb frekvenciájú jelek kisebb területet képesek bejárni, míg az alacsonyabb frekvenciájú jelek távolabbra is elérnek. Ez a gyakorlatban nem feltétlenül történik ilyen módon, ugyanis egy nagyobb erővel sugárzott 5GHz-es frekvenciájú rádió jel távolabbra is elérhet, mint egy 2.4GHz-es jel, amelyet kisebb erővel sugároznak. Ezt a teóriát tovább erősíti az, hogy az 5GHz-es frekvencia kevésbé szennyezett, mint a 2.4GHz, tehát kevesebb interferencia érheti. Számos más eszköz is a 2.4GHz-es frekvenciát használja, ilyenek például a garázs ajtók vagy számítógépes játékokra szánt fejhallgatók. A magasabb frekvencia egyben azt is jelenti, hogy nagyobb az átviteli sebesség, tehát minél magasabb a frekvencia, annál nagyobb átviteli sebességről beszélhetünk. (CISCO PRESS 2017) (AQUIRRE 2022) (LOHNES 2017)

2.8.3. fázis

A rádióhullám fázisa annak felel meg, hogy a jel milyen messze van egy referenciaponttól A referenciapont lehet egy adott időpont vagy egy másik jel adott állapota. Egy ciklus 360 fokot fed le, azt is mondhatjuk, hogy egy kör, viszont ez nem teljesen fedi a valóságot, hiszen két félkörről van szó. A kör két vége nem érintkezik, egy fektetett „S” alakként kell elképzelni, ahol az egyes görbületek 180 foknak felelnek meg. Amikor fáziseltolásról

beszélünk, akkor azt fejezzük ki, hogy mennyire toltuk el, azaz hány fokkal toltuk el a jelet a referenciaponttól. Például, ha egy 90 fokos eltolást vizsgálunk, akkor az egy negyed ciklussal való eltolásnak felel meg (90/360 = 1/4). Két rádiójel akkor van szinkronban, egy fázisban, amikor azonos fokszámmal vannak eltolva az egyes jelek. Az egy fázisban lévő jelek erősítik egymást. Ellenkező esetben, ha két frekvencia 180 fokos eltolásban van egymással, akkor kiiktatják egymást. A korábban említett 90 fokos eltolás negatívan érinti a két jelet, hiszen a két rádiófrekvencia nincs fázisban. Az újabb rádió technológiák figyelembe veszik a fázis tulajdonságát és változtatják a fázist a jobb eredmények érdekében. (CISCO PRESS 2017) (WELLING 2022)

A felsorolt attribútumok az idő folyamán változhatnak, hogy reprezentálják, kifejezzék az információt. Ezt a következő ábra jól bemutatja. A vízszintes tengely fejezi ki az idő múlását. Jól látható, hogy az idő múlásával többször is megváltozott az amplitúdó. Az amplitúdót a függőleges tengely fejezi ki. (CISCO PRESS 2017)



4. ábra: A rádióhullám attribútumai

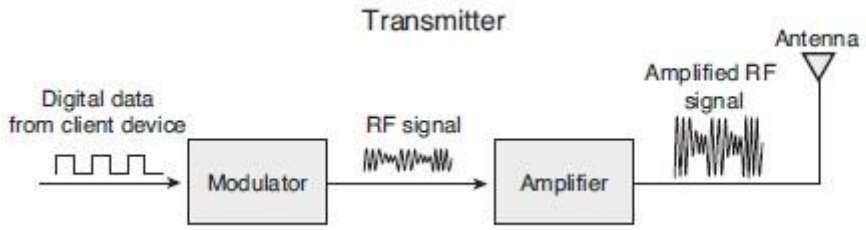
Forrás: CISCO PRESS 2017

2.8.4. Rádiófrekvenciás adóvevő

A rádiófrekvencia adó-vevő beépíthető a kliens eszközbe, amihez tartozik egy antenna is. Ezeket akár külső alkatrészként is csatlakoztathatjuk az eszközökhöz. Két antenna között található az átviteli közeg, ami javarészt a levegő, de akár folyékony anyag is lehet. Ez az eset előfordulhat például egy tengeralattjáróból indított kommunikációnál, ahol az átviteli közeg a víz lenne. Ezenfelül sok más egyéb akadályba is ütközhet a rádiójel, mint például

falakba és tárgyakba. Ezek is lehetnek az átviteli közeg részei, részben vagy teljes egészében. (CISCO PRESS 2017)

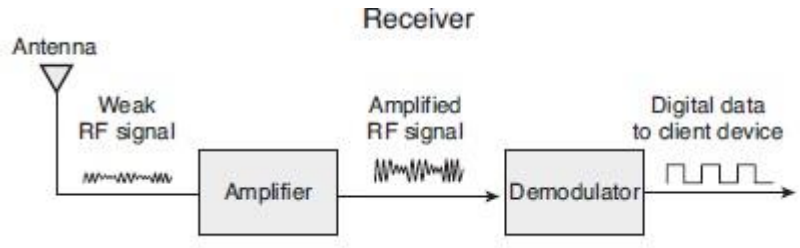
A WLAN eszköz fő komponense a rádiófrekvenciás adó-vevő, ami az elnevezéséből fakadóan tartalmaz egy adó és egy vevő alkomponenst. Megkülönböztetünk egy forrást és egy célt. A forrás küldi az információt, ő az adó. Cél fogadja az információt, ő a vevő. Az adó-vevő az esetek nagy részében a kliens rádió eszközében található, amelyre sokszor kliens kártyaként is szoktak utalni. (CISCO PRESS 2017)



5. ábra: Az adó komponensei

Forrás: CISCO PRESS 2017

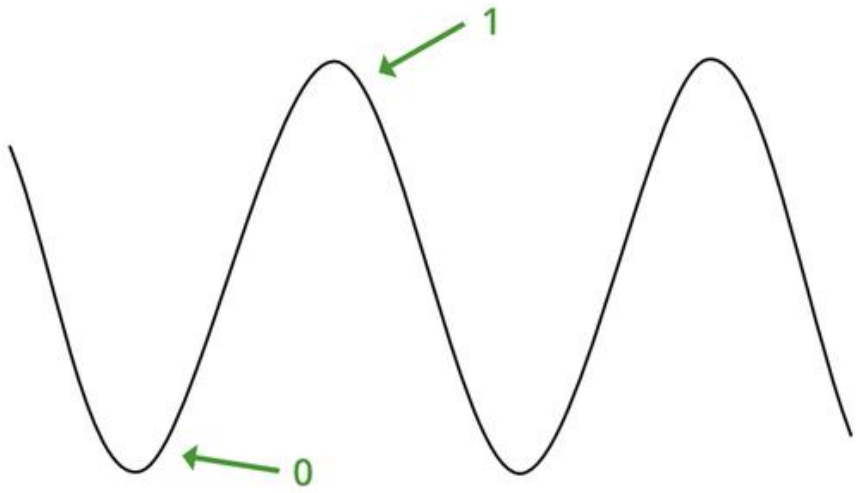
A fenti ábrán látható, hogy az adó több alkomponensre bomlik szét. Tartalmaz egy modulátort, ami a kliens eszközön bináris adattá átkonvertált információt alakítja rádiójelekké. A rádiójelek analóg jeleknek számítanak, így ez egy digitális-analóg transzformáció. A transzformáció során a modulátor a biteket átalakítja megfelelő frekvenciájú rádióhullámmá. Ezt követően az erősítő felerősíti a jeleket, azaz növeli az amplitúdóját a rádióhullámnak a kívánt átviteli erőre. Végül pedig az antenna elkezdi terjeszteni a rádióhullámokat. (CISCO PRESS 2017)



6. ábra: A vevő komponensei

Forrás: CISCO PRESS 2017

Az ötös számú ábrán láthatjuk, hogy a vevő komponensei értelemszerűen az adó inverzei. Találunk egy antennát, ami a viszonylag gyenge jeleket fogadja. Ezt a következő komponens, az erősítő, felerősíti egy a vevő általi minimum érzékenységre. Ha nem éri el a vevő általi minimum érzékenységet a jel, akkor nem tudja visszaalakítani digitálissá az információt. Egyébként a minimum érzékenység elérésének teljesülésekor a vevő, a demodulátorral képes az analóg jeleket digitális, bináris jelekké vissza konvertálni. A konverzió típusa, itt is az adó inverze, tehát itt egy analóg-digitális transzformációról beszélhetünk. (CISCO PRESS 2017)



7. ábra: Bitek reprezentálása rádióhullámokként

Forrás: MONDAL 2021

Ahogy a fenti ábrán látszódik, a bitek rádióhullámokban kifejezett változatát a következőképpen lehet elképzelni. A koszinusz függvényre hasonlító ábra minimum pontja nullának feleltethető meg, míg maximum pontja egyesnek. A bináris adat, így könnyedén kifejezhető a rádióhullámokként. Az internet elérés során minden információ bináris kóddá konvertálódik. Az információ cserét a felhasználó kezdeményezi. (MONDAL 2021) (LOHNES 2017)

2.8.5. csatorna és csatorna szélesség

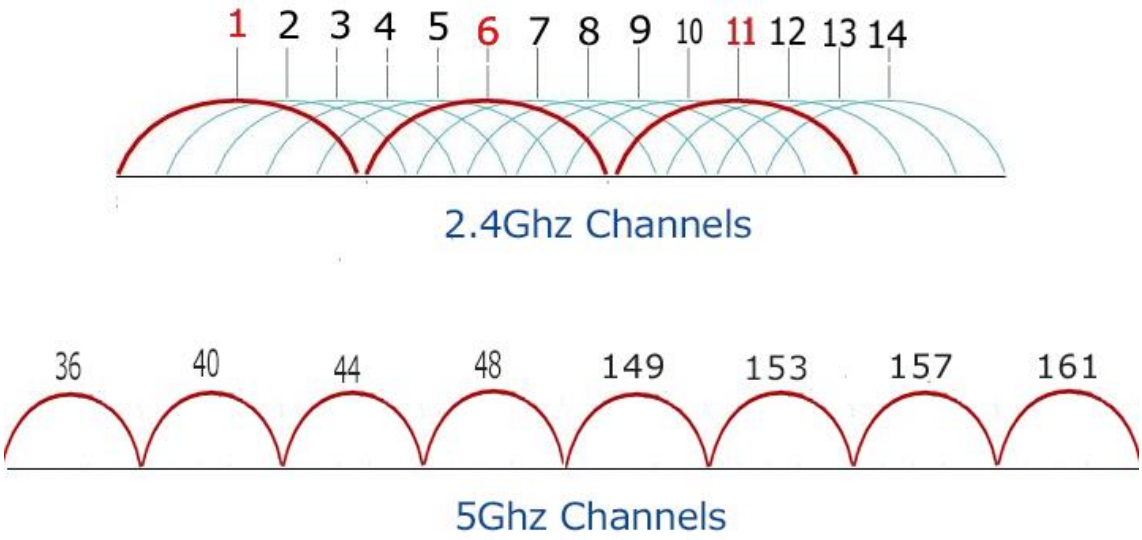
A korábban említett frekvenciák (pl. 2.4GHz, 5GHz, 6GHz) a Wi-Fi-knél frekvenciasávot jelentenek. A frekvenciasávokat tovább lehet bontani csatornákra. Ezek a csatornák szintén különböző frekvenciákon működnek, hiszen a csatorna a frekvenciasáv egy szegmense. A csatornák lényege, hogy kevesebb interferencia érje a rádióhullámokat a kommunikáció során, mivel feltételezhető, hogy nem egy eszköz fogja használni az adott frekvenciasávú rádióhullámot. Lényegében a csatornák célja, hogy kevesebb frekvencia átfedés legyen a Wi-Fi képes eszközök kommunikációja során. (WIFIADVISER dn.) (SIGNALBOOSTERS.COM 2022)

Interferenciát a következők okozhatnak Wi-Fi hálózatok esetén:

- más Wi-Fi hálózatok,
- más nem Wi-Fi standardon alapuló eszközök, mint a mikrohullámú sütők, mobiltelefonok és Bluetooth eszközök. (ALBALO 2022)

A 2.4GHz-es frekvenciasávon 14 csatorna található, melyek közül az 1-es, 6-os és a 11-es nem fedi egymást. Ezen a frekvenciasávon az előbbi csatornák a leghatékonyabbak, mivel nem történik átfedés közöttük és ezért kevesebb az interferencia. Az 5GHz-es frekvenciasávon 25 csatorna van, melyek közül csak 8 használható beltéri használat során. Ennél a frekvenciasávnál egyik csatorna sem fedi egymást. A 2.4GHz-es frekvenciasávnál a Wi-Fi standard szerint 5MHz-enként található egy újabb csatorna. (WIFIADVISER dn.) (ALBALO 2022)

A 2.4GHz-es frekvenciasávon az egyes csatornák szélessége 20MHz és 40MHz lehet, míg az 5GHz-es frekvenciasávon 20MHz, 40MHz, 80MHz és 160MHz is megengedett. Látható, hogy a felsorolt szélességek mindig az előző kétszeresének felelnek meg. Ez azért van így, mert két külön álló csatorna sugárzása történik egyszerre. Minél szélesebb a csatorna, annál nagyobb adatátvitel lehetséges, hiszen egyidejűleg nagyobb adatmennyiséget lehet átvinni. A szélesebb csatorna az interferencia esélyét is növeli. (WIFIADVISER dn.) (ALBALO 2022)



8. ábra: Wi-Fi frekvenciasávok csatornái

Forrás: WIFIADVISER dn.

