DEBRECENI EGYETEM
INFORMATIKAI KAR

VEZETÉK NÉLKÜLI HÁLÓZATOK BIZTONSÁGI KÉRDÉSEI

Témavezető:

Dr. Krausz Tamás
egyetemi adjunktus

Készítette:

Tóth János
programtervező matematikus

DEBRECEN
2010

0. Bevezetés

A vezeték nélküli hálózati technológiák megjelenése az 1990-es évek elejére tehető, azonban robbanásszerű elterjedésük 2000 után következett be a vezeték nélküli hálózati szabványok megjelenésének, valamint a szükséges hardverek előállítási költségének jelentős csökkenésének hatására. Az utóbbi években a vezeték nélküli hálózati hozzáférés és az eszközök könnyű összekapcsolásának igénye egyre jelentősebbé vált, így mára már szinte az összes hordozható eszköz rendelkezik ilyen képességekkel. Azonban a vezeték nélküli hálózatok széles körben történő felhasználása új biztonsági kérdéseket vetett fel.

A legnagyobb különbség a vezetékes és a vezeték nélküli hálózatok között biztonsági szempontból az, hogy egy vezetékes hálózat elleni támadáshoz a támadónak fizikai hozzáféréssel kell rendelkeznie ahhoz (vagy valamilyen más módon távolról kell változtatásokat végrehajtani azon), amíg egy vezeték nélküli hálózat esetén elegendő annak hatósugarán belül tartózkodnia. Sőt, a támadónak akár arra is lehetősége van, hogy nagy érzékenységű irányantennák használatával a támadáshoz használt eszközök hatósugarát jelentősen kiterjessze[1]. Emiatt a vezeték nélküli hálózatok elleni támadások nagyrészt az adatforgalom viszonylagosan könnyű lehallgathatóságán és az abba történő könnyű üzenet-beillesztésen alapulnak. Fontos azt is megjegyezni, hogy a vezeték nélküli hálózatok gyakran nem önállóan, hanem egy vezetékes hálózathoz csatlakozva működnek, így az onnan érkező támadásokra is fel kell készülni. A vezeték nélküli hálózatok elleni támadásokat két fő csoportba lehet sorolni: aktív és passzív támadások.

A *passzív támadások* közé azok a támadások tartoznak, amelyek során egy jogosulatlan személy hozzáférést szerez a hálózathoz, de nem zavarja meg annak működését és nem módosítja az átvitt adatokat sem. Két fajta passzív támadást szokás megkülönböztetni:

- lehallgatás: a támadó megfigyeli a hálózati adatátvitelt, hogy így olyan bizalmas információkhoz jusson hozzá, mint például hitelesítési adatok és jelszavak.

[1] Például 2004-ben egy kísérlet során a trifinite.group tagjainak sikerült 1,78 kilométer távolságról támadást indítaniuk Bluetooth-on keresztül egy Nokia 6310i készülék ellen, miközben az abban található Bluetooth egység hatósugara legfeljebb 10 méter.
Bővebben: http://trifinite.org/trifinite_suff_lds.html

- forgalomelemzés: a támadó az eszközök közötti adatforgalom monitorozásával megfigyeli a kommunikáció mintázatait, ezzel információhoz jutva a résztvevő felekről. Ez a támadás sokkal kifinomultabb, mint a lehallgatás.

Aktív támadások esetén a támadó nem csak megfigyeli az adatforgalmat, de azon módosításokat is végezhet, illetve befolyásolhatja a hálózat működését is. Ezeket a támadásokat általában fel lehet ismerni, viszont ez nem jelenti azt, hogy minden esetben kivédhetőek. Az aktív támadások a következő négy fő kategóriába - vagy ezek valamilyen kombinációjába - sorolhatóak:

- megszemélyesítés: a támadó egy, a hálózatot használni jogosult személy nevében fér hozzá ahhoz. (Például annak azonosítóit felhasználva.)
- visszajátszás: a támadó rögzíti a hálózati adatforgalmat és később újraküldi azt, ezzel legitim felhasználói kommunikációt imitálva.
- üzenetmódosítás: a támadó az adatforgalomból elkapott üzeneteket módosítja a céljainak megfelelően.
- szolgáltatás-megtagadás: a támadó megpróbálja lehetetlenné tenni a hálózaton belüli rendes kommunikációt, illetve elérhetetlenné tenni azt.

A vezeték nélküli hálózatokat is hatósugaruk szerint szokás leggyakrabban osztályozni. Ezen osztályozás szerint léteznek vezeték nélküli nagy kiterjedésű, lokális, személyi és testfelszíni hálózatok. Ezek közül az első fejezetben a vezeték nélküli lokális a második fejezetben pedig a vezeték nélküli személyi hálózatok biztonsági kérdései, legelterjedtebb szabványai és az azok által nyújtott biztonsági funkciók kerülnek tárgyalásra, a következő szempontok szerint:

- bizalmasság: annak biztosítása, hogy a kommunikáció során küldött adatokhoz illetéktelen személyek ne férhessenek hozzá.
- adatintegritás: az átvitt adatokban bekövetkezett szándékos vagy véletlen változások észlelése.
- rendelkezésre állás: a vezeték nélküli hálózat és a hálózati erőforrások elérhetőségének biztosítása.

1. Vezeték nélküli lokális hálózatok (WLAN)

1.1. Bevezetés

A vezeték nélküli lokális hálózat (Wireless Local Area Network, WLAN) hálózati csomópontok egy olyan csoportja, amely egy meghatározott földrajzi területen - például egy épületen belül – helyezkedik el és képes a rádiófrekvenciás kommunikációra. A WLAN-ok leggyakrabban egy már meglévő vezetékes helyi hálózatot egészítenek ki, lehetővé téve a felhasználók számára a mobilitást és az egyszerű hálózati hozzáférést.

Az IEEE 802.11 az uralkodó WLAN szabvány, de több másik is létezik. Ezek közül a legjelentősebb az ETSI által fejlesztett High Performance Radio Local Area Network (HIPERLAN), de a 802.11 térnyerésével ez mára már szinte teljesen kiszorult a kereskedelmi eszközök piacáról.

1.2. Az IEEE 802.11 szabványcsalád

Az IEEE 802 LAN/MAN Standards Committee 1990-ben indította el a 802.11 projektet azzal a céllal, hogy kifejlesszen egy olyan közeghozzáférés-vezérlési (Medium Access Control, MAC) és fizikai réteg (Physical Layer, PHY) specifikációt, ami lehetővé teszi helyhez kötött, hordozható és mozgó hálózati csomópontok vezeték nélküli összekapcsolását egy adott területen belül.

1.2.1. IEEE 802.11-1997

A 802.11 szabvány első változatát 1997-ben hagyta jóvá az IEEE. Ez két adatátviteli sebességet (1 és 2 Mbit/s) támogat és előremutató hibajavítást (FEC) alkalmaz. Három alternatív fizikai réteget definiáltak benne: diffúz infravörös fényen valamint frekvenciaugrásos szórt spektrumú (FHSS) és közvetlen sorozatú szórt spektrumú (DSSS) modulációt alkalmazó rádiós átvitelen alapulókat. A két utóbbi a 2,4 GHz-es Industrial, Scientific and Medical (ISM) frekvenciasávban működik.
1999-ben az IEEE két kiegészítéssel bővítette a szabványt: a 802.11a és a 802.11b új átviteli módszereket és modulációs technológiákat definiáltak

1.2.2. IEEE 802.11a

A 802.11a kiegészítés ugyanazt az adatkapcsolati réteg és keretformátum definíciókat tartalmazza, mint az eredeti szabvány, de ortogonális frekvenciaosztásos multiplexelést (OFDM) alkalmaz. A 802.11a az 5 GHz-es Unlicensed National Information Infrastructure (UNII) frekvenciasávban működik és 54 Mbit/s adatátviteli sebességet tesz lehetővé. Előnye, hogy ebben a frekvenciasávban az interferencia lehetősége sokkal kisebb, mint az ISM sávban, viszont így az elérhető maximális hatótávolság is alacsonyabb.

1.2.3. IEEE 802.11b

A 802.11b kiegészítést úgy tervezték, hogy a 2,4 GHz-es ISM frekvenciasávban működve a vezetékes helyi hálózatokkal összemérhető teljesítményt lehessen vele elérni, ennek köszönhetően gyorsan a legelterjedtebb vezeték nélküli szabvánnyá vált. A 802.11b ugyanazt a közeghozzáférés-vezérlés specifikációt tartalmazza, mint ami az eredeti szabványban került definiálásra. A 802.11b eszközök már 11 Mbit/s adatátviteli sebességet támogatnak.

1.2.4. IEEE 802.11g

A 802.11g kiegészítés 2003 közepén jelent meg. Ez is a 2,4 GHz-es frekvenciasávban működik, de a 802.11a ortogonális frekvenciaosztásos multiplexelését alkalmazza. Az adatátviteli sebessége legfeljebb 54 Mbit/s, ami lépésekben csökkenthető, ha szükséges. A szabvány úgy lett megtervezve, hogy visszafelé kompatibilis legyen az addigra már igen elterjedt 802.11b eszközökkel, de fontos megjegyezni, hogy a régebbi eszközökkel való kommunikáció rontja az egész hálózat teljesítményét.

1.2.5. IEEE 802.11-2007

Az IEEE TGma munkacsoportja 2003-ban kezdte el az 1999-es szabvány és annak nyolc kiegészítésének (IEEE 802.11a, b, d, e, g, h, i és j) összefésülését. Az eredményként előállt 802.11ma dokumentumot 2007 márciusában 802.11-2007 néven publikáltak szabványként.

1.2.6. IEEE 802.11n

2009 októberében került elfogadásra a 802.11n, a szabvány legfrissebb kiegészítéseként. Első vázlata 2006-ban jelent meg azzal a céllal, hogy növelje a WLAN-ok hatósugarát és átviteli sebességét, aminek érdekében számos új megoldás került bele. Többek között a MIMO (multiple input – multiple output) támogatása, ami azt jelenti, hogy az eszköz több antennát használ adatátvitelre, így képes egy időben akár három csatornán adni és kettőn fogadni adatokat, ezzel 600 Mbit/s-ig növelve az elméleti maximális adatátviteli sebességet. A másik jelentős újítás a payload-optimalizálás, ami lehetővé teszi ugyanannyi adat átvitelét kevesebb keret segítségével. Az IEEE 802.11n kiegészítés is visszafelé kompatibilis a korábbi eszközökkel.

A vezeték nélküli hálózatok adatátviteli sebességének növelésének fokozott igénye miatt a Wi-Fi Alliance már 2007-től ad ki ún. „draft-n” minősítést a kiegészítés aktuális vázlatainak megfelelő eszközök számára. Az így minősített eszközök a legtöbb esetben kompatibilisek, vagy szoftverfrissítéssel azzá tehetők a végleges 802.11n kiegészítéssel.

1.2.7. Az IEEE 802.11 hálózati komponensei és logikai szervezési módjai

Az IEEE 802.11 szabvány a következő két alapvető hálózati komponenst definiálja:

- **Állomás (Station, STA):** egy vezeték nélküli végpont, hálózati interfész.