3. WI-FI TÖRÉS

Ahogy a Wi-Fi védelem fejezetében olvashatjuk majd, egyes útválasztóknak vannak specifikus sebezhetőségei. Ezeken felül vannak egyéb törési módszerek, amelyek több kombinációjából jöttek létre, illetve különböző szoftverek, amelyek segíthetik a törési folyamatot. Tehát elmondhatjuk, hogy tág fogalomról van szó. Ebben a fejezetben csak a dolgozatom szempontjából releváns módszereket fogom megemlíteni. (POSTON 2021)

3.1. WPS támadás

A WPS-t (Wi-Fi Protected Setup) a Wi-Fi Alliance hozta létre 2006-ban azzal a céllal, hogy egyszerűsítse a kapcsolódást a hálózatokhoz. A működése nagyon egyszerű: a felhasználó megnyomja a WPS gombot az útválasztón, ekkor szabadon kapcsolódhat egy készülék anélkül, hogy beírt volna egy hosszabb jelszót. A kapcsolódó eszközön is meg kell nyomni a WPS gombot rövidesen az útválasztó WPS gombjának megnyomását követően. Ezenfelül lehetőség van egy rövid 8 jegyű PIN segítségével is csatlakozni (csak számokból áll). A WPS csatlakozási módszer praktikus lehet olyan esetekben, amikor olyan eszközt próbálunk csatlakoztatni, ahol a hosszabb jelszó beírása nehézkes. Ilyenek lehetnek az IoT eszközök is. Több sebezhetőséget is felfedeztek a kiberbiztonsági szakértők a funkció létrejötte óta. Fontos megemlíteni, hogy a funkció kikapcsolása sok esetben nem gátolja meg a WPS-en keresztüli támadás lehetőségét. Sok esetben ugyan elhárították a sebezhetőséget egy szoftverfrissítésen keresztül, de ez a felhasználótól függ, hogy telepítette-e, illetve a gyártótól, hogy ténylegesen jól javította a problémát, illetve az is elképzelhető, hogy olyan régi a Wi-Fi útválasztó, hogy nem kapott frissítést. A WPS támadás relevanciája tehát az imént említett esetektől függ. (HACKTHEBOX 2023) (REED 2022)

A PIN-en keresztüli hitelesítés a következő módon történik. A két eszköz a PIN beírását követően publikus kulcsot cserél. A következő üzenetcserék titkosítása ezzel történik. A kliens titkosítja az útválasztó publikus kulcsával az üzenetet, amit az útválasztó a privát kulcsával tud visszafejteni. A másik oldalon szintén, így történik a titkosítás csak a kulcsok cserélődnek a szerepnek megfelelően. Ezt követően a két eszköz megbizonyosodik, hogy mindketten ugyanazt a PIN kódot ismerik. Ez úgy történik, hogy a PIN-t elfelezik és két részletben ellenőrzik a kódot. A PIN utolsó karaktere egyébként

egy ellenőrző összeg az összes többi számjegyre nézve. (HACKTHEBOX 2023) (GRIGUTYTÉ 2023)

Két féle támadás létezik, az egyik az említett PIN online brute-force-a, a másik pedig a Pixie Dust, ami egy offline támadás. A dolgozatom szempontjából az online brute-force a releváns technika. (REED 2022)

Mivel az utolsó számjegy ellenőrzésre van ezért 7 számjegyet kell kitalálnia a támadónak. Ahogy említettem a hitelesítés két szakaszban történik, ezért az első 4 számjegy kitalálása 10,000 szám közül történik, a maradék 3 számjegynek pedig 1,000 variációja van, tehát összesen 11,000 variáció van. Ez lényegesen kevesebb, mintha egyben kellene kitalálni, ugyanis abban az esetben 10,000,000 variáció létezne. A Wi-Fi feltörése ezzel a technikával általánosságban 4 óra alatt megvalósítható. (HACKTHEBOX 2023) (REED 2022)

3.2. Wi-Fi törés esettanulmány

Az esettanulmány írója egy kiberbiztonsági szakember, aki Tel Aviv-ban élt hét évet és többször költözött az itt töltött ideje alatt, pontosan négyszer. A költözések során viszonylag sok időbe telt míg a szolgáltató bekötötte az internetet az apartmanjába. A megoldása erre a szituációra az esetek többségében az volt, hogy becsöngetett a szomszédba és elkérte a Wi-Fi-jük jelszavát, illetve telefonszámot is cseréltek. Sokszor azzal szembesült az esettanulmány alanya, hogy a Wi-Fi jelszava megegyezett a szomszéd telefonszámával. Ekkor megfordult a fejében, hogy valószínűleg rengeteg ember nem biztonságos jelszót használ a Wi-Fi hálózatának védelmére. (HOORVITCH 2021)

Ezen felbátorodva elhatározta, hogy megvizsgálja az esetet, kíváncsi volt tényleg bebizonyosodik-e a hipotézise. Az is ösztönözte, hogy ekkor 2021-et írtunk és a koronavírus járvány miatt az emberek többsége otthonról dolgozott, ami megkövetelné a hálózatok biztonságossá tételét. Hiszen így fontos vállalati adatokat tudnak ellopni a támadók. A teszt során 5,000 Wi-Fi hálózatból gyűjtött adatot a hátizsákjában található eszközzel. A tanulmányban összehasonlította a töréshez használt technikát más, korábbi módszerrel. Ebből kiderült, hogy az eddigi törési módszereknél viszonylag sokat kellett

a támadóknak a Wi-Fi hálózat közelében időzni és arra várni, hogy egy kliens csatlakozni fog a hálózathoz, ugyanis kapcsolódás menetét rögzítették. Az esettanulmány alanya egy ennél sokkal jobb módszert használt, hiszen itt nem kellett várni a hálózatok közelében csak adatokat kellett gyűjteni sétálás közben. A módszer lényege, hogy a gyűjtött adattal az offline generált jelszót lehet ellenőrizni, tehát a jelszó fejtésnél nem kell a hálózat közelében tartózkodni és a folyamat sokkal gyorsabb. A jelszó kitalálása brute-force elven zajlott és első körben a létező összes telefonszámmal kezdte a törését alanyunk. Ezzel 2,200 jelszót sikerült megfejtenie, ami a minta 44%-a. Ezt követte a szótármódszer (dictionary attack), amivel 900 jelszót sikerült megfejtenie, ez a mintának a 18%-a. (HOORVITCH 2021)

A tanulmány során a következő eredmény született:

Jelszó hossza	Törések száma
10	2405
8	744
9	368
12	14
11	14
14	7
13	7
Összesen	3,559

1. táblázat: Esettanulmány eredményei

Forrás: HOORVITCH 2021

A tanulmány alanya az 5,000 Wi-Fi hálózat közül 3,559-et tudott megfejteni. Ez a minta 71,18%-a. Az eredményeken látszik, hogy a jelszó hosszával a törések száma csökkent,

ami esettanulmányunk tanulságát adja. Válasszunk minél hosszabb jelszót. Esettanulmányunk alanya a következő tanácsokat adta hálózatunk védelme érdekében:

- válasszunk komplex jelszót,
- változtassuk meg a Wi-Fi alapértelmezett SSID-jét és jelszavát,
- frissítsük a Wi-Fi szoftverét,
- ne használjunk elavult titkosítási protokollt,
- kapcsoljuk ki a WPS funkciót. (HOORVITCH 2021)

3.3. A KRACK támadás

2017-ben egy kutató fedezte fel a KRACK (Key Reinstallation Attack) támadást, ami minden Wi-Fi-t érintett, ugyanis magában a standardban volt a hiba nem az egyes gyártók implementációjában. A támadás a WPA2 4-way handshake (4 ütemű kézfogás) gyengeségére épített. A kézfogás a kliens és az útválasztó kapcsolatának létrejöttekor történik. A folyamat közben jön létre a kommunikáció során használatos titkosítási kulcs. A támadó ezt a folyamatot manipulálja úgy, hogy egy már használatban lévő titkosítási kulcsot telepít újra a kézfogás harmadik fázisában, ez a programban található számlálókat visszaállítja nullára, így olyan folyamatok történhetnek meg újra, amiknek nem szabadna. Ez összességében ahhoz vezet, hogy a támadó képes belehallgatni a kommunikációba, azaz egy man-in-the-middle típusú támadásról beszélünk. Fontos megjegyezni, hogy a hacker nem szerzi meg a Wi-Fi jelszavát. A HTTPS kapcsolat a fogyasztott tartalomnál védelmet adhat, de ha az adott oldal rosszul implementálta a protokollt, akkor a támadó HTTP kapcsolatra állíthatja a HTTPS-t egy program segítségével. Ezzel pedig teljes hozzáférése lesz a kommunikáció során küldött adatcsomagokhoz. A támadás csak abban az esetben nem megvalósítható, ha a Wi-Fi útválasztó és a kliens is frissítve lett a támadás elhárítását célzó szoftverfrissítéssel. Tehát, ha a két eszköz közül valamelyik még ezt nem tette meg, akkor megvalósítható a támadás. (ENISA 2017) (GOODIN 2017) (VANHOEF 2017)

3.3.1. Hogyan releváns manapság a KRACK támadás

Ahogy korábban említettem, ha a kliens vagy az útválasztó nem frissült a KRACK támadás javításaival még manapság is végre lehet hajtani a támadást. Ezenfelül sok online

médium ösztönzi az embereket, hogy használják a régi, elavult Wi-Fi útválasztójukat a hálózat hatótávolságának kiterjesztésére. Ez látszólag jó ötletnek tűnhet, de valójában biztonsági rést hozunk létre, ugyanis nagy rá az esély, hogy ezek régebbi titkosítási módot használnak és az említett támadásra sem készült hozzá frissítés. (STEPHENSON 2023)

A CNBC 2023-as cikke azt állítja, hogy a dark weben tevékenykedő bűnözök az IoT eszközöket tekintik a következő célpontjuknak. Ez érthető, hiszen 17 milliárd eszközről beszélhetünk, amely egyre csak nő. A vásárlók egyre több ilyen készüléket vásárolnak. A Microsoft 2022-ben egy jelentésében arról tett állítást, hogy az IoT eszközök nem tartják ugyanazt a gyorsaságot a biztonsági frissítésekben, mint minden más eszköz (számítógép, okostelefon). A támadók arra használják az IoT eszközöket, hogy botnet hálózatokat hozzanak létre, azaz átveszik felettük az irányítást és különböző szervezett támadásokat hajtanak végre velük. Jelentős probléma még, hogy sok IoT eszközt nehézkes frissíteni és a felhasználók nagy része nem venné a fáradtságot a frissítésre vagy képzetlen lenne hozzá. A készülékek között találhatunk olyat is, ami nem is biztosít frissítési lehetőséget. Az IoT eszközök között találhatunk sok olyan készüléket, ami kényes adatokat tartalmaz, mint bankkártya adat, videó felvétel (kameráknál) stb. Az eddigiek alapján elmondhatjuk, hogy így ugyanolyan relevanciája lehet a KRACK támadásnak, még ha a főbb eszközeinket be is frissítettük. (MACBRIDE 2023)

4. WI-FI BIZTONSÁG

Az eddigiek alapján következtethetünk arra, hogy a Wi-Fi biztonság legalapvetőbb komponensei a jelszavak, a titkosítási protokollok és annak megfelelő kiválasztása. A WPS kikapcsolásáról sem szabad elfeledkeznünk. A továbbiakban ezenfelül említek néhány fontosabb módszert, amivel még jobban lehet növelni a Wi-Fi hálózatunk biztonságát.