- **Hozzáférési pont (Access Point, AP):** olyan eszköz, amely az állomásokat logikailag összekapcsolja egymással vagy egy másik, vezetékes vagy vezeték nélküli elosztó hálózattal.

A szabvány két lehetséges logikai szervezési módot tartalmaz: ad hoc mód és infrastrukturális mód.

1.2.7.1. Ad hoc mód

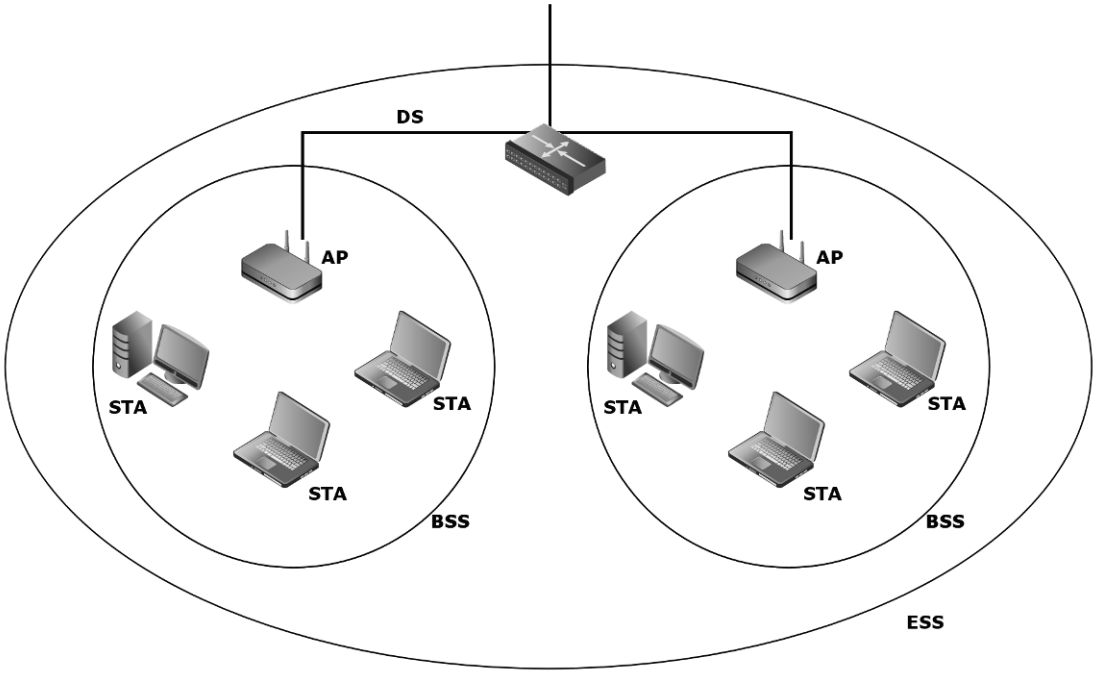
Ebben az esetben nincs szükség hozzáférési pontra, az állomások közvetlenül kommunikálnak egymással. Ez a szervezési mód akkor lehetséges, ha kettő vagy több, egymás hatósugarán belül tartózkodó állomás képes egymással közvetlenül kommunikálni. Az állomások egy ad hoc módon szervezett halmazát nevezzük független alapszolgáltatás készletnek (Independent Basic Service Set, IBSS). Az IBSS alapvető tulajdonsága, hogy nem biztosít forgalomirányítást és csomagtovábbítást, így bármely két kommunikáló eszköznek egymás hatósugarán belül kell lennie.

Az ad hoc hálózatok egyik legfőbb előnye hogy elvileg bárhol könnyen kialakíthatóak, lehetővé téve állomások gyors összekapcsolását, minimális hardverigénnyel. Az ad hoc módon szervezett hálózatok jellemzően néhány számítógép ideiglenes összekapcsolására használják, de számos más felhasználása is lehetséges, mint pl. PDA-k, mobiltelefonok szinkronizálása, fényképezőgépek összekapcsolása nyomtatókkal stb.

1.2.7.2. Infrastrukturális mód

Infrastrukturális mód esetén a WLAN egy vagy több alapszolgáltatás készletből (Basic Service Set, BSS) áll. A BSS egy hozzáférési pontot és egy vagy több állomást tartalmaz. A BSS-ben az állomások a hozzáférési ponton keresztül kommunikálnak egymással és csatlakoznak az elosztó hálózathoz (Distribution System, DS). Az állomások a DS-en keresztül tudnak kapcsolódni más helyi hálózatokhoz, illetve tudnak hozzáférni külső erőforrásokhoz, mint pl. az Internet.

A DS és több BSS alkalmazásával lehetséges tetszőleges méretű és komplexitású vezeték nélküli hálózat létrehozása. Az IEEE 802.11 szabványban a DS-ből és a BSS-ekből összeálló hálózatot kiterjesztett szolgáltatáskészletnek (Extended Service Set, ESS) nevezik.



1.1. ábra: infrastrukturális szervezési mód

1.3. Az IEEE 802.11-1997 szabvány biztonsága

Az IEEE 802.11-1997 szabvány több eszközt tartalmazott arra, hogy a vezetékes hálózatok titkosítás nélkül történő kommunikációval összemérhető biztonsági szintet nyújtson. Ezen funkciókat nagyrészt a Wired Equivalent Privacy (WEP) protokoll biztosította, azonban ennek hamarosan számos biztonsági hiányosságra derült fény. 2001-ben Fluhrer, Mantin és Shamir publikálta a WEP által használt RC4 folyamtitkosító kriptoanalízisét, aminek eredményeként ma már automatikus eszközökkel néhány perc alatt feltörhetőek a WEP-et használó vezeték nélküli hálózatok[2].

Néhány hónappal később az IEEE létrehozta a 802.11i munkacsoportot a WEP problémáinak megoldására. A 802.11i kiegészítés 2004-ben került elfogadásra.

[2] Stubblefield, Ioannidis és Rubin: „*Using the Fluhrer, Mantin and Shamir Attack to Break The WEP"* (2001, Rice University, forrás: http://www.isoc.org/isoc/conferences/ndss/02/papers/stubbl.pdf)
Fluhrer, Martin és Shamir: „*Weaknesses in the Key Scheduling Algorithm of RC4"* (2000, Berkeley University, forrás: http://www.math.psu.edu/mathnet/mdoc/md15/rc4_ksaproc-1.pdf)

Ismert gyengeségei ellenére a WEP máig széles körben használt. Számos gyártó próbálta a WEP biztonsági hiányosságait javítani a saját eszközeiben, de e törekvések gyakran oda vezettek, hogy a különböző gyártóktól származó eszközök nem voltak képesek egymással kommunikálni. Ezen felül számos korai eszközben a biztonsági funkciók alapértelmezés szerint le is voltak tiltva, mivel a szabvány nem tette kötelezővé azok használatát. Ebben a fejezetben a szabvány 802.11i előtti biztonsági megoldásai kerülnek részletezésre, annak érdekében, hogy az RSN létrehozásának motivációi világosak legyenek.

1.3.1. Hozzáférés szabályozás és hitelesítés

Az IEEE 802.11 szabvány első változata két módszert definiál a vezeték nélküli hálózathoz csatlakozni kívánó eszközök hitelesítésére. E két módszer a nyílt hitelesítés (Open System Authentication), amit minden implementációnak támogatnia kell és az osztott kulcsú hitelesítés (Shared Key Authentication), amelynek támogatása opcionális.
Egy ESS-ben minden állomásnak hitelesítenie kell magát az AP felé, viszont egy IBSS-ben az állomások közötti hitelesítés opcionális.

1.3.1.1. Nyílt hitelesítés (Open System Authentication)

A nyílt hitelesítés egy null-hitelesítési mechanizmus, azaz nem szolgáltat valódi identitás ellenőrzést.
Ennél a módszernél az állomásokat az AP csak a következő adatokat felhasználásával hitelesíti:

- **Service State Identifier (SSID):** az SSID az adott WLAN neve, ez teszi lehetővé az állomások számára a hálózat azonosítását. Az SSID nyílt szövegként kerül továbbításra a vezeték nélküli kommunikáció során, tehát egy lehallgató könnyen megtudhatja azt. Mindezek mellett az SSID nem egy hozzáférés szabályozási eszköz, és nem is szánták annak.
- **Az állomás fizikai címe (Media Access Control, MAC):** a MAC cím egy egyedi, 48 bites azonosító, amely egy konkrét hálózati interfészhez van hozzárendelve. Számos implementáció lehetővé teszi a hitelesített eszközök fizikai címének adminisztrálást, így később az AP csak a jogosult eszközöket engedi csatlakozni. Ezt nevezik fizikai cím szűrésnek is.

Az állomások MAC címe az adatcsomagok titkosítatlan fejrészében szerepel, ezért a forgalom figyelésével könnyen meg lehet szerezni azokat. Mivel majdnem minden hálózati interfész lehetővé tesz a fizikai cím megváltoztatását, ezért ez egy könnyen kivitelezhető támadás.

A nyílt hitelesítés használata esetén nincs lehetőség az AP hitelesítésére, ezért az állomásoknak meg kell bízniuk abban, hogy valóban ahhoz az AP-hoz akartak csatlakozni.

1.3.1.2. Osztott kulcsú hitelesítés (Shared Key Authentication)

Az osztott kulcsú hitelesítési módszer egy egyoldalú kihívás-válasz protokollon alapul, amely során az AP azt ellenőrzi, hogy a csatlakozni kívánó állomás ismeri-e a titkos kulcsot.

A hitelesítés menete a következő:

1. Az állomás elküld egy hitelesítési kérelmet az AP felé.
2. Az AP generál egy 128 bites kihívás értéket, amit visszaküld az állomásnak.
3. Az állomás az előre kiosztott WEP kulcs felhasználásával titkosítja az értéket és visszaküldi az AP-nak.
4. Az AP dekódolja a kapott választ a WEP kulccsal és megnézi, hogy az általa elküldött kihívás értéket kapta-e vissza. Ha a két érték megegyezik, az állomás hitelesítésre került.

Az állomás a WEP titkosítást használja arra, hogy a választ kiszámítsa, ami ez esetben nem más, mint a kihívásként kapott érték és az RC4 folyamtitkosító által generált pszeudovéletlen kulcs összekapcsolása XOR művelettel. Ez a hitelesítési módszer sérülékeny, hiszen a támadó egyszerűen visszakaphatja a titkosító kulcsot a kihíváson és a válaszon elvégzett XOR művelettel. Ezt a kulcsot később felhasználhatja arra, hogy saját eszközeit hitelesítse.

Egy másik jelentős probléma az osztott kulcsú hitelesítéssel, hogy az összes hálózati csomópont ugyanazt a kulcsot (vagy ugyanazt a néhány kulcsot) használja a hitelesítéshez.

Ez azt a veszélyt rejti magában, hogy ha nyilvánosságra kerül a hitelesítéshez használt WEP kulcs, akkor azt minden eszközön azonnal ki kell cserélni a későbbi támadások kivédésére, hiszen ezt nem csak hitelesítéshez használják, de ezen alapul a titkosítás és az adatintegritás ellenőrzés is. Az eredeti IEEE 802.11 szabvány nem ad semmilyen ajánlást a kulcskezelésre, ezért a hálózatok adminisztrátorainak maguknak kell megoldaniuk a kulcs generálását és kiosztását. A kulcs kezelésének problémái így határt szabhatnak a WLAN-ok méretének.

Az osztott kulcsú hitelesítés esetén a gyenge WEP kulcsok alkalmazása is okozhatja a hitelesítés gyengeségét. Például a csupa nulla, 12345678 vagy egyéb triviális kulcsok

alkalmazása elősegíti a szótár támadások végrehajtását. A kulcsnak ideális esetben véletlenszerűen generáltnak kellene lennie és rendszeresen kellene cserélni a támadás e formájának megelőzésére.

Az osztott kulcsú hitelesítést úgy tervezték, hogy a nyílt hitelesítéstől robosztusabb legyen, de ez sem nyújt nagyobb biztonságot. E módszer esetén is probléma, hogy az AP nem kerül hitelesítésre, emellett támadható man-in-the-middle és szótár támadásokkal, viszont a kihívás üzenetek megakadályozhatják a visszajátszásos támadásokat.

Az osztott kulcsú hitelesítést már csak a 802.11i kiegészítést nem támogató eszközökkel való lefelé kompatibilitásért szükséges implementálni.

1.3.2. Titkosítás

A WEP az RC4 folyamtitkosítót használja a titkosításhoz. A szabvány 40 bites WEP kulcsot definiál (WEP-40), ami egy 24 bites inicializáló vektorral (initialization vector, IV) konkatenálva alkotja az RC4 64 bites[3] tikosító kulcsát, de léteznek olyan változatok, amelyek ettől hosszabb, 104 bites WEP kulcshossz használatát is lehetővé teszik (lásd később). Elméletileg, a hosszabb kulcsok alkalmazása növeli a biztonságot, de a WEP egyéb ismert hiányosságai miatt nem jelentős mértékben.

Az inicializáló vektort az RC4 kulcsfolyam inicializálásához kerül felhasználásra, ezzel megelőzve annak ismétlődését, de mivel összesen 2^{24}-en IV értéket lehet generálni, ezért ezek egy forgalmas WLAN-on hamar elfogyhatnak. Emellett, még ha az inicializáló vektorokat teljesen véletlenszerűen választjuk is ki, a születésnap paradoxon miatt 2^{12} keret titkosítása után 50%-os eséllyel fordul elő ugyan az a IV érték.

A WEP elleni legtöbb támadás is az inicializáló vektorral kapcsolatos. Az RC4 tikosító kulcs IV része nyílt szövegként kerül továbbításra, ami az IV hosszával és a gyenge RC4 implementációval együtt lehetővé teszi a támadók számára, hogy viszonylag kevés hálózati adatforgalom monitorozásával és elemzésével megszerezze a WEP kulcsot.

Továbbá, a WEP nem definiálja pontosan, hogy hogyan kell az IV-t generálni és milyen gyakran kell cserélni azt, ezért néhány eszköz statikus (és így jól ismert) értékeket alkalmaz.

[3] Amikor az IEEE 802.11 szabvány első változata megjelent az Egyesült Államok kereskedelmi eszközök kriptográfiai jellemzőire vonatkozó törvényi szabályozása nem tette lehetővé erősebb titkosítás alkalmazását.

Ha két üzenetet ugyan azzal az IV-vel generált titkosító kulccsal kerül titkosításra, és rendelkezésre áll az egyik üzenet nyílt szövegként és titkosítva is, akkor viszonylag egyszerű a másik üzenet visszafejtése. Ilyen szöveget nem nehéz találni, legegyszerűbb valamilyen hálózati protokollra jellemző adatot felhasználni.

1.3.2.1. WEP2 (Wired Equivalent Privacy 2, WEP-104)

A WEP2 a WEP ideiglenes továbbfejlesztéseként került bele az IEEE 802.11i szabvány korai vázlataiba, mivel a WEP-et támogató eszközök nagy részén lehet implementálni egy firmware frissítéssel. A tikosító kulcs hosszát 128 bitre növelték (104 bites kulcs egy 24 bites inicializáló vektorral konkatenálva), annak reményében, hogy ezzel csökkenteni lehet a brute force támadások esélyét.

1.3.2.2. WEPplus

A WEPplus (vagy más néven WEP+) az Agere Systems által szabadalmaztatott WEP javítás, ami a tikosítás erősségét az inicializáló vektorral kapcsolatos változtatásokkal próbálja javítani, de csak akkor hatékony, ha mindkét kommunikáló eszköz támogatja azt.

1.3.2.3. Dinamikus WEP

Ez esetben a kulcsok dinamikus cseréjével próbálják a protokollt javítani. A dinamikus WEP-et gyártó-specifikusan implementálták (pl. a 3Com) így általában csak ugyanazon gyártó termékei tudtak ezt felhasználva kommunikálni.
A dinamikus kulcscsere ötletét beépítették a 802.11i szabványba a TKIP (lásd később) részeként.

1.3.3. Adatintegritás ellenőrzés

A WEP adatintegritás ellenőrzést végez minden fogadott keretre. Az adatintegritás ellenőrzése egy titkosított ellenőrzőösszegen alapul, amelyet a keret payload része felett a CRC-32 (Cyclic Redundancy Check 32 bit) algoritmussal kiszámított érték RC4 folyamtitkosítóval történő titkosításával állítanak elő. Ezt nevezik ICV-nek (Integrity Check Value). Az ellenőrzéshez az eszköz dekódolja a fogadott keretet és újra kiszámítja az ellenőrzőösszeget. Ha az így kapott érték nem egyezik meg az elküldöttel, akkor az eszköz a keretet érvénytelennek tekint.

A CRC-32 érzékeny a bitcserén alapuló támadásokra, mivel a támadó meg tudja határozni, hogy az ellenőrzőösszeg mely bitjei fognak megváltozni, ha az üzenetet megváltoztatják.
A WEP-ben ez ellen a CRC-32 által előállított érték titkosításával próbálnak védekezni, de az alkalmazott folyamtitkosító RC4 algoritmus egyik tulajdonsága, hogy bitcsere esetén a tikosítás során előállt értékben is ugyan az a bit cserélődik fel, tehát ez a biztonságot nem növeli.
A CRC-32 nagyon hatékonyan számítható, de mivel véletlen bithibák kivédésére tervezték, ezért a szándékos módosításokat nem tudja jelezni.

1.3.4. Visszajátszás elleni védelem

Az IEEE 802.11 szabvány nem definiál semmilyen eszközt a visszajátszásos támadások ellen, mivel a kereteken nincs időbélyeg, nem alkalmaznak inkrementális számlálót, vagy más, ideiglenes adatot, ami lehetetlenné tenné ezt.

1.3.5. Rendelkezésre állás

A szolgáltatásmegtagadási támadások (Denial of Service, DoS) ellen minden rádiófrekvenciás kommunikáció esetén nehéz védekezni. Az IEEE 802.11 szabvány jelenleg nem nyújt eszközöket az ilyen támadások ellen. A vezeték nélküli hálózatok elleni szolgáltatásmegtagadási támadások közül a legjelentősebbek a frekvenciazavarás és az elárasztás.

- **Frekvenciazavarás (frequency jamming):** Ennek végrehajtásához egy olyan eszköz szükséges, ami a WLAN által használt frekvenciasávban sugároz elektromágneses jeleket, ezzel használhatatlanná téve azt.
- **Elárasztás (flooding):** A másik lehetőség az elárasztás, ami nagy mennyiségű üzenet küldését jelenti az AP felé, olyan intenzitással, hogy az ne legyen képes azt feldolgozni, ezzel részben vagy teljesen lehetetlenné téve a kommunikációt, illetve ez alatt egy másik állomás nem lesz képes az adott csatornát használni.

  Ezzel párhuzamosan a támadók elhelyezhetnek egy hamis AP-t is (úgy nevezett rogue AP-t), amivel elhitethetik az állomássokkal, hogy a legitim AP-hez csatlakoznak. Ez ellen nyújt bizonyos védelmet a szabvány 802.11w kiegészítése a hitelesítési és asszociációs keretek védelmével.

1.4. Robust Security Network (RSN)

Az IEEE 802.11i kiegészítés vezeti be a Robust Security Network (RSN) és a Robust Security Network Association (RSNA) fogalmát.
A kiegészítés az RSN-t olyan vezeték nélküli lokális hálózatként definiálja, amely csak RSNA alapú kapcsolatok létrehozását engedélyezi. Az RSNA egy olyan biztonsági összerendelés két hálózati entitás között, amely az IEEE 802.11i négyutas kézfogási protokollját felhasználva jön létre (lásd később, 1.5.2.3.1). A négyutas kézfogás során ellenőrzésre kerül, hogy rendelkezik-e a protokollban résztvevő mindkét fél a páronkénti mester kulccsal (Pairwise Master Key, PMK) valamint szinkronizálásra kerülnek az ideiglenes kulcsok. Ezek mellett a kiegészítésben definiálásra kerül egy új hálózati komponens, a hitelesítő szerver (Authentication Server, AS) fogalma is.
A 802.11i kiegészítés lehetővé teszi olyan vezeték nélküli lokális hálózatok kiépítését is, amelyek megengedik az RSNA mellett a WEP alapú kapcsolatok létrehozását is, azzal a céllal, hogy az RSN-re való áttérését elősegítse. Ezeket a hálózatokat Transient Security Network-nek (TSN) nevezik.

1.4.1. Az RSN jellemzői

Az IEEE 802.11-2007 szabványban definiált biztonsági funkciókat két fő csoportra lehet osztani. Az egyik csoportba az eredeti IEEE 802.11 szabványban definiált nyílt és osztott kulcsú hitelesítés és a WEP tartozik, a másik pedig a 802.11i kiegészítésben definiált RSN-ek létrehozásához szükséges biztonsági mechanizmusokat tartalmazza.
Fontos megjegyezni, hogy az RSN csak az adatkapcsolati réteg szintjén és csak a hozzáférési pont és az állomások között (illetve ad hoc szervezési mód esetén két állomás között) biztosítja a kommunikáció védelmét, a hálózat többi részén, például a DS-en, már nem.

Az RSN a következő biztonsági funkciók használatát teszi lehetővé a WLAN-okban:

- fejlett felhasználó-hitelesítési mechanizmusok
- kulcs menedzsment
- titkosítás
- az adatok forrásának hitelesítése és az adatintegritás ellenőrzése
- visszajátszás elleni védelem

1.4.2. Kulcs hierarchiák és kulcs menedzsment

Az RSN számos kriptográfiai kulcsot alkalmaz a kulcsgenerálási, titkosítási, hitelesítési és az adatintegritás védelmi funkciók működtetéséhez, amelyek két kulcshierarchiát alkotnak: a páronkénti kulcs hierarchiát a unicast adatforgalom védelmére és a csoportszintű kulcs hierarchiát a broadcast és multicast adatforgalom védelmére.