4.1. MAC szűrő

A MAC szűrő vagy MAC cím szűrő, az eszközök hozzáférését szabályozó beállítás az útválasztó admin felületén. Amikor csatlakozik egy eszköz a hálózathoz, akkor az SSID-hez kapcsolódó jelszó megadásával hozzáférése van a hálózathoz. Ez a beállítás egy plusz réteget helyez a hitelesítési folyamatba, azáltal hogy csak a megadott MAC címmel rendelkező eszközök engedélyezettek a csatlakozáshoz. (BABU 2022) (MITCHELL 2021)

Az útválasztó admin felületén két listát készíthetünk: egy engedélyezett eszközök listát és egy nem engedélyezett, blokkolt eszközök listát. Egyszerre csak az egyik módot választhatjuk, mert logikailag ütközne, ha mindkettőt használnánk. Ez azért van így, mert amikor engedélyező listát hozunk létre, akkor csak a listán szereplő eszközök kapcsolódhatnak, viszont amikor a blokkoló listát, akkor bárki csatlakozhat a hálózathoz, kivéve a listán szereplő eszközök. Ez utóbbi például, akkor lehet hasznos, ha találtunk egy idegen készüléket a hálózatunkon és nem szeretnénk semmilyen más adatot megváltoztatni az útválasztó admin felületén. (BABU 2022) (MITCHELL 2021)

Ez a mechanizmus alapjában véve nagyon jó biztonságot adna a hálózatunknak, ugyanis ahogy a MAC fejezetben említettem nem lehet megváltoztatni és minden eszköz egyedi azonosítóval rendelkezik. Ennek ellenére a támadók képesek megváltoztatni ezt az értéket és így már hiteltelenné válik a technológia. Általánosságban, viszont sok támadót megállíthat a hálózatunk feltörésében, érdemes tehát a használata. (BABU 2022) (MITCHELL 2021)

4.2. Elrejtett SSID

Az SSID-k elrejtéséről elsőre azt gondolhatjuk, hogy segíti a hálózatunk biztonságát, hiszen a kliensnek két adatot kell ismernie a csatlakozáskor: az SSID-t és a hálózat jelszavát. Ennek ellenére ez a valóságban nem nevezhető hatékony megoldásnak, hiszen mint ahogy az SSID fejezetében írtam, az adatcsomag tartalmazza az SSID nevét, így egy program segítségével az elküldött adatcsomagokból ki lehet szedni az SSID nevét. Ez akár valós időben is történhet, vagy a másik eset, hogy a támadó lementi a megszerzett adatcsomagokat és később visszafejti az adatokból az információt, ha már rendelkezik a megfelelő kulcsokkal. (MITCHELL 2021)

A hálózat SSID-jának elrejtése, különböző kapcsolódási problémákat okozhatnak a klienseknél. A nagyobb probléma abban rejlik, hogy egyes kliensek felfedhetik a hálózat hitelesítéséhez szükséges adatokat. (HOFFMAN 2017)

Az Apple 2023-as Wi-Fi-routerek és -hozzáférési pontok ajánlott beállításairól szóló cikke a következőt állítja:

„A hálózati név elrejtése nem védi meg a hálózatot a felfedezéstől, sem az illetéktelen hozzáféréstől. Ráadásul a rejtett Wi-Fi-hálózat használata az eszközök hálózatkeresési és csatlakozási mechanizmusai miatt az Ön és a használt rejtett hálózat (például az Ön otthoni hálózata) azonosítására alkalmas információkat is felfedhet. Ezért ha rejtett hálózathoz csatlakozik, egyes eszközök adatvédelmi figyelmeztetést is megjelenítenek.” (APPLE 2023)

„Ha szeretné korlátozni a hálózathoz való hozzáférést, inkább használja a megfelelő biztonsági beállításokat.” (APPLE 2023)

Az Asus rejtett SSID-ről szóló cikke a következőket állítja:

Az otthoni hálózatunk SSID-jének elrejtése, akkor ideális választás, ha sok ismeretlen ember próbál csatlakozni a hálózatunkhoz és az útválasztónknak ezeket a kérelmeket mindig el kell utasítania, ami sok erőforrást pazarol. Rejtett SSID-jű hálózathoz csatlakozott eszköz még a kapcsolat létrejötte után is küld felderítő kéréseket (probe request), ami biztonsági szempontból nem ideális. Illetve a kliens platformjától függően,

akár más hálózathoz is próbálhat csatlakozni a rejtett hálózat helyett, mind ezt magas prioritásban téve. A korábban említett felderítő kérések kiszivárogtatják az SSID-t. A támadók egyébiránt szívesen szimatolnak rejtett hálózatoknál, tehát önkéntelenül is célponttá tesszük magunkat. (ASUS 2023)

Az NSA (National Security Agency) bevált gyakorlatok az otthoni hálózatok biztonságossá tételére című dokumentuma is ezt az álláspontot képviseli. (NATIONAL SECURITY AGENCY 2023)

Az esetet megvizsgáltuk klienst és útválasztót gyártó cég szempontjából, mellette pedig állam biztonsági oldalról is. Mindhárom álláspont ugyanazt képviselte, tehát kimondhatjuk, hogy otthoni hálózatunk SSID-jának elrejtése nem segíti a biztonságot, pont az ellenkezőjét okozza.

4.3. Vendég hálózat

Biztos mindannyiunk adta már kölcsön a Wi-Fi jelszavát rokonának vagy ismerősének. Ez a látszólag ártalmatlan cselekedet nagy veszélyt rejthet a hálózat működéséből kifolyólag, hiszen akkor beszélünk hálózatról, ha az egyes eszközök kapcsolódnak egymáshoz a kommunikáció érdekében. A veszély abban rejlik, ha az egyik eszköz letölt valamilyen vírust vagy már alapból fertőzötten kapcsolódik a hálózathoz. Egyes vírusok képesek a hálózaton terjedni, megfertőzve a többi kapcsolódó készüléket. (AVER 2018) (DFT COMMUNICATIONS dn.)

Ilyen esetekben lehet hasznos a vendég hálózatok használata. A hálózatnak külön SSID-je van. Ennél a külön hozzáférési pontnál is fontos a megfelelő biztonság kialakítása, tehát jelszóval kell védeni és megfelelő titkosítási protokollt kell beállítani hozzá. Érdemes itt is törekedni az erős jelszó használatára, amiről a későbbiekben részletesebben is írni fogok. Arra is érdemes figyelni, hogy a fő hálózatunktól különböző jelszóval védjük a vendég hálózatot. Továbbá el kell különíteni, izolálni kell a fő, otthoni hálózatunktól, erre a legtöbb útválasztónál van lehetőségünk. Ezáltal nem férnek hozzá a hálózatunkon lévő megosztott fájlokhoz és nem tudnak kommunikálni az eszközeinkkel sem. Érdemes egy másik beállítást is keresni a hálózat létrehozásakor. Egy olyan beállítást, ami meggátolja az útválasztó admin felületéhez való hozzáférést. Ezen a felületen több érzékeny

beállításhoz férhetünk hozzá, például az imént említett beállításokat is itt kellett elvégezni. (AVER 2018) (DFT COMMUNICATIONS dn.)

Ahogy korábban említettem az IoT eszközök sokkal sebezhetőbbek, mint bármely más készülékek, ezért érdemes őket inkább egy vendég hálózathoz kapcsolni, ezáltal nem tudnak a vírusok átterjedni fontosabb eszközeinkre, mint az okostelefonunk, számítógépünk. Ha az említett készülékek kíbertámadás áldozatati lennének, a többi magasabb prioritással rendelkező eszközünkhöz nehezebben vagy egyáltalán nem férhetnek hozzá a támadók. (AVER 2018) (DFT COMMUNICATIONS dn.)

Az FTC (Federal Trade Commission, azaz az amerikai fogyasztóvédelem is megemlítette egy, az otthoni hálózatok biztonságáról szóló cikkében, hogy érdemes bekapcsolni a vendég hálózatot, a vírusok terjedésének megakadályozása érdekében. (FEDERAL TRADE COMMISSION 2022)

A fentiek alapján kimondhatjuk, hogy egy jó biztonsági módszerről van szó, amely segítségünkre lehet féltett eszközeink védelmében.

4.4. Alapértelmezett értékek megváltoztatása

Az alapértelmezett értékek, amellyel az útválasztók érkeznek a gyárból sokszor könnyű támadási pontot adnak a támadóknak. Az alapértelmezett SSID a legtöbb esetben meghatározza az útválasztó típusát, ezáltal a támadó kihasználhatja a konkrét típus hibáit. Az adott útválasztóhoz, pedig felhasználhatja a típushoz nyilvánosan elérhető jelszavakat. Ezért fontos ezeknek az adatoknak a megváltoztatása. (BRAIN – HOMER 2021) (CISA 2021) (FITZPATRICK 2022)

Minden Wi-Fi útválasztóhoz tartozik egy adminisztrációs felület is, ahol az adatokat lehet megváltoztatni. Itt is ajánlott megváltoztatni a bejelentkezési adatokat, hiszen ez még több támadásnak adhat lehetőséget. Egyes útválasztóknál a felhasználó nevet és a jelszót is meglehet változtatni, viszont akadnak típusok, amelyeknél csak a jelszót lehet. Ha van lehetőségünk változtassuk meg mindkét értéket, hiszen ez csökkenti a feltörés esélyét. (MITCHELL 2021) (CONSTANTIN 2018)

4.4.1. Kutatás az admin felület feltöréséről

Egy 2021-es kutatás során minden 16. Wi-Fi-t sikerült feltörni az alapértelmezett adatok használatával. A pontos érték 6,4% ($100 \div 6{,}4 \approx 16$). A kísérlet során az Amazon webáruházon található 12 legnépszerűbb Wi-Fi útválasztóra kerestek rá online és ezeken hajtották végre a támadást távolról. A támadás teljesen automatizált módon zajlott. 9927 útválasztót vizsgáltak, ezek közül 635 volt ilyen módon sebezhető. A kutatás során különböző programokkal szkennelték az internetet olyan IP címekre vadászva, amelyek ezeken az útválasztókon keresztül kapcsolódtak a webre. A kutatók a tesztelendő felhasználónév és jelszó párosokat elsőként manuálisan is letesztelték, hogy tényleg helyesek-e. (BISCHOFF 2023)