1.4.2.1. Páronkénti kulcs hierarchia

A páronkénti kulcs hierarchia gyökerében egy előre kiosztott kulcs (Pre-shared Key, PSK) vagy egy Authentication, Authorization and Accounting (AAA) kulcs áll, amelyből majd a későbbi kommunikáció során használt többi kulcs kerül származtatásra.
E két kulcs egyikéből (az ún. gyökérkulcsból) kerül előállításra a páronkénti mester kulcs. A PMK-ból, az állomás fizikai címéből és egy, az AP által generált véletlen számból kerül előállításra a páronkénti átmeneti kulcs (Pairwise Transient Key, PTK).

- **Előre kiosztott kulcs (PSK):** egy statikus kulcs, ami az AS és az állomások számára a hálózati kommunikációtól különböző módon kerül kiosztásra. A szabvány nem tartalmazza, hogy ezeket a kulcsokat hogyan kell generálni és kiosztani, ezért ezeket a kérdéseket a hálózat implementálása során kell megoldani.

  Az előre kiosztott kulcsok használata során két fő probléma merülhet fel. Az egyik az, hogy már egyetlen nem megfelelő erősségű kulcs alkalmazása is az egész RSN biztonságát veszélyeztetheti, a másik pedig az, hogy a kulcsok menedzsmentje nagyméretű hálózatok esetén nehézkesen oldható meg.
- **Authentication, Authorization and Accounting (AAA) kulcs:** vagy más néven Master Session Key (MSK), ami az Extensible Authentication Protocol (EAP) (lásd később) segítségével kerül elhelyezésre az AP-n az RSNA kiépítése során. Ahányszor egy állomás újra hitelesíti magát a hálózaton, a hozzá tartozó AAA kulcs annyiszor cserélődik le.

1.4.2.2. Csoportszintű kulcs hierarchia

Ez az IEEE 802.11i által definiált második kulcs hierarchia. Ez egyetlen kulcsból áll, amelyet csoportszintű átmeneti kulcsnak (Group Temporal Key, GTK) neveznek. A GTK-t a hozzáférési pont generálja és küldi el az állomások számára. A GTK generálásának pontos módszerét sem definiálja a szabvány, így az az AP implementációjától függ.

A GTK hossza attól függ, hogy milyen protokollal kerül majd felhasználásra. TKIP-vel történő felhasználás esetén a GTK 256 bit, CCMP-vel 128 bit, WEP-pel pedig 40 vagy 104 bit hosszúságú.

1.4.3. Az RSN titkosítási és adatintegritás ellenőrzési protokolljai

A 802.11i kiegészítés két titkosítási és adatintegritás ellenőrzési protokollt definiál: Temporal Key Integrity Protocol (TKIP) és Counter Mode with Cipher Block Chaining MAC Protocol (CCMP).
Minden RSNA képes eszköznek támogatnia kell a CCMP-t, míg a TKIP támogatása csak opcionális.

1.4.3.1. Temporal Key Integrity Protocol (TKIP)

A TKIP létrehozásának célja az volt, hogy a már meglévő hálózati eszközök lecserélése nélkül is lehetőség legyen az eredeti szabványban definiáltnál erősebb biztonsági funkcionalitás megvalósítására, mivel a WEP képes eszközöket a firmware és az illesztőprogramok frissítésével képessé lehet tenni a TKIP használatára is. Azonban, mivel a TKIP az ismert gyengeségekkel rendelkező RC4 és Michael MIC algoritmusokat használja, ezért fokozott biztonsági szintet igénylő környezetekben való használatra nem alkalmas.
A TKIP a következő alapvető biztonsági funkcionalitásokat nyújtja:

- Titkosítás az RC4 folyamtitkosító algoritmus felhasználásával. Mivel minden keret titkosítása új kulccsal történik, így a Fluhrer-Mantin-Shamir támadás ellen is képes védelmet nyújtani.
- Adtaintegritás védelem, többek között a bitcserén alapuló támadások és a megszemélyesítéses támadások ellen
- Aktív támadások észlelése a Michael MIC algoritmus felhasználásával
- Visszajátszás elleni védelem

1.4.3.2. Counter Mode with Cipher Block Chaining MAC Protocol (CCMP)

A CCMP a másik titkosítási és adatintegritás ellenőrzési protokoll amelyet az RSNA létrehozásakor választani lehet. A CCMP tervezésekor annak hosszú távú használhatósága volt a legfőbb szempont, így már nem volt követelmény a korábbi eszközökkel való kompatibilitás.

A CCMP az AES blokktitkosító CCM működési módján alapul. A CCM működési mód általánosan definiált minden 128 bites blokkmérettel működő titkosító algoritmus számára. A CCM két jól ismert és ellenőrzött technikát használ: CTR-t a tikosításhoz és Cipher Block Chaining MAC (CBC-MAC) az üzenet forrásának hitelesítésére és az adatintegritás védelmére. A CCMP nem csak a keret payload részét védi, hanem a keret fejlécének bizonyos részeit is. A csatorna védelméhez a CCMP egy 128 bites titkosító kulcsot alkalmaz.

A CCMP-t a következő követelményeknek való megfelelést szem előtt tartva tervezték:

- Ugyanaz a kulcs kerüljön felhasználásra a titkosításhoz és az adatintegritás ellenőrzéshez is, ezzel egyszerűsítse a protokollt és növelve a teljesítményt.
- Az adatintegritás ellenőrzés a keret payload és fejléc részét is védje, növelve ezzel az átvitt adatok megbízhatóságát.
- Egy keret fogadásakor képes legyen elvégezni azokat a kriptográfiai számításokat, amelyekhez nem szükséges a teljes keret beolvasása.
- A biztonsági funkciókkal kapcsolatos adatok mérete legyen minimális.

	WEP	TKIP	CCMP
Kriptográfiai algoritmusok alapja	RC4	RC4	AES
Kulcsméretek	40 vagy 104 bit (titkosítás)	128 bit (titkosítás) 64 bit (adatintegritás ellenőrzés)	128 bit (titkosítás és adatintegritás ellenőrzés)
Keretenkénti titkosító kulcs	A WEP kulcs és a 24 bites IV konkatenálásával generálódik	A TKIP generálja	Nincs rá szükség, az ideiglenes kulcs elegendő
Adatintegritás ellenőrzési mechanizmus	Titkosított CRC-32	Michael MIC	CCM
Fejléc védelem	Nincs	A forrás és a cél cím védelme; Michael MIC	A forrás és a cél cím védelme; CCM
Visszajátszás elleni védelem	Nincs	IV sorozat	IV sorozat
Kulcs kiosztás	Manuális	IEEE 802.1X vagy manuális	IEEE 802.1X vagy manuális
Hitelesítés	Nyílt hitelesítés vagy osztott kulcsú hitelesítés	IEEE 802.1X vagy PSK	IEEE 802.1X vagy PSK

1.2. táblázat: A 802.11 biztonsága

1.5. Az IEEE 802.11i RSN működési alapelvei

1.5.1. A 802.11 kerettípusai

Az IEEE 802.11 szabvány a következő három kerettípust definiálja:

- **adat keretek:** a magasabb szinten elhelyezkedő protokollok (pl. IP) csomagjainak beágyazással történő átvitelére szolgálnak. Az RSNA biztonsági funkciói védelmet nyújtanak az adat keretek számára.
- **menedzsment keretek:** a MAC menedzsmentjéhez szükséges információk cseréjére szolgálnak (pl. hitelesítési keretek). Ezek a keretek nem kerülnek továbbításra felsőbb rétegek felé. A menedzsment kereteket viszonylag könnyen lehetett hamísítani, mivel a 2009 szeptemberében elfogadott 802.11w kiegészítés előtt a szabvány nem tartalmazott semmilyen mechanizmust ezek védelmére.
- **vezérlő keretek:** a vezeték nélküli közeghez való hozzáférés szabályozására szolgálnak. Ilyen például a nyugtázó keret, amely minden adat keret fogadása után elküldésre kerül, jelezve, hogy az sikeresen megérkezett és nincs szükség újraküldésre. Jelenleg a vezérlő keretek védelmét nem biztosítja a szabvány.

1.5.2. A 802.11i RSN működési fázisai

A 802.11 hálózatok működése öt önálló fázisra osztható.

1.5.2.1. Első fázis: felderítés

Első lépésként az állomás megpróbálja azonosítani azt a hozzáférési pontot, amely ahhoz a vezeték nélküli hálózathoz tartozik, amihez csatlakozni szeretne. Az azonosítás történhet passzívan, a hozzáférési pont által periodikusan elküldött *beacon* keretek figyelésével, amelyek szinkronizációs információkat tartalmaznak, illetve aktívan, az állomás által küldött *probe request* keretekre kapott válaszok alapján.

A sikeres azonosítást követően az állomás és a hozzáférési pont egyeztetésbe kezd, amelynek során megállapodnak a hitelesítéshez használt metódusban és a kulcskiosztási módszerben, illetve a későbbi kommunikáció során alkalmazott titkosítási és adatintegritás védelemi algoritmusokban.

1.5.2.2. Második fázis: hitelesítés

Ezen fázis során az állomás és az AS bizonyítják egymásnak az identitásukat. A hozzáférési pont ebben a fázisban az állomás által küldött keretek közül csak a hitelesítési kereteket engedi át, az IEEE 802.1X szabványt alkalmazva. Az állomás és az AS az EAP keretrendszert (lásd később) használja a hitelesítéshez, ami lehetővé teszi többek között statikus és dinamikus jelszavak, tanúsítványok és tokenek használatát is.
A hitelesítés befejezése után mindkét fél rendelkezik az AAA kulccsal, aminek felhasználásával kerül majd előállításra a kommunikáció során használt többi kulcs (pl. a titkosító kulcs).

1.5.2.3. Harmadik fázis: kulcsgenerálás és kiosztás (Key Generation and Distribution, KGD)

E fázis során az állomás és az AP közösen előállítják a kommunikáció során használt többi kulcsot. A kulcsok generálása két kézfogási protokoll felhasználásával történik: négyutas kézfogás és csoportkulcs-kézfogás.

1.5.2.3.1. Négyutas kézfogás

A KGD fázis egy négyutas kézfogással kezdődik, amelynek során négy EAP keret (lásd később) kerül átvitelre az állomás és a hozzáférési pont között:

1. Az AP elküld egy értéket az STA-nak, amely ebből és a korábban egyeztetett attribútumok felhasználásával előállítja a PTK-t.
2. Az STA is elküld egy értéket az AP-nek, egy üzenethitelesítő kóddal együtt (MIC).
3. Az AP válaszul elküldi a GTK-t, egy sorszámot (ami majd a következő broadcast vagy multicast keret sorszáma lesz), valamint a MIC-t. A sorszám a visszajátszás elleni védelemre szolgál.
4. Az STA nyugtázza a fogadott keretet.

A protokoll befejezése után mind az állomás mind a hozzáférési pont hitelesítettnek tekinthető és rendelkezik a szükséges kulcsokkal. Ezután az AP lehetővé teszi adat keretek átvitelét is az állomás számára.