4.4.2. Tanulmány a jelszó visszafejtésről

A legtöbb internet előfizető biztos találkozott már a Wi-Fi útválasztók oldalára nyomtatott véletlenszerűnek tűnő Wi-Fi jelszóval. 2015-ben Hollandiában, egy egyetemi kutatás során az előfizetők, szolgáltatóktól kapott Wi-Fi útválasztóinak a jelszó véletlenszerűségét vizsgálták. (NOVELLA LORENTE ET AL. 2015)

A kutatás menete a következőképpen zajlott:

1. Megszerezték a holland útválasztók firmware-jét, azaz az útválasztó működéséért felelős szoftvert. Ezt többféleképpen tették meg, többek között például letöltötték a gyártó oldaláról vagy kihasználtak egy-egy sebezhetőséget az útválasztóban. Ezeken kívül, sok egyéb más módot is ismertettek.
2. Kicsomagolták, a tömörítést megszüntették.
3. A bináris firmware állományt assembly nyelvé alakították.
4. Megkeresték a jelszó generáló algoritmust.
5. Megvizsgálták annak bemenetét és kimenetét.
6. Visszafejtették az algoritmus logikáját egy magasabb rendű nyelvre.
7. Készítettek egy támadásra képes eszközt, ami képes megfejteni az alapértelmezett jelszavát az útválasztónak. (NOVELLA LORENTE ET AL. 2015)

Az algoritmus legtöbbször MAC címből, sorozatszámból és SSID-ből hozta létre a gyengének mondható jelszavakat. Az SSID-t pedig MAC címből és sorozatszámból. Ezek közül a MAC cím és SSID szabadon hozzáférhető. A MAC cím például az adatcsomagban is benne van. Azok az algoritmusok, amelyek a sorozatszámot használták sem teljesen biztonságosak, ugyanis voltak esetek amikor az SSID és jelszó is így készült. Az SSID szabadon hozzáférhető, így az algoritmussal addig próbálgathatja a támadó a random sorozatszámait, amíg meg nem kapja a hálózat SSID-jét. Ezt követően pedig létre tudja hozni a jelszót is. Az eddigiek alapján elmondhatjuk, hogy pseudo-random jelszavakról van szó. A kutatók által készült támadó eszköz percek alatt képes volt létrehozni a jelszavakat. (NOVELLA LORENTE ET AL. 2015)

A kutatások alapján kijelenthetjük, hogy kifejezetten ajánlott az alapértelmezett bejelentkezési, illetve csatlakozási értékek megváltoztatása a támadások elhárítása érdekében.

4.5. Távoli hozzáférés kikapcsolása

A távoli hozzáférés kikapcsolása az útválasztóban jó biztonsági intézkedés lehet, hiszen a kiberbűnözők kihasználhatják a támadásuk során az adminisztrációs felülethez való hozzáférés érdekében. Ez sokszor a rosszul implementált funkció miatt történhet meg. A funkció kikapcsolását sok szolgáltató nem teszi lehetővé. Ekkor érdemes megkeresni az adott szolgáltatót, hogy igényt tartanánk az funkció kikapcsolására. A beállítás kikapcsolása után, csak a hálózaton belül van lehetőség az adminisztrációs felülethez való hozzáféréshez, ami a támadások egy részét képes elhárítani. (CONSTANTIN 2018) (BRAIN – HOMER 2021)

4.6. Jelszó biztonság

A Wi-Fi jelszavakra ugyanaz a szabály vonatkozik, mint minden más felületen használt jelszóra. A felhasználóknak érdemes minél hosszabb jelszót készíteni az illetéktelen hozzáférések elkerülése érdekében. Az NSA (National Security Agency) bevált gyakorlatok az otthoni hálózatok biztonságossá tételére című dokumentuma 20 karakter hosszúságú jelszót tart biztonságosnak. A WPA titkosítási protokolltól kezdve minimum

8 és maximum 63 karakter hosszú lehet egy Wi-Fi hálózat jelszava. (HOROWITZ 2023) (NATIONAL SECURITY AGENCY 2023)

A CISA (Cybersecurity and Infrastructure Security Agency), azaz az amerikai kiberbiztonsági ügynökség az alábbi javaslatokat teszi:

- Kerülni kell a szótárakban található szavakat.
- A félreírt szavak segíthetnek egyes támadások ellen, például a szótármódszer ellen, amiről a későbbiekben lesz szó.
- Jó technika lehet egy mondat kezdő betűinek a használata is, ezáltal könnyebb lesz a jelszó memorizálása.
- Kerülni kell a híres idézeteket, dalszövegeket vagy ismert kifejezéseket.
- Minden felületen külön jelszót kell használni.
- Az adott felületen megengedett maximum hosszúságú jelszót kell használni.
- Ajánlott a jelszó menedzser használata.
- Ne használjunk személyes adatokat a jelszavakban, mert így könnyebb a támadóknak megfejteni a jelszavunkat.
- A papírlapra leírt jelszavunkat ne hagyjuk publikus helyen, ahol mások is hozzáférhetnek. (CISA 2019)

Paul Moore, információ biztonsági szakértő 2017-ben azt állította, hogy három random szó használata nem ajánlott jelszavak kreálásánál, ugyanis brute-force által viszonylag könnyű feltörni. Ez érthető, hiszen az olyan brute-force támadások, amelyek szavakat raknak össze nagyobb eséllyel törnek fel egy ilyen jellegű jelszót, mint egy karakter kombinációkra építő brute-force támadás. Három szónál a változók száma hárommal egyenlő, míg random jelszavaknál minden karakter egyenlő egy változóval, amit meg kell fejtenie a brute-force algoritmusnak. Szókombinációval 7 óra alatt fel lehet törni egy 14 karakter hosszú, 3 szót használó jelszót, míg a karakterkombinációra építő támadással ugyanezt a jelszót 10 évig tartana feltörni. (MOORE 2019)

Másik fontos szabály, hogy kerüljük a mások által már használt jelszavakat, hiszen sok közülük kikerült adatszivárgások által az internetre. Ezeket a támadók felhasználhatnak egy szótármódszeres támadás során, ahol az előbb említett jelszavakat használják fel a folyamat során. (HOROWITZ 2023)

A jelszavunkat manapság sok jelszó menedzser ellenőrzi, hogy kikerült-e valamilyen adatszivárgás során, de ezenfelül van lehetőségünk egy kiberbiztonsági weboldalon ellenőrizni, amit a következő url-en találunk meg: haveibeenpwned.com/Passwords. A weboldal a beírt jelszót SHA1 algoritmussal hash-seli a böngészőnkben, majd a hash első 5 karakterével egy szintén SHA1 algoritmussal hash-selt adatbázisban keres. Ez az adatbázis tartalmazza a kiszivárgott jelszavakat. A hash-selés az a folyamat, amikor egy bármilyen hosszúságú bemenetből, azonos hosszúságú kimenetet gyártunk egy függvény segítségével. Mivel csak az első 5 karaktert használja keresésre, így teljes anonimitásunk van, hiszen lényegesen több eredményt kapunk vissza. Átlagosan 478 elemet tartalmaz a halmaz. A hash maradék karaktereivel, pedig ebben a halmazban keres a web applikáció és ha van egyezés, akkor a jelszó kiszivárgott, ezáltal nem ajánlott a használata. (HUNT 2018) (GOOGLE 2023) (HAVEIBEENPWNED.COM 2023) (GEEKSFORGEEKS 2023)

4.7. Publikus Wi-Fi hálózatok

A publikus Wi-Fi hálózatok mindenki számára hozzáférhetőek, ezáltal nagy veszélyt rejthetnek, amit a legtöbb ember a szükség miatt elfelejt. A következőkben a Forbes kutatását fogom bemutatni ebben a témában, más forrásokkal kiegészítve.

4.7.1. Publikus Wi-Fi hálózatokról készült kutatás

A kutatás 2000 amerikai munkavállalóra irányult, akik rendszeresen használnak nyílt Wi-Fi hálózatokat. A hibahatár az adatokban +/- 2,2 pont 95%-os konfidencia szint mellett. A kutatás legfontosabb megállapítása, hogy a válaszolók 40%-ának veszélybe került már az adata nyílt Wi-Fi hálózat használata során. (HAAN 2023)

A legtöbb ember különböző oknál fogva használ publikus Wi-Fi hálózatot. A tevékenységek között egyaránt megtalálható munka és szórakozás jellegű is. Ezek közül a három leggyakoribb indítékot említem meg, amiért az emberek publikus hálózatért nyúlnak:

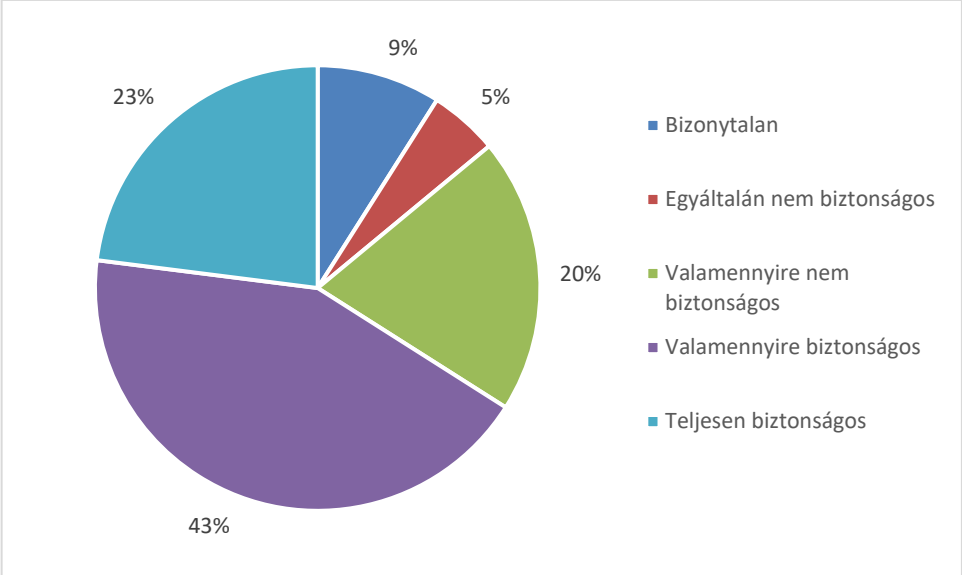
1. elfogyott vagy nincs mobilinternete a felhasználónak (32%),
2. közösségi médiát szeretné böngészni (29%),

3. online hívás indítására használja (28%). (HAAN 2023)

A válaszadók legkevesebb százaléka használja tanulásra. Sok helyen találkozhatunk nyílt hálózatokkal, de az emberek az alábbi három helyen használják a legtöbbet:

1. kávézó vagy étterem (38%),
2. hotel (38%),
3. könyvtár (33%). (HAAN 2023)

A kutatás egyik kérdése arra irányult, hogy mennyire tartják biztonságosnak nyílt Wi-Fi hálózatokat, amelyet az alábbi ábra szemléltet. (HAAN 2023)



9. ábra: A publikus Wi-Fi-ket mennyire tartják biztonságosnak a felhasználók

Forrás: saját szerkesztés HAAN 2023 alapján

Az ábrán látható, hogy a válaszolók többsége valamilyen szinten biztonságosnak tartja ezeket a hálózatokat és csupán kis százaléka gondolja inkább veszélyesnek (25%). A kérdőív kérdései között egy arra irányult, hogy egy jelszóval titkosított hálózathoz csatlakozna-e szívesebben vagy titkosítatlanhoz. A kitöltők megosztó választ adtak, hiszen majdnem 50-50%-ra bomlott az adathalmaz. 56% inkább jelszó nélküli hálózathoz csatlakozna szívesebben, 44% pedig titkosítással rendelkezőhöz. A teljesen publikus hálózatoknál a felhasználók által küldött adatcsomagokat könnyedén le lehet hallgatni, ahogy korábban említettem. Az adatcsomagok visszafejtése a weblap titkosítási

protokolljától függhet, azaz hogy használ-e HTTPS kapcsolatot. Ugyanis egyes HTTPS protokollokkal titkosított adatcsomagokat nem lehet visszafejteni későbbi időpontokban. Ezt a böngésző címsoránál található lakat ikon jelez. Ezek alapján kijelenthetjük, hogy a felhasználókat illene tájékoztatni a lehetséges veszélyekről. (HAAN 2023) (FEDERAL TRADE COMMISSION 2023) (SALTER 2019)

A válaszadók a repterek, éttermek/kávézók és tömegközlekedések Wi-Fi-jeit gondolták a legveszélyesebbnek, míg az iskolák hálózatát vélték a legkevésbé veszélyesnek. A kutatás szerint az előbb említett helyek közül ténylegesen a reptérek és éttermek/kávézók Wi-Fi-jei használata során történtek a támadások nagy százaléka. Harmadik helyen a hotelek vannak. A kitöltők 40%-a használ VPN-t miközben nyílt hálózaton böngészik. A VPN-t használók a következőképpen oszlanak meg a használati szokások alapján:

- 35% mindig használ,
- 26% gyakran használ,
- 34% néha,
- 4% ritkán vagy soha nem használ VPN-t. (HAAN 2023)

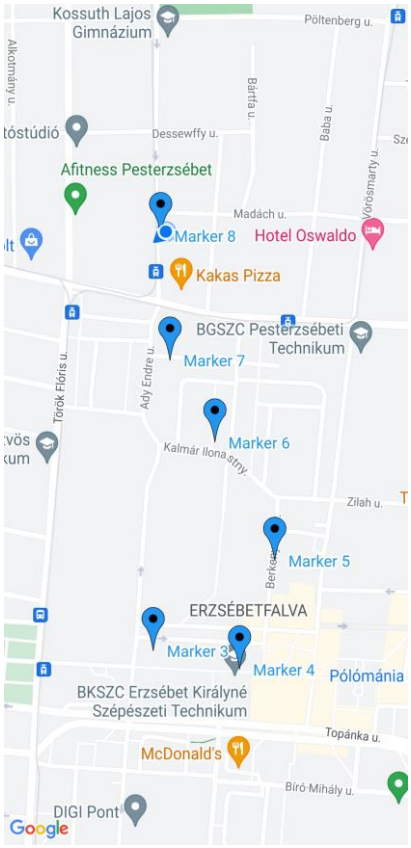
A VPN használat viszonylag magasnak mondható, ahhoz viszonyítva, hogy a legtöbb válaszoló nagyrészt biztonságosnak gondolja a nyílt Wi-Fi hálózatokat, ami feltételez egyfajta hozzá nem értést. Az, hogy a publikus hálózatot nagy százalékban biztonságosnak tartották elképzelhető, hogy a magas VPN használati aránynak köszönhető, hiszen úgy lényegesen nagyobb biztonságban vannak a felhasználók.

A WPA3 titkosítási protokoll megfelelő védelmet biztosít a publikus hálózatok használata során. Az összes adatot a kommunikáció során titkosítja, így hasonló biztonságot érhetünk el, mint egy otthoni hálózaton. (SALTER 2019) (NG 2018)

5. WI-FI HÁLÓZATOK BIZTONSÁGÁNAK FELMÉRÉSE

5.1. Elérhető Wi-Fi hálózatok elemzése

Kutatásom során egy a Google Play Store-ban elérhető open-source Wi-Fi analizáló applikáció segítségével 537 Wi-Fi adatait gyűjtöttem össze. A mintavétel típusa önkényes volt, tehát nem nevezhető reprezentatívnak. A gyűjtés menete diszkrét esetekből állt és az egyes gyűjtési pontokat a térképen, egy másik Androidra elérhető applikációval rögzítettem, hogy követhető legyen a mintavétel. Az alábbi ábrán láthatjuk, hogyan is néz ki. A Marker-ek jelzik a gyűjtési pontokat. (DARÓCZI 2008)



10. ábra: Wi-Fi adatgyűjtési pozíciók

Az összegyűjtött adatok a következőképpen néztek ki:

Time Stamp|SSID|BSSID|Strength|Primary Channel|Primary Frequency|Center Channel|Center Frequency|Width (Range)|Distance|Timestamp|802.11mc|Security

2023/11/29-12:44:05|OE-hotspot|00:0c:42:6b:a5:d5|-83dBm|6|2437MHz|6|2437MHz|20MHz (2427 - 2447)|~138.2m|860762527128|false|[ESS]

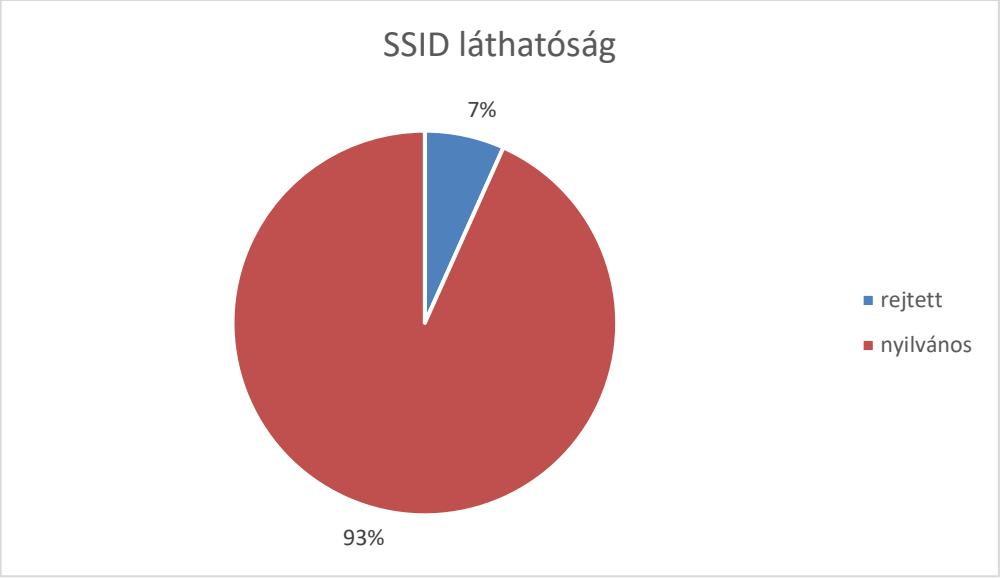
Észrevehetjük, hogy hasonlít egy CSV fájlra, egy különbségben, hogy itt az adatok nem vesszővel, hanem egy függőleges vonallal vannak tagolva, ami beimportálható Excelbe. Az elemzés így könnyedén kivitelezhető.

5.1.1. Célok ismertetése

A kutatás célja megkeresni azokat a hálózatokat, amelyek rejtett SSID-t használnak és feltérképezni, hogy mennyire elterjedt a WPA3 használata. Ezenfelül megvizsgálni, hogy mennyi hálózat használ WPS-t és a biztonság szempontjából veszélyesnek mondható titkosítási protokollt.

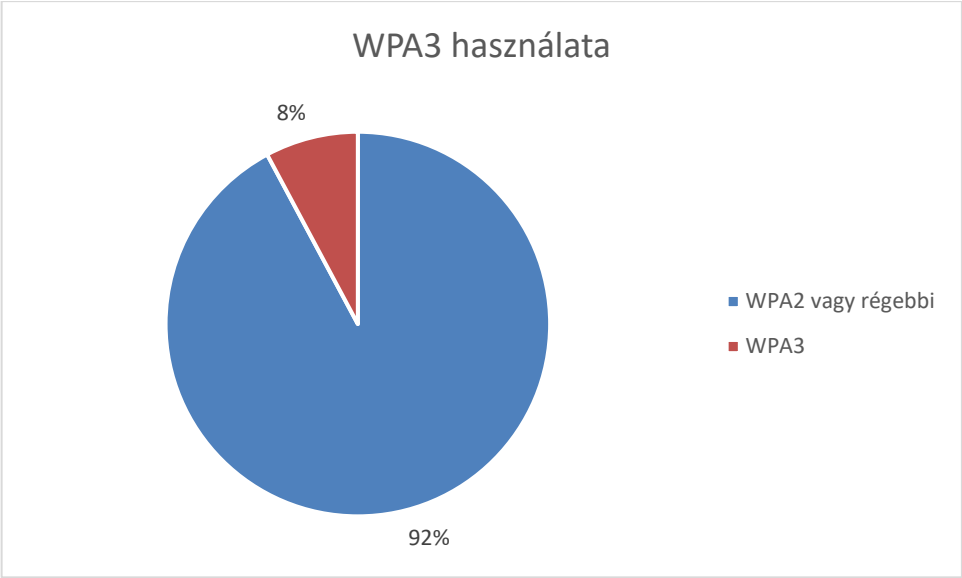
5.1.2. Elemzés

A kísérlet során a következő eredmények születtek.



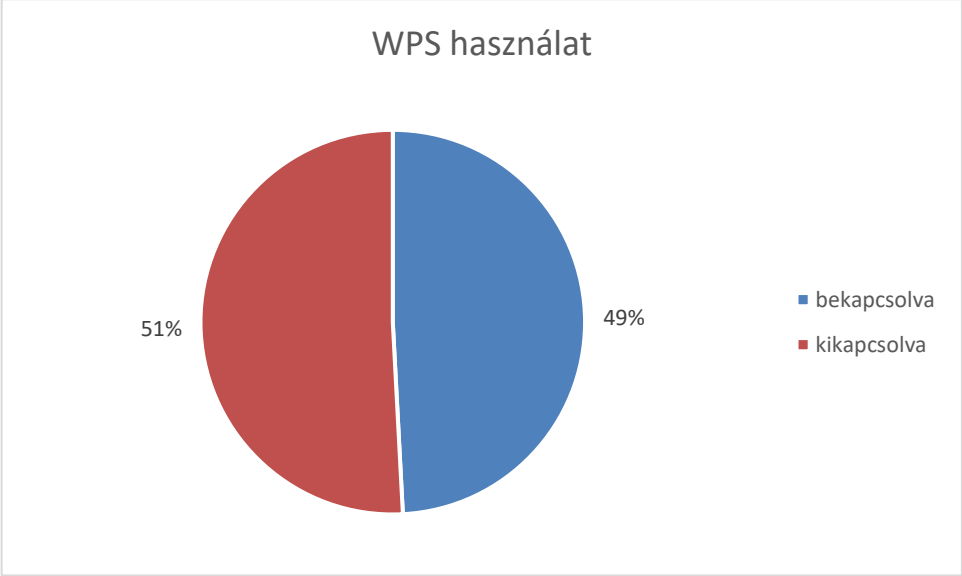
11. ábra: SSID-k láthatósága

Láthatjuk, hogy szerencsére nem sok hálózat rejti el az SSID-jét, ami a biztonság szempontjából veszélyes lehet. Ezt a Wi-Fi biztonság fejezetében fejtettem ki részletesen.



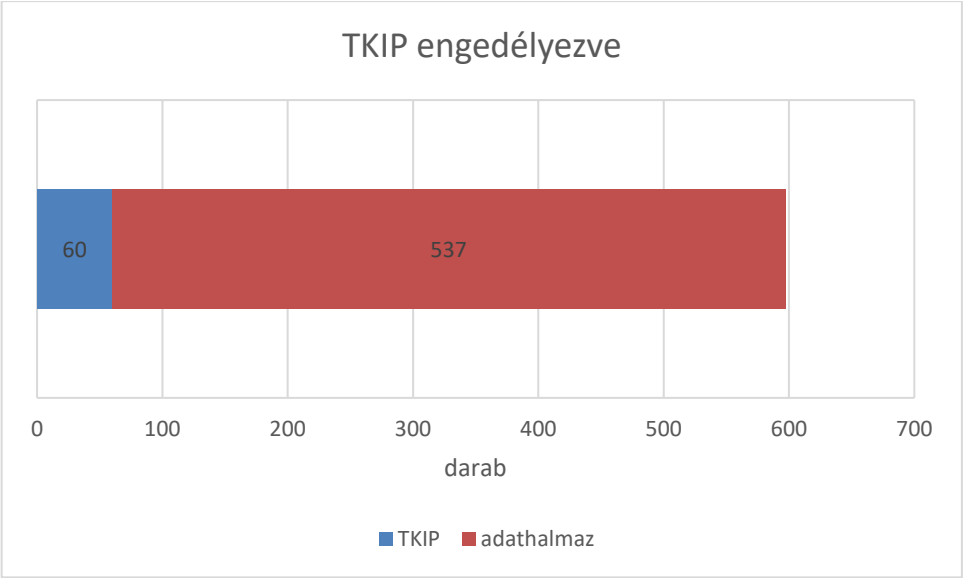
12. ábra: WPA3 használatának elterjedése

A WPA3 használata csupán 8%-ot tesz ki. A WPA2-t használó hálózatoknál meg van az esély a KRACK támadás használatára, ami jelentős veszélyt jelent.