1.5.2.3.2. Csoportkulcs-kézfogás

A csoportkulcs kézfogás arra szolgál, hogy a hozzáférési pont egy új GTK-t küldjön az állomások számára, például a konfiguráció változása esetén, illetve ha a biztonsági előírások szerint azt periodikusan frissíteni kell.

Mindkét kézfogási protokoll a következő két-két titkosítási és adatintegritás ellenőrzési algoritmus egyikét használja: AES Key Wrap és RC4, illetve HMAC-SHA-1-128 és HMAC-MD5

1.5.2.4. Negyedik fázis: biztonságos adatátvitel

Ebben a fázisban történik maga az adatátvitel a hozzáférési pont és az állomások között az előző fázisokban kialakított biztonsági szabályoknak megfelelően. Fontos megjegyezni, hogy a biztonságos adatátvitel csak a hozzáférési pont és az állomások között biztosított, a hálózat többi részén (pl. a DS-en) már nem.

1.5.2.5. Ötödik fázis: lebontás

A hozzáférési pont és az állomás közötti vezeték nélküli kapcsolat lebontása történik ebben a fázisban.

A 802.11i kiegészítésben definiált öt fázis közül csak az első és a negyedik volt része az eredeti szabványnak. Igaz, hogy kezdetleges hitelesítésre már abban is volt lehetőség, de csak a felderítési fázis részeként.
Azoknak a szervezeteknek, amelyek IEEE 802.11i RSN-eket akarnak kiépíteni, úgy kell konfigurálniuk a hozzáférési pontjaikat, hogy azok csak RSNA-k felépítését engedélyezze. Amennyiben a felderítési fázis során az AP lehetővé teszi WEP alapú kapcsolat kiépítését is, akkor nem csak az a kapcsolat nem lesz RSNA, de a teljes vezeték nélküli hálózat sem tekinthető RSN-nek, mivel a WEP alapú kapcsolatok jelentős biztonsági kockázatot jelentenek.

1.6. Extensible Authentication Protocol (EAP)

Az Extensible Authentication Protocol az RSN működésének hitelesítési fázisában kerül felhasználásra. Az EAP-t 1998 márciusában publikálták az RFC 2284-ben, de 2004

júniusában újrafogalmazták, mivel az eredeti dokumentum leginkább a csomagformátumra és az üzenettípusokra fókuszált. A javított RFC 3748 már számos új leírást tartalmaz az EAP keretrendszerről, a biztonsági megfontolásokról és a más protokollokkal való együttműködésről.

Az EAP-t arra fejlesztették ki, hogy a Pont-Pont Protokollhoz (Point-to-point Protocol, PPP) nyújtson hitelesítési szolgáltatásokat. Az EAP előtt a PPP a Password Authentication Protocol-t (PAP)[4] és a Challenge-Handshake Authentication Protocol-t (CHAP)[3] használták hitelesítéshez, de mivel egyre nagyobb igény merült fel arra, hogy más fajta hitelesítési metódusokat is alkalmazzanak (mint pl. a One Time Password (OTP)[5] vagy a token alapú hitelesítés), ezért szükségessé vált egy olyan protokoll megalkotása, ami ezen új igényeknek megfelel. Ennek eredményeként jött létre az EAP.

Az EAP számos hitelesítési metódust támogat: többek között jelszavakon, tanúsítványokon, tokeneken és smart kártyákon alapulókat, illetve ezek kombinációit, pl. tanúsítvány alapú és jelszavas hitelesítés. E flexibilitás miatt szinte bármilyen környezetbe integrálható, ahol WLAN-ok működhetnek.

Az IEEE 802.11i nem specifikálja az alkalmazandó hitelesítési metódust, ezzel lehetővé téve, hogy a szervezetek a számukra legmegfelelőbb hitelesítést tudják kiválasztani. A szabvány mindössze az EAP alapvető követelményeit tartalmazza, amik a biztonsági modell felállításához szükségesek. Viszont, ha a szervezet gyenge hitelesítést választ, vagy ha rosszul implementálja azt, akkor az alapvetően befolyásolja a hálózat biztonságát, illetve további problémákat is okozhat, amennyiben a hálózati hitelesítést más erőforrások hozzáférésének szabályozására is felhasználják.

1.6.1. EAP metódusok

Az EAP metódusok végzik a hitelesítési tranzakciót és annak a kulcsnak az előállítását, ami majd a későbbi kommunikáció védelmére kerül felhasználásra. Az EAP keretrendszerhez számos hitelesítési metódus létezik, amelyeket leggyakrabban IETF vázlatok vagy RFC dokumentumok formájában tesznek közzé, lehetővé téve a fejlesztők számára, hogy saját implementációikat elkészíthessék.

[4] RFC 1334: PPP Authentication Protocols, http://tools.ietf.org/html/rfc1334
[5] RFC 2289: A One-Time Password System, http://tools.ietf.org/html/rfc2289

A leggyakrabban használt EAP metódusokhoz az Internet Assigned Numbers Authority (IANA) rendel egy azonosítószámot és teszi közzé azokat az általánosan alkalmazható metódusok listáján[6]. Az EAP szoftver ezen azonosítószám alapján tudja meghatározni majd az alkalmazandó EAP metódust.

1.6.2. Követelmények az RSN-ben használt EAP metódusokkal szemben

Nem minden EAP metódus felel meg az IEEE 802.11i RSN-ekben való használatra. Az EAP metódusok által nyújtott biztonsági funkciók áttekinthetőségéért az RFC 3748 dokumentum tartalmazza azon biztonsági követelmények listáját, amelyek alapján egy EAP metódust értékelni lehet. Ezen dokumentum megjelenése óta minden új metódus deklarálásakor meg kell adni, hogy e listából mely követelményeknek felel meg.
Az RFC 4017 tartalmazza azon biztonsági követelmények listáját, amelyek az RSN-ekben használt EAP metódusok számára kötelezőek, ajánlottak és opcionálisak.

Kötelező

- **Kulcsszármaztatás:** a metódus legyen képes előállítani a későbbi kommunikáció védelmére használt gyökérkulcsot. Ez a legalapvetőbb kritérium, az ennek nem megfelelő metódusuk alkalmatlanok az EAP keretrendszerben történő felhasználásra.
- **Kulcserősség:** egy EAP metódus akkor felel meg az RSN-ben való használatra, ha az általa generált kulcs hossza legalább 128 bit.
- **Kölcsönös hitelesítés:** a metódus alkalmazásával legyen képes ugyanabban az EAP tranzakcióban az AS is hitelesíteni az állomást és az állomás is az AS-t. Két függetlenül indított egyoldalú hitelesítés együtt nem alkot kölcsönös hitelesítést.
- **Shared state equivalence:** ez azt jelenti, hogy a metódus alkalmazása során a hitelesítő és hitelesítendő félnek is rendelkeznie kell az összes állapotleíró attribútummal, többek között az alkalmazott EAP metódus azonosítószámával, a hitelesítéshez használt egyedi azonosítókkal és a többi, metódus specifikus attribútummal is. Továbbá mindkét félnek képesnek kell lennie több hitelesítési tranzakció kezelésére egyidejűleg.
- **Szótár támadások elleni védelem:** egy jelszó alapú EAP metódus akkor nyújt védelmet a szótár támadásokkal szemben, ha az nem teszi lehetővé a támadó számára az EAP tranzakció során küldött üzenetekből a jelszó kinyerését szótár felhasználásával.

[6] IANA EAP Registry: http://www.iana.org/assignments/eap-numbers

- **Man-in-the-middle támadások elleni védelem:** a metódusnak képesnek kell lennie többek között a kriptográfiai összerendelés létrehozására, az adatintegritás ellenőrzésére és az újrajátszás elleni védelem biztosítására.
- **Ciphersuite egyeztetés:** az EAP tranzakció során történő üzenetválás tartalmának és integritásának védelmére használt titkosító algoritmus és kulcs egyeztetésének lebonyolítása.

Ajánlott

- **Csomagok darabolása és összeillesztése:** a csomagok darabolásával és összeillesztésével a metódus legyen képes az EAP MTU-jánál (1200 byte) nagyobb üzenetek kezelésére is.
- **Bizalmasság:** ez többek között az EAP üzenetek és a felhasználói azonosítók titkosítását jelenti.

Opcionális

- **Csatorna hozzárendelés:** a csatorna hozzárendelés biztosítja a hitelesítő azonosságát, amikor az áteresztő módban van. Ennek egyik módja a fizikai címek vagy más végpont-azonosítók felhasználása a tikos kulcs generálása során.
- **Gyors újracsatlakozás:** a metódus lehetővé teszi, hogy a korábban felépített biztonságos kapcsolatot újra fel lehessen építeni kevesebb üzenetváltással.

1.7. A Wi-Fi Alliance biztonsági tanúsítványai

A Wi-Fi Alliance-t hat hálózati eszközöket gyártó cég hozta létre 1999-ben azzal a céllal, hogy a nagysebességű vezeték nélküli lokális hálózatok szabványait elterjesszék. A Wi-Fi Alliance 2000 áprilisában kezdte meg a vezeték nélküli hálózati eszközök együttműködési képességét biztosító tanúsítványok kiosztását.

1.7.1. Wi-Fi Protected Access (WPA)

A Wi-Fi Alliance az IEEE 802.11 munkacsoport irányítása mellett hozta létre a Wi-Fi Protected Access (WPA) biztonsági tanúsítványt, amely átmeneti megoldást jelentett a WEP leváltására az IEEE 802.11i kiegészítés végleges változatának elfogadásáig. A WPA biztonsági tanúsítvány 2003 elejétől kerül kiadásra.

Ahhoz, hogy egy eszköz megfeleljen a WPA tanúsítvány követelményeinek a következő biztonsági jellemzőkkel kell rendelkeznie:

- IEEE 802.1X és EAP alapú hitelesítés
- Kulcs generálás és kiosztás az IEEE 802.11i négyutas kézfogását felhasználva
- A TKIP mechanizmusok közül:
  - enkapszuláció és dekapszuláció
  - visszajátszás elleni védelem
  - Michael MIC integritás védelem

A WPA tanúsítvánnyal rendelkező eszközökből felépített hálózatok megfelelnek a 802.11i-ben definiált TKIP alapú RSN-nek, annak ellenére, hogy mind a TKIP mechanizmusokban, mind a négyutas kézfogásban van néhány kisebb eltérés.

1.7.2. Wi-Fi Protected Access 2 (WPA2)

Az IEEE 802.11i kiegészítés végleges változatának elfogadása után, 2004 szeptemberében kezdte meg a Wi-Fi Alliance a WPA2 tanúsítvány kiadását.

A WPA2 tanúsítvány az IEEE 802.11i kiegészítés végleges változatának való megfelelést jelenti, illetve, hogy ezek az eszközök a legtöbb esetben probléma nélkül képesek egymással kommunikálni.

Az, hogy a tanúsítvány nem biztosítja, hogy az eszközök minden esetben képesek együttműködni abból adódik, hogy azok a WPA2 tesztek során csak néhány elterjedt EAP metódussal kerülnek kipróbálásra, illetve, mivel jelenleg nincs WPA2 tanúsítvány AS-ek számára, ezért a Wi-Fi Alliance által a teszthez használt RADIUS implementációtól eltérő AAA szerver használata esetén sem biztosított az együttműködés.