13. ábra: WPS funkció használatának eloszlása

A WPS funkció bekapcsolva hagyása Wi-Fi törési módszereknek adhat szabadutat.



14. ábra: TKIP engedélyezési aránya

Az utolsó diagrammal azt vizsgáltam, hogy mennyi hálózat használ teljesen elavult technológiát. A TKIP titkosítás használatának esélyét is meghagyó hálózatok száma nem nevezhető kifejezetten magasnak, de ha úgy nézzük, hogy mekkora biztonsági rést hagy a hálózaton és ha a technológia korát nézzük, úgy viszont mérsékelten magasnak mondható.

5.1.3. Következtetés

A legnagyobb veszélyt a KRACK támadás rejti még manapság is az IoT eszközök által. Ezenfelül a WPS támadásra is nagy esélye lehet a hálózatoknak tekintve, hogy sok hálózat még mindig megadja a TKIP használatának az esélyét is, ami egy modern Wi-Fi útválasztónál nem megengedett. Ebből pedig lehet következtetni arra, hogy az emberek nagy százaléka elavult készülékeket használhat. Tehát a KRACK és WPS támadás is kivitelezhető sok hálózatnál. Összességében kijelenthetjük, hogy megannyi hálózatnál meg van a feltörésre való lehetőség esélye.

5.2. Kérdőíves felmérés

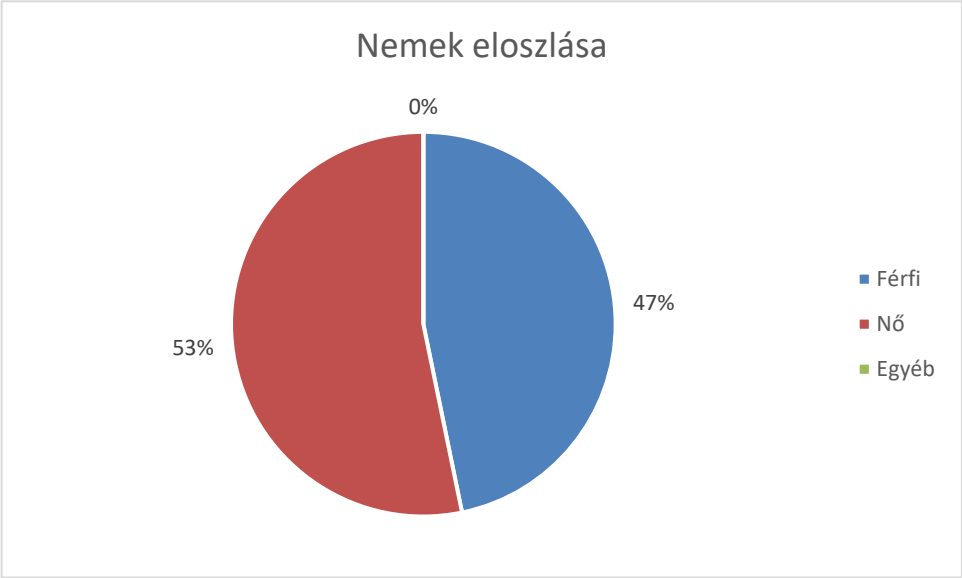
Hólabda módszerű mintavétellel kérdőíves kutatást végeztem. A kérdőívre 2 hét folyamán lehetett válaszokat leadni. Ez idő alatt 62 válasz érkezett. Nem nevezhető tehát reprezentatívnak a kutatás, viszont érdekességnek és feltételezések felállításához megfelelő. A kérdéseim felállításához az alapértelmezett értékek megváltoztatása és jelszó biztonság alfejezeteket vettem alapul, kérdéseim tehát ezekre a témakörökre irányulnak.

5.2.1. Célok ismertetése

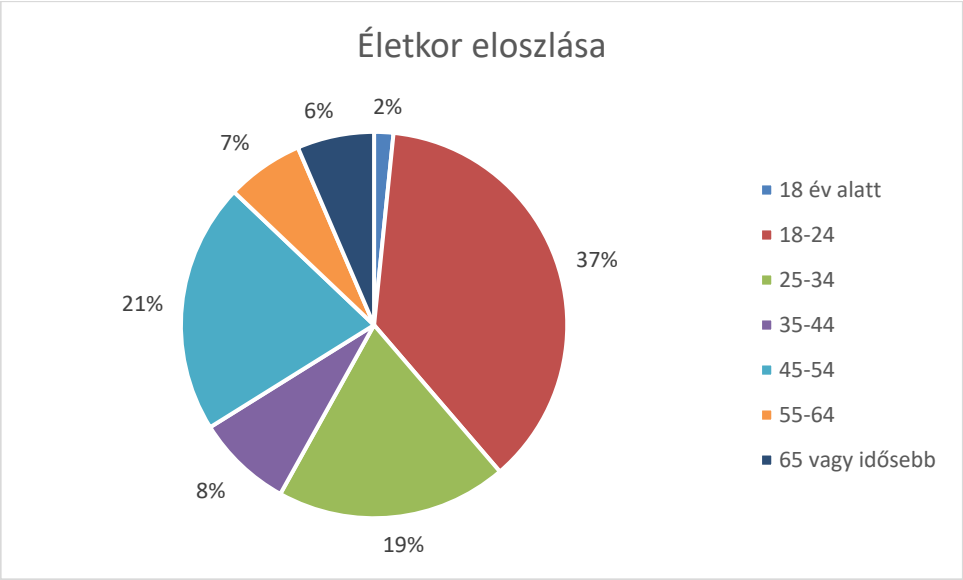
A kérdőívem célja, hogy rálátást szerezzek azzal kapcsolatban, hogy hányan változtatják meg az alapértelmezett SSID-t és jelszót. Abban az esetben, ha a válaszoló megváltoztatta a jelszavát, megszeretném tudni, hogy az mennyire biztonságos.

5.2.2. Elemzés

A kérdőív kezdetén alapvető adatokat kérdeztem meg, mint a válaszoló neme és életkora. Életkornál intervallumokat használtam az ábrákon való jobb megjelenítés érdekében.



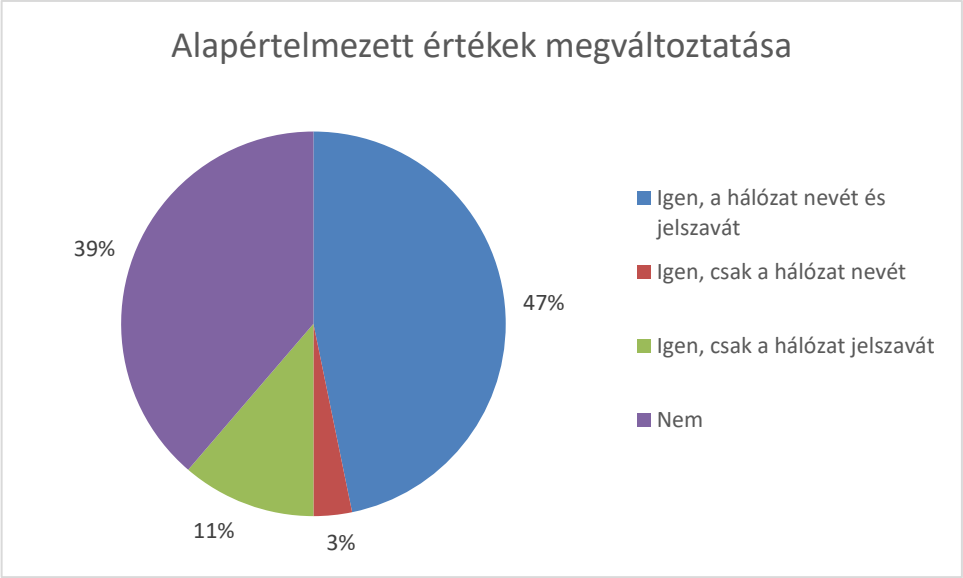
15. ábra: Nemek eloszlása



16. ábra: Életkor eloszlása

A férfiak és a nők aránya majdnem megegyezett. Az életkorok tekintetében a 18-24, 45-54 és 25-34 évesek voltak többségben.

A következő kérdésem arra kérdezett rá, hogy a válaszadó megváltoztatta-e a Wi-Fi hálózat alapértelmezett csatlakozási értékeit. Itt 4 válasz közül lehetett választani és egyszerre csak egyet. A következő ábra ezt jól bemutatja.



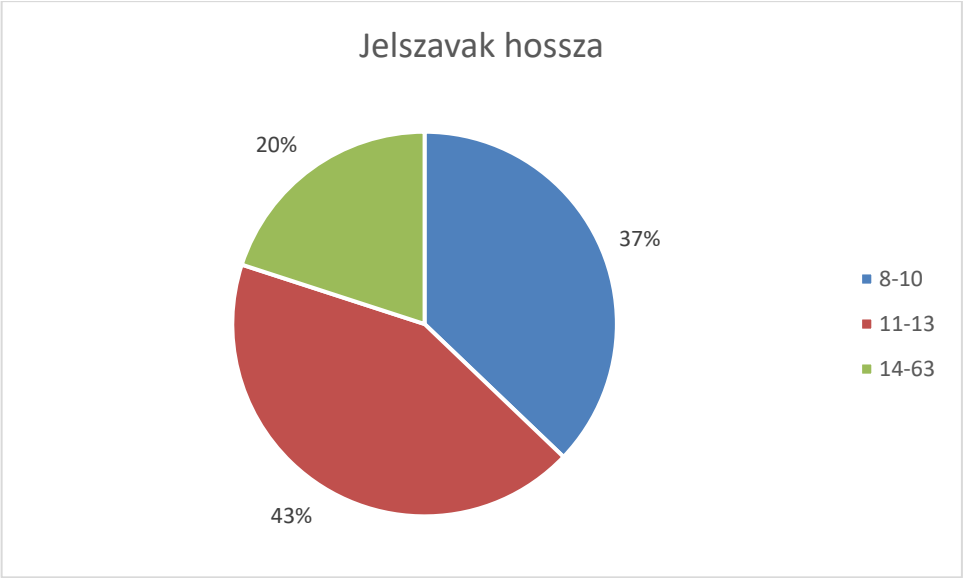
17. ábra: Alapértelmezett értékek megváltoztatásának aránya

Látható, hogy 39% egyáltalán nem változtatta meg az alapértelmezett értékeket, ezáltal ahogy a jelszó biztonság fejezetében említettem sebezhetőek. Akik csak a hálózat SSID-jét változtatták meg, nagyobb biztonságban vannak, hiszen az útválasztót nehezebb így azonosítani és mivel egyes útválasztóknál az SSID-ből hozták létre az alapértelmezett jelszót, ezáltal annak visszafejtését ellehetetleníti.

A következőkben azt vizsgáltam, hogy akik megváltoztatták a jelszavukat, azok ténylegesen segítették a hálózatuk biztonságát vagy megkönnyítették a támadás lehetőségét.

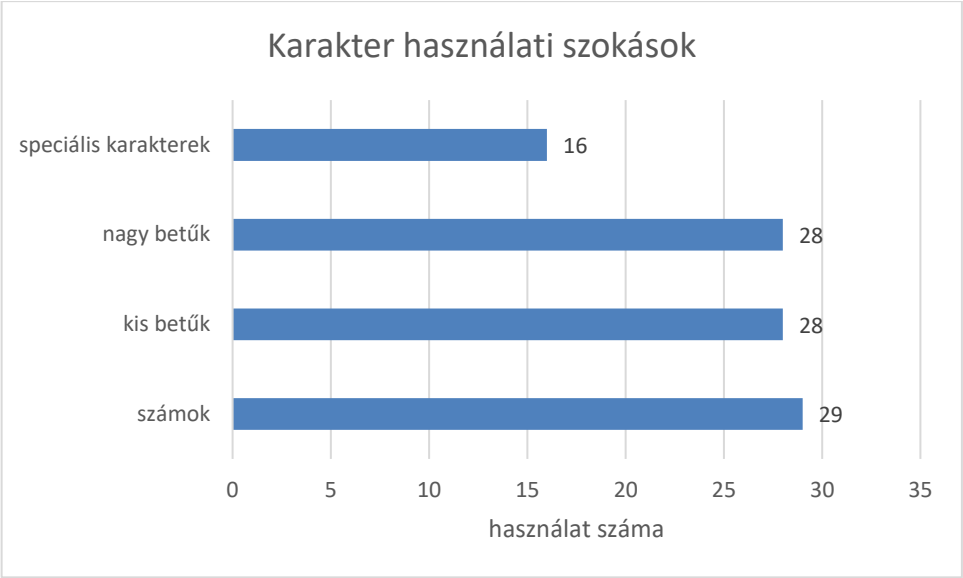
18. ábra: Jelszó újrahasználás

31% máshol is használta azt a jelszót, amit a hálózatának adott. A jelszó biztonság fejezetében ismertettem, hogy nem ajánlott többször is használni egy jelszót, mert növeli a feltörés esélyét. Az eredmény jelentősnek mondható. A kérdőív következő kérdésével a jelszó hosszát vizsgáltam.



19. ábra: Jelszavak hossza

A válaszokat intervallumokban adtam meg. Az intervallumok szélsőértékeit a Bitwarden jelszóbiztonságra irányuló cikke alapján határoztam meg. A Bitwarden egy jelszó menedzselő applikáció. A cikk szerint a 8-10 hosszúságú jelszó gyengének, a 11-13 közepesnek és a 14-63 erősnek számít. Az intervallum készítésénél figyelembe vettem a WPA protokoll minimum és maximum jelszó hosszúságát, amit korábban a jelszó biztonság fejezetében ismertettem. Látható, hogy az emberek jelentős százaléka gyenge vagy közepes jelszót hozott létre (37%, 43%). Utolsó kérdésem a karakter használati szokásokra irányult. A Bitwarden cikkéből ugyanis kiderült, hogy ha minél nagyobb karakterkészlettel hozunk létre egy jelszót, annál nehezebb annak a feltörése. (ORENSTEIN 2022)



20. ábra: Karakter használati szokások

Az ábrából látható, hogy a speciális karakterek kivételével, amelyet lényegesen kevesebb ember használt, a válaszadók bátran alkalmaztak kis és nagy betűket, számokat. Általánosságban tehát elmondható, hogy nagy karakterkészlettel dolgoztak a válaszolók a jelszavuk létrehozásánál.

5.2.3. Következtetés

Az eredmények alapján megállapíthatjuk, hogy az emberek nem fordítanak kellő figyelmet az otthoni Wi-Fi hálózatuk biztonságára. Ez megnyilvánul abban, hogy a válaszolók jelentős százaléka nem változtatják meg az alapértelmezett bejelentkezési adatait. Egyéb észrevételem, hogy sokan a válaszolók közül feltételezhetően azzal a szándékkal változtatták meg a Wi-Fi hálózatuk jelszavát, hogy könnyítsék a bejelentkezésüket, ami a jelszó hosszának gyakori rövidségéből és az újrafelhasználás magas számából látszódik.

6. ÖSSZEFOGLALÁS

A dolgozatom során részletesen bemutattam a Wi-Fi technológiát, amiből kiderült, hogy milyen komplex eszközöket használunk nap, mint nap. A komplexitás folytán sok hibát véthetnek a technológia fejlesztői, amit a támadók kitudnak használni a hálózatok illetéktelen hozzáféréséhez és különböző bűntettek végrehajtásához. A dolgozat során ismertettem a főbb támadási módszereket és relevanciájukat. Ezenfelül a biztonság szempontjából hasznos gyakorlatokat is bemutattam, amik segítségével felvehetjük a versenyt a támadókkal szemben. Végül felmértem, hogy az emberek mennyire védik a hálózatukat, amiből kiderült, hogy sok esetben támadhatóak különböző módszerekkel és jelentős százalékuk nem foglalkozik kellően a biztonsággal.

IRODALOMJEGYZÉK

1. S. TANENBAUM Andrew – J. WETHERALL David (2013): Számítógép-hálózatok. Panem könyvek, Taramix Kft., Budapest, 2013. (Elérhető: https://gyires.inf.unideb.hu/GyBITT/30/)

Elektronikus hivatkozások

1. What Is Wi-Fi?. Cisco, dn. https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html (Utolsó letöltés: 2023.11.11.)
2. Who We Are, Our Brands. Wi-Fi Alliance https://www.wi-fi.org/who-we-are/our-brands (Utolsó letöltés: 2023.11.11.)
3. IEEE STANDARDS ASSOCIATION (IEEE SA) (2023): The Evolution of Wi-Fi Technology and Standards. IEEE, 2023. május 16. https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/ (Utolsó letöltés: 2023.11.13.)
4. What Is a Wireless Router? Wi-Fi Router. Cisco, dn. https://www.cisco.com/c/en/us/products/wireless/wireless-router.html (Utolsó letöltés: 2023.11.13.)
5. What is a Router?. Cisco, dn. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-router.html (Utolsó letöltés: 2023.11.13.)
6. What is an Access Point?. Cisco, dn. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-access-point.html (Utolsó letöltés: 2023.11.13.)
7. What Is an Access Point and How Is It Different From a Range Extender?. Linksys, dn. https://www.linksys.com/what-is-a-wifi-access-point.html (Utolsó letöltés: 2023.11.13.)
8. LOHNES Kate (2017): How Does Wi-Fi Work?. Encyclopedia Britannica, 2017. október 25. https://www.britannica.com/story/how-does-wi-fi-work (Utolsó letöltés: 2023.11.28.)
9. BRITANNICA, THE EDITORS OF ENCYCLOPAEDIA (2023): frequency. Encyclopedia Britannica, 2023. augusztus 1.

https://www.britannica.com/science/frequency-physics (Utolsó letöltés: 2023.11.28.)

10. BRAIN Marshall - HOMER Talon (2021): How WiFi Works. HowSuffWorks, 2021. augusztus 17. https://computer.howstuffworks.com/wireless-network.htm (Utolsó letöltés: 2023.11.28.)
11. GRIDELLI Stefano (2019): How WiFi Connection Works. NetBeez, 2019. június 26. https://netbeez.net/blog/how-wifi-connection-works/ (Utolsó letöltés: 2023.11.28.)
12. S. GILLIS Alexander (2022): Wi-Fi Protected Access (WPA). TechTarget, 2022. december https://www.techtarget.com/searchmobilecomputing/definition/Wi-Fi-Protected-Access (Utolsó letöltés: 2023.11.28.)
13. Wireless Security Wi-Fi Authentication Modes. tutorialspoint, dn. https://www.tutorialspoint.com/wireless_security/wireless_security_wifi_authentication_modes.htm (Utolsó letöltés: 2023.12.06.)
14. UY Melanie (2020): Wi-Fi Tutorial: How to Connect to a Wireless Network. LifeWire, 2020. május 4. https://www.lifewire.com/wi-fi-tutorial-how-to-connect-to-a-wireless-network-2378222 (Utolsó letöltés: 2023.12.06.)
15. Wi-Fi, 2023. https://www.wi-fi.org/ (Utolsó letöltés: 2023.12.01.)
16. CISCO PRESS (2017): WiFi Networking: Radio Wave Basics. NetworkComputing, 2017. január 11. https://www.networkcomputing.com/wireless-infrastructure/wifi-networking-radio-wave-basics (Utolsó letöltés: 2023.12.01.)
17. AQUIRRE Austin (2022): Understanding Wi-Fi Frequencies: Choosing Between 2.4 GHz and 5 GHz. HighSpeedInternet, 2022 október 20. https://www.highspeedinternet.com/resources/2-4-ghz-vs-5-ghz-wi-fi (Utolsó letöltés: 2023.12.01.)
18. WELLING Jon (2022): Frequency, Amplitude, Phase: 3 RF Characteristics. CBTnuggets, 2022. március 24. https://www.cbtnuggets.com/blog/technology/networking/frequency-amplitude-phase-3-rf-characteristics (Utolsó letöltés: 2023.12.02.)

19. MONDAL Soumik (2021): What is Wi-Fi?. GeeksForGeeks, 2021. december 28. https://www.geeksforgeeks.org/what-is-wi-fiwireless-fidelity/ (Utolsó letöltés: 2023.12.02.)
20. What is WiFi Channel and Channel Width?. WiFiAdviser, dn. https://wifiadviser.com/blog/what-is-wifi-channel-width/ (Utolsó letöltés: 2023.12.03.)
21. Why a router has two WiFi bands and how they work. NetSpot, dn. https://www.netspotapp.com/blog/all-about-wifi/why-a-router-has-two-wifi-frequency-bands.html (Utolsó letöltés: 2023.12.03.)
22. SIGNALBOOSTERS.COM (2022): What is WiFi and How Does It Work?. SignalBoosters, 2022. április 4. https://www.signalboosters.com/blog/what-is-wifi-and-how-does-it-work/ (Utolsó letöltés: 2023.12.03.)
23. ALBALO Pedro (2022): Why are WiFi channels 1, 6 and 11 used on 2.4GHz?. Acrylic, 2022. április 20. https://www.acrylicwifi.com/en/blog/why-are-wifi-channels-1-6-and-11-used-on-2-4ghz/ (Utolsó letöltés: 2023.12.03.)
24. SIGNALBOOSTERS.COM (2020): What are the WiFi IEEE 802.11 Standards?. SignalBoosters, 2020. október 29. https://www.signalboosters.com/blog/what-are-the-wifi-ieee-80211-standards/ (Utolsó letöltés: 2023.12.03.)
25. ROUSE Margaret (2012): Industrial, Scientific and Medical Radio Band. Technopedia, 2012. április 25. https://www.techopedia.com/definition/27785/industrial-scientific-and-medical-radio-band-ism-band (Utolsó letöltés: 2023.12.03.)
26. DROTÁR István – KOVÁCS Ákos (2013): Kommunikációs Rendszerek Programozása. Széchenyi István Egyetem, 2013. november 14. https://www.tilb.sze.hu/tilb/targyak/NGB_TA024_1/WiFi_jegyzet_2013.pdf (Utolsó letöltés: 2023.12.04.)
27. MITCHELL Bradley (2021): What Is a Service Set Identifier (SSID)?. LifeWire, 2021. május 20. https://www.lifewire.com/definition-of-service-set-identifier-816547 (Utolsó letöltés: 2023.12.04.)
28. 802.11 TOPOLOGIES AKA SERVICE SETS. WiFi Professionals, 2019. március 3. https://www.wifi-professionals.com/2019/03/802-11-topologies-aka-service-sets (Utolsó letöltés: 2023.12.04.)