A WPA2 eszközöknek a lefelé való kompatibilitás miatt implementálniuk kell továbbá a WEP TKIP mechanizmusait és négyutas kézfogását is.

1.7.3. A WPA és a WPA2 működési módjai

A WPA és a WPA2 is két működési móddal rendelkezik: *personal* és *enterprise*.

A personal működési mód, amelyet otthoni felhasználásra ajánlanak, előre kiosztott kulcsokat használ a hitelesítéshez, míg az enterprise működési mód esetén erre a célra az IEEE 802.1X és EAP kerül felhasználásra. A hálózati eszközöket lehet mindkét, vagy csak personal működési módhoz tanúsítani. Vállalati környezetben az enterprise minősítésű eszközök használata javasolt, mivel az előre kiosztott kulcsok esetén nehézkes azok generálása,

kiosztása és periodikus cseréje, továbbá a legtöbb olyan AP, amely csak az előre kiosztott kulcsokon alapuló hitelesítést ismeri nem képes egyedileg azonosítani a felhasználókat.

2. Vezeték nélküli személyi hálózatok (WPAN)

2.1. Bevezetés

A vezeték nélküli személyi hálózatok (Wireless Personal Area Network, WPAN) olyan kisméretű és kis hatótávolságú hálózatok, amelyek működtetéséhez nincs vagy csak minimális infrastrukturális eszközre van szükség. A WPAN-ok jellemzően csak pár eszközből állnak, amelyek egy személy környezetében, például egy szobában helyezkednek el.

A WPAN-ok célja hordozható eszközök (notebookok, PDA-k, mobiltelefonok), perifériák és más elektronikai eszközök ad hoc összekapcsolása vezeték nélkül, lehetővé téve azok kommunikációját és együttműködését.

A vezeték nélküli személyi hálózatok egyaránt alkalmaznak rádiófrekvenciás és infravörös fényen alapuló jelátvitelt is. Számos WPAN technológia létezik, mint például az Ultra-Wideband (UWB), a WiMedia, a Z-Wave vagy a ZigBee, de a két legelterjedtebb és legáltalánosabban használható a Bluetooth és az IrDA.

2.2. A Bluetooth

A Bluetooth egy általános célú, kis hatótávolságú, rádiófrekvenciás kommunikációt leíró specifikáció, ami lehetővé teszi hordozható eszközök ad hoc összekapcsolását egymással vagy perifériákkal. Tervezésekor a széleskörű használhatóság érdekében a kis méretet és fogyasztást, illetve az olcsó előállíthatóságot tartották szem előtt. A Bluetooth technológia fejlesztését az Ericsson kezdte meg 1994-ben, majd 1998 szeptemberében az IBM-mel, az Intel-lel, a Nokia-val és a Toshiba-val közösen alapította meg a Bluetooth Special Interest Group-ot (Bluetooth SIG). A 2002-ben bejelentett IEEE 802.15.1 szabványt a Bluetooth specifikáció 1.1-es verzióját alapul véve hozták létre.

2.2.1. A Bluetooth specifikáció

A Bluetooth specifikáció két részre osztja az általa definiált protokollokat, azok működtetője szerint:

- A magasabb szinten elhelyezkedő protokollok, mint pl. a Logical Link Control and Adaptation Protocol (L2CAP) és a Service Discovery Protocol (SDP) működtetéséért a *hoszt* a felelős. A hoszt szerepét leggyakrabban egy személyi számítógép vagy valamilyen más, de szintén programozható eszköz tölti be.
- Az alacsonyabb szinten elhelyezkedő protokollok (Bluetooth Radio, Bluetooth Baseband és Link Manager Protocol (LMP)) működtetését a *hoszt kontroller* végzi. A hoszt kontroller általában maga a Bluetooth hálózati adapter.

A hoszt és a hoszt kontroller a Host Controller Interface-en (HCI) keresztül kommunikál egymással. Speciális esetekben előfordulhat, hogy e két szerep nincs szétválasztva (pl. headset-ek esetében).

2.2.1.1. Bluetooth Radio

A Bluetooth Radio a specifikáció legalsó rétege, ez tartalmazza az adó-vevő leírását, az átvitelhez használt frekvenciasáv, a frekvenciaugrásos szórt spektrumú moduláció megadását és a csatornák definiálását.

A Bluetooth eszközök is az ISM frekvenciasávban működnek, ezért különösen fontos kiküszöbölni a más eszközök által okozott interferenciát. Erre a frekvenciaugrásos szórt spektrumú modulációt használják. A frekvenciaugrás miatt csökken az ütközések

valószínűsége, de ha mégis bekövetkezne, akkor a spektrumszórás miatt továbbra is minimális lesz a csomagvesztés. Ezen felül az átvitel során alkalmazható hibajavító kódolás is. A Bluetooth eszközök a kimeneti teljesítményük szerint 3 osztályba sorolhatóak.

Teljesítményosztály	Kimeneti teljesítmény	Hatótávolság
1	1mW (0 dBm) - 100 mW (20 dBm)	≤ 100 m
2	0,25 mW (-6 dBm) - 2,5 mW (4 dBm)	≤ 10 m
3	0 mW – 1 mW (0 dBm)	≤ 1 m

2.1. táblázat: Bluetooth teljesítmény osztályok

A vevő figyeli a jelerősséget és LMP parancsokkal (lásd később) jelzi a forrásnak, ha a kimeneti teljesítményt növelni vagy csökkenteni kell.

2.2.1.2. Bluetooth Baseband

A Baseband a Bluetooth fizikai rétege, ez kezeli a fizikai csatornákat, végzi a kapcsolatok felépítését, az időzítések kezelését, a frekvenciaugrás kiválasztását, a keretezést és definiálja a Bluetooth keretformátumát. Ezen felül a felette álló rétegeknek olyan szolgáltatásokat nyújt, mint más eszközök felderítése, torlódásvédelem, hibajavítás és kapcsolatszintű biztonság hitelesítés segítségével.

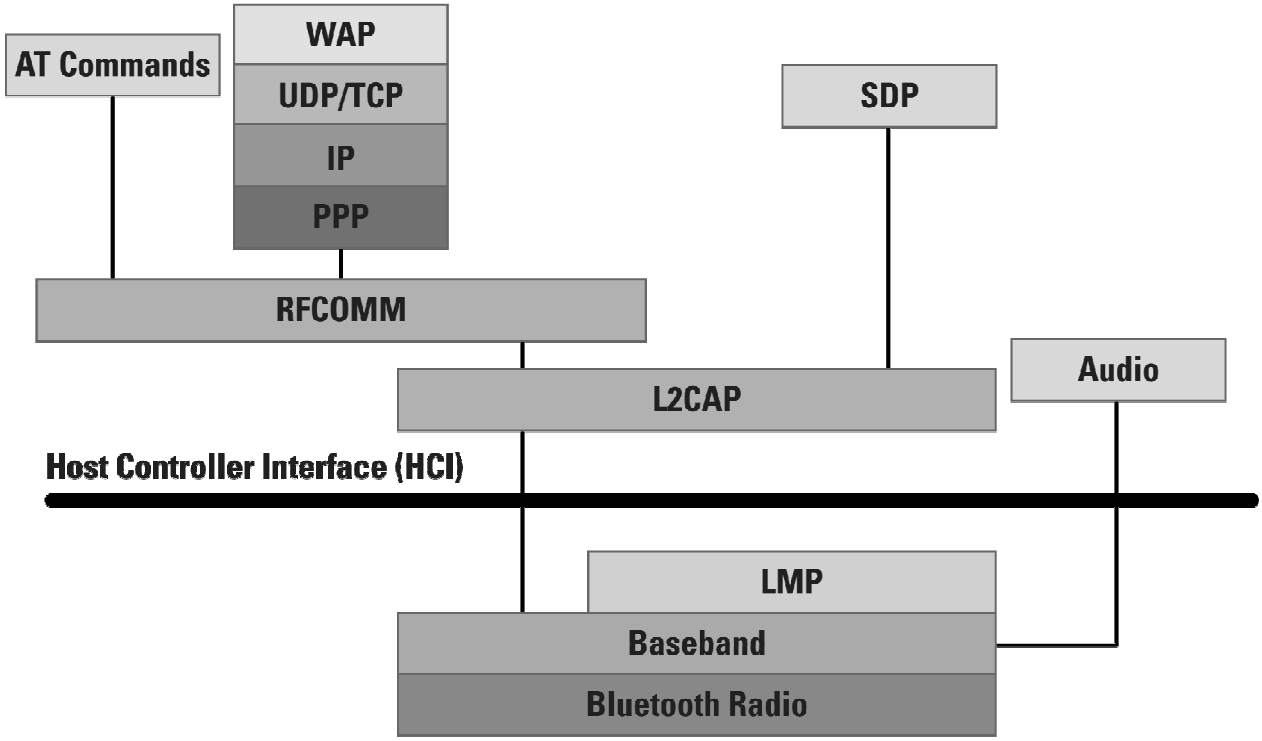
2.2.1.3. Link Manager Protocol (LMP)

Az LMP egy tranzakciós protokoll, amelynek feladata a csatornák felépítése, illetve a hitelesítés és a kapcsolat konfigurálása.

A kommunikáló eszközök az LMP segítségével azonosítják egymást, végzik a kódolási paraméterek beállítását, jelzik egymásnak az esetleges kapcsolattípus vagy kapcsolatminőség változtatási szándékukat. Az eszközök e protokollon keresztül végzik továbbá az adóteljesítmény vezérlését és a vételi jelerősség visszajelzését is, valamint ez a protokoll kezeli az eszközök pikohálózatbeli állapotát is (hold, park, sniff üzemmódok). A mester eszköz által kezdeményezett két lekérdezés közötti időtartamok kezeléséhez is az LMP nyújt funkciókat, ezzel valósítva meg a Bluetooth hálózatminőség-biztosítási (Quality of Service, QoS) támogatását.

2.2.1.4. Host Controller Interface (HCI)

A HCI egy szabványos parancs interfészt nyújt, amin keresztül lehet elérni a link kontrollert és a link menedzsert, illetve a hardver állapot és a vezérlő regisztereket. Ennek segítségével lehet például hálózati kapcsolatok létrehozását kérni, a specifikációban definiált 32 eseményhez tartozó paramétereket lekérdezni vagy valamelyik energiatakarékos üzemmódra váltani.



2.2. ábra: A Bluetooth protokoll stack (forrás: The Internet Protocol Journal 2008/4. szám)

2.2.1.5. Logical Link Control and Adaptation Protocol (L2CAP)

Az L2CAP a Baseband felett helyezkedik el és feladata a logikai csatornák vezérlése. A logikai csatornáknak három típusa van: jelzés (signaling), kapcsolat nélküli (connectionless) és kapcsolatalapú (connection-oriented) csatorna. Az L2CAP a felette elhelyezkedő rétegek számára a logikai csatorna típusának megfelelő csomagformátumot definiál. Ezek nagyobbak (akár 64 kB) is lehetnek, mint a fizikai réteg csomagjai, ezért az adó oldalon szegmentálásra, a vevő oldalon pedig a csomagok újraszerkesztésére lehet szükség, ami a többi réteg számára transzparensen zajlik le. Az L2CAP végzi a QoS információk kezelését is.

2.2.1.6. Service Discovery Protocol (SDP)

Az SDP gondoskodik egy Bluetooth eszköz hatósugarán belül újonnan elérhetővé vált, illetve a már nem elérhető szolgáltatások dinamikus felderítéséről. Maga az SDP protokoll nem biztosít hozzáférést a szolgáltatásokhoz, csak azok jellemzőit és az igénybevételükhöz szükséges információkat teszi elérhetővé, amelyek alapján a Bluetooth eszközök képesek egy szolgáltatást megtalálni.

2.2.2. A Bluetooth profilok

A Bluetooth profilok olyan általános viselkedéseket írnak le, amelyek segítségével az eszközök különböző szituációkban képesek együttműködni egymással. A Bluetooth specifikáció definiálja, hogy hogyan lehet olyan új profilokat megadni, amelyek kompatibilisek a Bluetooth eszközökkel.

Minden új profil leírásnak tartalmaznia kell a következőket:

- az egyéb profiloktól való esetleges függőségeket
- a javasolt interfész leírását
- azon magasabb szintű Bluetooth protokollok és azok paramétereinek listáját, amelyet a profil a működése során használ. Ez magában foglalhatja a szolgáltatási rekord megadását is, amennyiben az szükséges.

2.2.3. A Bluetooth architekturális modelljei

A Bluetooth szabvány lehetővé teszi a hálózat kiépítése során az ad hoc és az infrastrukturális logikai szervezési mód használatát is, azonban a gyakorlatban a Bluetooth eszközöket szinte mindig ad hoc módon kapcsolják össze. Ebben a fejezetben csak az ad hoc szervezési mód szerint kiépített hálózatok kerülnek tárgyalásra.

2.2.3.1. Pikohálózatok és szórt hálózatok

A pikohálózat a Bluetooth hálózatok alapegysége, ami egy mester eszközből és legfeljebb hét aktív szolga eszközből áll. A szolgák egymással közvetlenül nem kommunikálnak, csak a mesterrel és csak akkor, amikor az engedélyezi számukra.

A pikohálózat tagjait a 3 bites logikai cím (Logical Transport Address, LT_ADDR) azonosítja[7]. A nem aktív, de a mesternél regisztrált (park állapotban lévő) eszközből hétnél

[7] A szabvány eredeti változatában ezt a címet aktív tag címnek (Active Member Address, AM_ADDR) nevezték.

több is lehet. Egy Bluetooth eszköz egy időben több pikohálózathoz is tartozhat, amelyet az időosztásos multiplexelésen (Time Division Multiplexing, TDM) alapuló csatornafelosztás tesz lehetővé. Egy pikohálózat bármelyik tagja lehet egy másik pikohálózatban szolga vagy mester, de mester csak az egyikben. Ha egy mester akar csatlakozni egy másik pikohálózathoz, akkor a hozzá tartozó eszközök közötti kommunikáció a mester szerepbe való visszaváltásáig szünetel. Az egymással így összekötött pikohálózatok együtt egy szórt hálózatot alkotnak.

2.2.4. Link típusok

A Bluetooth három link típust definiál a mester és a szolga eszközök között: az SCO-t és az eSCO-t valós idejű hangátvitelhez és az ACL-t általános adatátvitelhez.
A link kiépítéséhez a szabvány két eljárást definiál. Az inquiry eljárás arra szolgál, hogy egy eszköz képes legyen a hatótávolságán belüli más Bluetooth eszközök felderítésére, egy speciális kérés küldésével. Azon eszközök, amelyek láthatóvá kívánnak válni más eszközök számára, a kapott kérésre egy inquiry választ küldenek, ami többek között tartalmazza a 48 bites fizikai címüket (Bluetooth Device Address, BD_ADDR). Ha a mester ismeri a csatlakoztatni kívánt eszköz címét, akkor a kapcsolat felépítése a *page* eljárással történik.

2.2.4.1. Szinkron kapcsolatorientált link (Synchronous Connection Oriented, SCO)

Az SCO link szimmetrikus, pont-pont összeköttetéseket támogat két eszköz között, amelyet leggyakrabban hangátvitelre használnak. A csatornán az SCO link számára egyenlő időközönként két egymás utáni időrést foglalnak le. A maximális átviteli sebessége 64 kb/s mindkét irányban.

2.2.4.2. Kibővített szinkron kapcsolatorientált link (Extended SCO, eSCO)

Az eSCO link annyiban tér el az SCO linktől, hogy nem feltétlenül szimmetrikus, azaz az egyik irányba nagyobb sávszélesség foglalható, továbbá lehetőség van a lefoglalt időréseket követő időrésekben az újraküldésre.

2.2.4.3. Aszinkron kapcsolat nélküli link (Asynchronous Connectionless, ACL)

Az ACL link csomagkapcsolt, pont-pont és pont-többpont összeköttetéseket támogat. Aszinkron kommunikáció csak azokban az időrésekben folyhat, amelyek nincsenek lefoglalva szinkron átvitelre. A mester és egy szolga eszköz között csak egy ACL összeköttetést lehet

létrehozni. Az ACL kapcsolatok vezérlését a mester eszközök lekérdezéssel valósítják meg, azaz egy szolga csak akkor küldhet csomagot a páratlan sorszámú (szolga-mester) időrésben, ha a mester az előző páros sorszámú (mester-szolga) időrésben lekérdezte. Aszinkron összeköttetés esetén lehetőség van a pikohálózatban résztvevő összes egység csoportos címzésére is üzenetszórással, így minden szolga lekérdezésre kerül.

2.2.5. Energiatakarékos üzemmódok

A Bluetooth szabvány az eszközök ezen üzemmódjait nem csak abból a célból definiálja, hogy csökkentsék az energiafelvételt, hanem ezek segítségével oldható meg az is, hogy, hogy egy aktív eszköz page és inquiry eljárásokat hajtson végre, illetve, hogy részt vegyen egy másik pikohálózatbeli kommunikációban is. A Bluetooth szabvány energiatakarékos üzemmódjai a következőek:

2.2.5.1. Sniff üzemmód

Ebben az üzemmódban a legnagyobb az energiafelvétel. Amikor egy szolga eszköz ACL linken keresztül kommunikál a mesterrel, akkor minden páros időrésben figyelnie kell annak adását. Sniff üzemmódban a szolga azonban csak minden előre egyeztetett n-edik időrésben figyeli a mester adását, de nem veszíti el a mester által neki kiosztott LT_ADDR címét.

2.2.5.2. Hold üzemmód

Hold üzemmódban az eszköz egy meghatározott ideig nem fogad ACL csomagokat. Ezen időintervallum alatt a szolga felszabadíthatja az erőforrásait, és például csatlakozhat egy másik pikohálózathoz. A szolga közli a mesterrel, hogy mennyi ideig marad hold üzemmódban, mielőtt arra átváltana. Amikor ez az idő lejárt a szolga szinkronizálódik a csatornához, majd fogadja a mester további utasításait. A hold üzemmódba váltó szolga is megtartja az LT_ADDR címét.

2.2.5.3. Park üzemmód

Park üzemmódba lépéskor a szolga elveszíti az LT_ADDR címét, de kap két másikat: egy 8 bites park üzemmód cím (Parked Mode Address, PM_ADDR), ami a park üzemmódban lévő szolgák azonosítására szolgál, és egy szintén 8 bites hozzáférés kérési cím (Access Request Address, AR_ADDR), ami a szolga pikohálózatba való visszatérése során használnak. Azért, hogy a park üzemmódú szolgák megtartsák a szinkronizációt a mesterrel azok periodikusan

felébrednek, és belehallgatnak a beacon csatornába, aminek paramétereit az eszközök a mestertől kapják meg, mielőtt erre az állapotra váltanának. A mester szintén a beacon csatornát használja a szolgák felébresztésére. Ha a szolga vissza szeretne térni a pikohálózatba, akkor a beacon csatorna időrését követő első időrésben küld egy üzenetet a mesternek. A park és az aktív üzemmód közötti váltogatással lehet virtuális egy mesterhez akár 255 szolgát kapcsolni.

2.3. A Bluetooth specifikáció biztonsága

A Bluetooth specifikáció eddigi verziói összesen négy biztonsági módot definiáltak. Minden eszköznek e módok valamelyikében kell működnie.

- **Security mode 1:** Ennél a módnál az eszközök nem alkalmaznak sem hitelesítést, sem titkosítást. A Security mode 1 csak a Bluetooth v2.1+EDR előtti verziói által támogatott.
- **Security mode 2:** A Security mode 2 (SM 2) szolgáltatás szintű biztonsági mód. A biztonsági procedúrák az LMP link kiépítése után, de az L2CAP csatorna létrehozása előtt kerülnek végrehajtásra. Ennél a biztonsági módnál egy – a Bluetooth specifikációban definiált – biztonságkezelő vezérli az eszközökhöz és az azok által nyújtott szolgáltatásokhoz való hozzáférést. A biztonságkezelő segítségével eltérő biztonsági politikákat és bizalmi szinteket (lásd később) lehet hozzárendelni az egymással párhuzamosan működő, de eltérő biztonsági követelményekkel rendelkező szolgáltatásokhoz. A Bluetooth specifikáció az SM 2-ben vezeti be az authorizációt, amely arra szolgál, hogy a biztonságkezelő eldönthesse, hogy mely eszköz mely szolgáltatásokhoz férhet hozzá. Fontos megjegyezni, hogy az SM 2 által használt hitelesítési és titkosítási mechanizmusok az LMP rétegben vannak implementálva. Minden Bluetooth eszköz támogatja a SM 2-t, de a v2.1+EDR-nél újabb verziójú eszközök csak a régebbi verziókkal való lefelé kompatibilitás miatt.
- **Security mode 3:** A Security mode 3 (SM 3) kapcsolat szintű biztonsági mód. A Bluetooth eszköz azelőtt kezdeményezi a biztonsági procedúrák végrehajtását, mielőtt a link kiépítése befejeződne.

  Az SM 3-ban működő Bluetooth eszközök minden esetben megkövetelik a kommunikációban résztvevő eszközök hitelesítését és az adatforgalom tikosítását is. A hitelesítés lehet egy és kétirányú is. A hitelesítés és a titkosítás a titkos összekötő kulcson

alapulnak, ami az eszközök párosításakor kerül kiosztásra. Ez a biztonsági mód csak a v2.1+EDR előtti verziók által támogatott.

- **Security mode 4:** A Bluetooth v2.1+EDR specifikációban került definiálásra. Az SM 2-höz hasonlóan ez is szolgáltatás szintű biztonsági mód, amelynél a biztonsági procedúrák végrehajtása csak a link kiépítése után kezdeményeződik. A biztonságos egyszerű párosítás (Secure Simple Pairing, SSP) elliptikus görbe feletti Diffie-Hellman algoritmust használ a kulcscseréhez és a kulcsgeneráláshoz. Az eszközök hitelesítése és az alkalmazott titkosítási algoritmusok megegyeznek a Bluetooth v2.0+EDR és a korábbi verziók által használttal.