29. TUCKER Chloe (2020): The OSI Model – The 7 Layers of Networking Explained in Plain English. freeCodeCamp, 2020. december 21. https://www.freecodecamp.org/news/osi-model-networking-layers-explained-in-plain-english/ (Utolsó letöltés: 2023.12.04.)
30. SAM Samuel (2023): Medium Access Control Sublayer (MAC sublayer). tutorialspoint, 2023. október 31. https://www.tutorialspoint.com/medium-access-control-sublayer-mac-sublayer (Utolsó letöltés: 2023.12.04.)
31. GEEKSFORGEEKS (2023): What is MAC Address?. GeeksForGeeks, 2023. október 19. https://www.geeksforgeeks.org/mac-address-in-computer-network/ (Utolsó letöltés: 2023.12.04.)
32. JOHNSON Allan (2020): Wireless Concepts. Cisco Press, 2020. március 27. https://www.ciscopress.com/articles/article.asp?p=2999384&seqNum=6 (Utolsó letöltés: 2023.12.04.)
33. Wireless Security Protocols: WEP, WPA, WPA2, and WPA3. NetSpot, dn. https://www.netspotapp.com/blog/wifi-security/wifi-encryption-and-security.html (Utolsó letöltés: 2023.12.04.)
34. SLATER Jim (2019): A brief history of Wi-Fi security protocols from “oh my, that’s bad” to WPA3. Ars Technica, 2019. október 3. https://arstechnica.com/gadgets/2019/03/802-eleventy-who-goes-there-wpa3-wi-fi-security-and-what-came-before-it/ (Utolsó letöltés: 2023.12.04.)
35. RANA Muhammad Ehsan - ARUN Kuruvikulam. (2021): Common Security Protocols for Wireless Networks: A Comparative Analysis. ResearchGate, 2021. szeptember. https://www.researchgate.net/publication/354887719_Common_Security_Protocols_for_Wireless_Networks_A_Comparative_Analysis (Utolsó letöltés: 2023.12.04.)
36. HOFFMAN Chris (2017): What Is an SSID, or Service Set Identifier?. How-To Geek, 2017. december 7. https://www.howtogeek.com/334935/what-is-an-ssid-or-service-set-identifier/ (Utolsó letöltés: 2023.12.06.)
37. A Wi-Fi-routerek és -hozzáférési pontok ajánlott beállításai. Apple, 2023. október 11. https://support.apple.com/hu-hu/HT202068 (Utolsó letöltés: 2023.12.06.)

38. [Wireless Router] Hidden SSID: Few things you should know. Asus, 2023. május 26. https://www.asus.com/US/support/FAQ/1047947 (Utolsó letöltés: 2023.12.06.)
39. Best Practices for Securing Your Home Network. National Security Agency. 2023. február https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF (Utolsó letöltés: 2023.12.06.)
40. AVER Hugh (2018): What's a guest Wi-Fi network, and why do you need one?. Kaspersky, 2018. szeptember 17. https://www.kaspersky.com/blog/guest-wifi/23843/ (Utolsó letöltés: 2023.12.07.)
41. What's a guest Wi-Fi network and why do you need one?. DFT Communications, dn. https://dftcommunications.com/internet-and-wi-fi/whats-a-guest-wi-fi-network-and-why-do-you-need-one/ (Utolsó letöltés: 2023.12.07.)
42. How To Secure Your Home Wi-Fi Network. Federal Trade Commission, 2022. december. https://consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network (Utolsó letöltés: 2023.12.07.)
43. MITCHELL Bradley (2021): MAC Address Filtering: What It Is and How It Works. LifeWire, 2021. augusztus 4. https://www.lifewire.com/enabling-mac-address-filtering-wireless-router-816571 (Utolsó letöltés: 2023.12.07.)
44. BABU Sandeep (2022): Everything You Need to Know About MAC Address Filtering. MakeUseOf, 2022. december 29. https://www.makeuseof.com/mac-address-filtering-explained/ (Utolsó letöltés: 2023.12.07.)
45. CONSTANTIN Lucian (2018): How to Protect Your Home Router from Attacks. Vice, 2018. január 3. https://www.vice.com/en/article/9kn3g7/how-to-protect-your-home-router-from-attacks (Utolsó letöltés: 2023.12.08.)
46. Securing Wireless Networks. Cisa, 2021. február 1. https://www.cisa.gov/news-events/news/securing-wireless-networks (Utolsó letöltés: 2023.12.08.)
47. BISCHOFF Paul (2023): One in 16 home wi-fi routers tested vulnerable to default password attacks: report. CompariTech, 2023. augusztus 8. https://www.comparitech.com/blog/information-security/default-password-routers-study/ (Utolsó letöltés: 2023.12.08.)

48. FITZPATRICK Jason (2022): Is Your Router's Default Wi-Fi Password a Security Risk?. How-To Geek, 2022. szeptember 1. https://www.howtogeek.com/826701/is-your-routers-default-wi-fi-password-a-security-risk/ (Utolsó letöltés: 2023.12.08.)
49. MITCHELL Bradley (2021): Why You Should Change the Default Password on a Wi-Fi Router. LifeWire, 2021. július 7. https://www.lifewire.com/changing-default-password-on-wifi-network-816567 (Utolsó letöltés: 2023.12.08.)
50. NOVELLA LORENTE Eduardo – MEIJER Carlo – VERDULT Roel (2015): Scrutinizing WPA2 Password Generating Algorithms in Wireless Routers. USENIX Association, 2015. augusztus. https://www.usenix.org/system/files/conference/woot15/woot15-paper-lorente.pdf (Utolsó letöltés: 2023.12.09.)
51. MOORE Paul (2019): Passwords: Using 3 Random Words Is A Really Bad Idea!. Paul.reviews, 2019. szeptember 23. https://paul.reviews/passwords-why-using-3-random-words-is-a-really-bad-idea/ (Utolsó letöltés: 2023.12.09.)
52. HOROWITZ Michael (2023): WiFi Passwords. Router Security, 2023. március 14. https://routersecurity.org/wifi.passwords.php (Utolsó letöltés: 2023.12.09.)
53. Save, manage & protect your passwords. Google, 2023. https://support.google.com/accounts/answer/6208650#zippy=%2Ccheck-for-unsafe-passwords (Utolsó letöltés: 2023.12.09.)
54. Pwned Passwords. haveibeenpwned.com, 2023. https://haveibeenpwned.com/Passwords (Utolsó letöltés: 2023.12.09.)
55. HUNT Troy (2018): I've Just Launched "Pwned Passwords" V2 With Half a Billion Passwords for Download. TroyHunt, 2018. február 22. https://www.troyhunt.com/ive-just-launched-pwned-passwords-version-2/ (Utolsó letöltés: 2023.12.09.)
56. Choosing and Protecting Passwords. CISA, 2019. november 18. https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords (Utolsó letöltés: 2023.12.09.)
57. NG Alfred (2018): Your local public Wi-Fi network may be a whole lot safer soon. CNET, 2018. január 8. https://www.cnet.com/news/privacy/public-wifi-ces-wpa3-security-privacy-online-traffic-safe/ (Utolsó letöltés: 2023.12.09.)

58. HAAN Katherine (2023): The Real Risks Of Public Wi-Fi: Key Statistics And Usage Data. Forbes, 2023. február 9. https://www.forbes.com/advisor/business/public-wifi-risks/ (Utolsó letöltés: 2023.12.09.)
59. Are Public Wi-Fi Networks Safe? What You Need To Know. Federal Trade Commission, 2023. február. https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know (Utolsó letöltés: 2023.12.09.)
60. POSTON Howard (2021): 13 popular wireless hacking tools [updated 2021]. Infosec, 2021. május 6. https://resources.infosecinstitute.com/topics/hacking/13-popular-wireless-hacking-tools/ (Utolsó letöltés: 2023.12.10.)
61. REED Catherine (2022): How WPS Attacks Work – And How to Protect Your Network. Firewall Times, 2022. október 3. https://firewalltimes.com/wps-attacks/ (Utolsó letöltés: 2023.12.10.)
62. WPS PIN attacks: How to crack WPS-enabled Wi-Fi networks with Reaver. HackTheBox, 2023. október 10. https://www.hackthebox.com/blog/wps-pin-attacks-and-cracking-wps-with-reaver (Utolsó letöltés: 2023.12.10.)
63. GRIGUTYTÉ Monika (2023): SSH public key authentication explained: What it is and how to generate an SSH public key. NordVPN, 2023. szeptember 4. https://nordvpn.com/blog/ssh-public-key-authentication/ (Utolsó letöltés: 2023.12.10.)
64. GOODIN Dan (2017): Serious flaw in WPA2 protocol lets attackers intercept passwords and much more. ArsTechnica, 2017. október 16. https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/ (Utolsó letöltés: 2023.12.10.)
65. An overview of the Wi-Fi WPA2 vulnerability. ENISA, 2017. október 19. https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability (Utolsó letöltés: 2023.12.10.)
66. VANHOEF Mathy (2023): Key Reinstallation Attacks. KU Leuven, 2017. https://www.krackattacks.com/ (Utolsó letöltés: 2023.12.10.)
67. STEPHENSON Brad (2023): How to Use a Router as a Wi-Fi Extender. LifeWire, 2023. október 5. https://www.lifewire.com/use-router-as-wifi-extender-5190828 (Utolsó letöltés: 2023.12.10.)

68. MACBRIDE Elizabeth (2023): The dark web’s criminal minds see Internet of Things as next big hacking prize. CNBC, 2023. január 9. https://www.cnbc.com/2023/01/09/the-dark-webs-criminal-minds-see-iot-as-the-next-big-hacking-prize.html (Utolsó letöltés: 2023.12.10.)
69. HOORVITCH Ido (2021): Cracking WiFi at Scale with One Simple Trick. CyberArk, 2021. október 26. https://www.cyberark.com/resources/threat-research-blog/cracking-wifi-at-scale-with-one-simple-trick (Utolsó letöltés: 2023.12.10.)
70. ORENSTEIN Gary (2022): How long should my password be?. Bitwarden, 2022. október 11. https://bitwarden.com/blog/how-long-should-my-password-be/ (Utolsó letöltés: 2023.12.11.)
71. DARÓCZI Gergely (2008): Mintavételi eljárások. PPKE-BTK, 2008. október 6. https://ppke.snowl.net/files/2010/08/mintavetel.pdf (Utolsó letöltés: 2023.12.11.)

TARTALMI KIVONAT

A szakdolgozat során bemutatásra került a Wi-Fi technológia részletes működése és a fontosabb komponensei. Ez a fejezet jól bemutatta mennyire komplex technológiáról van szó. A komplex rendszerek sok hibát rejthetnek, amit a támadók kitudnak használni támadásaik során. A dolgozat második fejezetében a lényeges, mindenkit érintő támadási lehetőségek kerültek tisztázásra. Szó esett arról, hogy mennyire relevánsak az említett törési módszerek manapság úgy, hogy léteznek már az elhárításukkal rendelkező technológiák. A harmadik fejezet bemutatta a bevett gyakorlatokat a Wi-Fi hálózatok biztosítására. Az utolsó fejezetben elemzésre kerültek a publikusan elérhető Wi-Fi hálózatok, ami feltérképezte, hogy van-e könnyedén beazonosítható támadási pontjuk. Ezenfelül egy kérdőíves kutatással részletesebben is kivizsgálásra kerültek az otthoni Wi-Fi hálózatok biztonságának állapotai.

SUMMARY

The detailed operation of Wi-Fi technology and its most important components were presented during the thesis. This chapter has shown how complex technology is. Complex systems can hide many errors that attackers can exploit during their attacks. In the second chapter of the thesis, the essential attack possibilities affecting everyone were clarified. It was discussed how relevant the mentioned craking methods are today, as there are already technologies to prevent them. The third chapter presented best practices for securing Wi-Fi networks. In the last chapter, publicly available Wi-Fi networks were analyzed, which mapped whether they have easily identifiable attack points. In addition, the state of security of home Wi-Fi networks was investigated in more detail with a questionnaire survey.