  A Security mode 4 esetén a szolgáltatások a következő biztonsági igényekkel rendelkezhetnek:
  - az összekötő kulcs hitelesítése is szükséges
  - nincs szükség az összekötő kulcs hitelesítésére
  - nincs szükség semmilyen biztonsági intézkedésre.

  Az SM 4 kötelező v2.1+EDR vagy újabb verziójú eszközök között.

2.3.1. Összekötő kulcs generálása

A Bluetooth eszközök, attól függően, hogy melyik biztonsági módban működnek, két féle módon generálhatják az összekötő kulcsot.

2.3.1.1. Kulcsgenerálás Security mode 2 és 3 esetén

A Bluetooth v2.0+EDR és korábbi verzióiban az eszközök szimultán állítják elő az összekötő kulcsot a párosítási folyamat során, miután a felhasználók megadják a PIN kódot az egyik, vagy mindkét eszközön. A PIN kód hossza 1 és 16 byte között változhat. Amennyiben a PIN kód rövidebb, mint 16 byte, akkor a BD_ADDR-el kerül kiegészítésre, így előállítva az inicializáló kulcsot.
Miután az inicializálás befejeződött, az eszközök automatikusan és transzparens módon kezdeményezik a hitelesítést és a titkosítást.

2.3.1.2. Kulcsgenerálás Security mode 4 esetén

A biztonságos egyszerű párosítást a v2.1+EDR specifikáció tartalmazza. Az SSP egyszerűbbé teszi a párosítási folyamatot az által, hogy a különböző beviteli képességekkel rendelkező

eszközök számára más-más párosítási módszert tesz lehetővé. Az SSP elliptikus görbe feletti Diffie-Hellman kulcsgenerálást és kulcscserét használ, ami jelentősen megnehezíti a későbbi lehallgatást és a man-in-the-middle támadásokat.

Az SSP a következő négy összerendelési módszert teszi lehetővé:

- **Numerikus összehasonlítás:** abban az esetben használható, ha mindkét párosítandó eszköz képes megjeleníteni egy hatjegyű számot és a felhasználónak van lehetősége „Igen" vagy „Nem" válasz bevitelére. A lényegi különbség e módszer és a specifikáció első változatában használt PIN kód alapú párosítás között, hogy a megjelenített szám a későbbiekben nem kerül felhasználásra az összekötő kulcs generálása során.
- **Jelszó megadás:** ez abban az esetben használható, amikor az egyik eszköz rendelkezik valamilyen beviteli lehetőséggel, de a másik eszköz csak megjelenítésre képes. Ekkor a megjelenítővel rendelkező eszköz mutat a felhasználó számára egy hatjegyű számot, amit annak a másik eszközön be kell vinnie. Ahogy a numerikus összehasonlítás esetén, itt sem kerül a hatjegyű szám felhasználása a későbbiek során, így ennek nincs értéke a támadó számára.
- **„Just works":** abban az esetben használható, ha az egyik eszköz nem rendelkezik se beviteli, se megjelenítési képességekkel (például headset-ek). Ekkor a felhasználónak a párosításhoz csak az eszköz csatlakozási kérelmét kell elfogadnia.
- **Out of Band (OOB):** olyan eszközök esetén alkalmazható, amelyek képesek valamilyen más vezeték nélküli technológiával (például Near Field Communication, NFC) is kommunikálni a Bluetooth-on kívül, így elvégezve az eszközök felderítését és a kulcscserét. Például az említett NFC esetén lehetőség nyílik az eszközök párosítására mindössze azok egymáshoz érintésével és egy gomb megnyomásával. Az OOB párosítás esetén figyelni kell arra, hogy a kulcscseréhez használt másik technológia is kellően biztonságos legyen.

A fenti négy módszer mindegyike, a „Just works" kivételével hitelesített összekötő kulcsok előállítását teszi lehetővé.

2.3.2. Hitelesítés

A Bluetooth az eszközök hitelesítésére egy kihívás-válasz protokollt használ. A hitelesítési folyamatban az eszközök két szerepkörben vehetnek részt. Az igénylők azok az eszközök,

amelyek megpróbálják az azonosságukat bizonyítani, a vizsgálók pedig azok, amelyek az igénylők azonosságát ellenőrzik.

A hitelesítéshez használt kihívás-válasz protokoll működése azon alapul, hogy a vizsgáló ellenőrzi, hogy az igénylő ismeri-e az előre megosztott tikos kulcsot, ami ebben az esetben a Bluetooth összekötő kulcs.

2.3.2.1. A hitelesítési folyamat

A hitelesítési folyamat a következő lépésekből áll:

1. A vizsgáló eszköz generál és elküld az igénylőnek egy 128 bites véletlen értéket (AU_RAND).
2. Az igénylő az E1[8] algoritmust használva kiszámítja a vizsgálónak küldendő választ. Ennek bemenetei a 48 bites BD_ADDR, az összekötő kulcs és a vizsgáló által küldött AU_RAND érték. Ezzel párhuzamosan a vizsgáló is elvégzi ugyan ezt a számítást. Az E1 algoritmus által előállított 128 bites értéknek csak a legszignifikánsabb 32 bitje kerül felhasználásra a hitelesítési folyamatban. A maradék 96 bit, az úgy nevezett ACO (Authenticated Ciphering Offset) érték, amelyet majd a későbbiekben a titkosító kulcs generálásához használnak fel.
3. Az igénylő válaszként visszaküldi az E1 algoritmus kimenetének legszignifikánsabb 32 bitjét a vizsgálónak.
4. A vizsgáló összehasonlítja a válaszként kapott értéket a saját maga által számított értékkel. Ha a kettő megegyezik, akkor a hitelesítési folyamat sikeres. Amennyiben nem, akkor az újabb hitelesítési kísérlet előtt az eszköz kivár egy adott időintervallumot. Ez az időintervallum a kísérletek számával exponenciálisan növekszik, hogy megakadályozza az összekötő kulcs próbálgatással történő megszerzését.

Ezen lépések egyszeri végrehajtásával egyirányú hitelesítés lehetséges. A Bluetooth szabvány lehetővé teszi az eszközök kétirányú hitelesítését is, ez esetben a fenti folyamatot még egyszer meg kell ismételni, úgy, hogy az eszközök szerepkört cserélnek.

Az összekötő kulcs az eszközök párosítási folyamata során áll elő és soha nem kerül felfedésre a Bluetooth eszközökön kívül. Fontos megjegyezni, hogy hitelesítés

[8] A hitelesítéshez használt E1 függvény a SAFER+ (Secure And Fast Encryption Routine) iterált blokktitkosító algoritmus egy módosított változata.

megbízhatósága egyedül az összekötő kulcs titkosságán alapul, mivel a Bluetooth eszközök címe és a vizsgáló által küldött AU_RAND érték is nyilvános paraméter.

2.3.3. Titkosítás

A Bluetooth specifikációban három titkosítási mód van definiálva:

- **Encryption mode 1:** a teljes adatforgalom titkosítás nélkül zajlik.
- **Encryption mode 2:** az egyedileg címzett eszközök felé az adatforgalom titkosítva halad. A titkosító kulcs az egyes eszközök összekötő kulcsait felhasználva számítódik ki. Az üzenetszórással küldött adatok nincsenek titkosítva.
- **Encryption mode 3:** a teljes adatforgalom a mester összekötő kulcsán alapuló titkosító kulccsal tikosítva zajlik.

Az Encryption mode 2 és az Encryption mode 3 ugyanazt a titkosítási mechanizmust alkalmazza.

2.3.3.1. Az E0 folyamtitkosító

A Bluetooth titkosítása az E0 folyamtitkosítón alapul. Ez a generált kulcsfolyamot kizáró vagy művelet segítségével kapcsolja össze az adatfolyammal és ez kerül elküldésre a fogadó eszköznek.

Az E0 titkosító algoritmus négy lineáris visszacsatolású shift-regisztert (LFSR) használ, amelyek szélessége 25, 31, 33 és 39 bit, összesen 128 bit. Ezek kezdőértéke a következő bemenetekből áll elő: a mester eszköz fizikai címe (BD_ADDR), egy 128 bites véletlenszám, egy résszám és a tikosító kulcs. A folyamtitkosító által használt résszám minden csomagnál változik és a LFSR regiszterek is újra inicializálásra kerülnek.

A titkosító algoritmus által használt kulcsot az E3 belső kulcsgenerátor állítja elő. A titkosító kulcs a 128 bites összekötő kulcs (amely a Bluetooth eszközben tárolt titok), egy 128 bites véletlenszám és a hitelesítési folyamat során előállt 96 bites ACO érték felhasználásával számítódik ki.

A titkosító kulcs hossza 8 és 128 bit között változhat, ezért szükség van egy kulcsméret egyeztetési folyamatra a mester és a szolga eszközök között. Ennek során a mester eszköz egy kulcsméret ajánlást tesz a szolgáknak, amelyet azok elfogadhatnak vagy egy másik kulcsméretet ajánlhatnak. Ez a folyamat addig ismétlődik, ameddig valamely ajánlás elfogadásra nem kerül. A mester által elsőként felajánlott kulcsméret a gyártó által rögzített

annak hoszt kontrollerében. Ez a kulcsméret függ az eszköz jellegétől, ezért nem feltétlenül 128 bit.

A specifikáció nem követeli meg, de az implementációkban gyakran megadnak egy olyan minimális kulcsméretet is, amely még elfogadható az eszköz számára, annak megakadályozására, hogy az egyeztetés során olyan rövid kulcsméret kerüljön elfogadásra, amivel már nem lehet kellő biztonsággal kommunikálni.

2.3.3.2. Az E0 folyamtitkosító erőssége

Az E0 folyamtitkosító algoritmus vizsgálata során annak számos gyengeségére derült már fény. A legfrissebb ismert eredmények[9] szerint elméletben lehetséges egy olyan ismert nyíltszövegen alapuló támadást végrehajtani, amelynek segítségével meg lehet határozni a titkosító kulcsot és műveletigénye mindössze 2^{38}, szemben a nyers erő alapú támadással, amely 2^{128} lehetséges kulcs tesztelését igényli.

2.3.4. A Bluetooth eszközök bizalmi szintjei

A Bluetooth eszközöknek két bizalmi szintje van:

- A megbízható eszközök azok, amelyek állandó kapcsolattal csatlakoznak az eszközhöz és annak minden szolgáltatásához korlátlanul hozzáférhetnek. Ezeket az eszközöket először hitelesíteni kell, majd ezután az összekötő kulcsuk tárolásra kerül és az eszköz adatbázisban megbízhatóként kerülnek megjelölésre.
- A nem megbízható eszközöknek nincs állandó kapcsolata az eszközzel és csak korlátozottan férhetnek hozzá annak szolgáltatásaihoz. Egy új, ismeretlen eszköz mindig nem megbízhatóként kerül be az eszköz adatbázisba.

2.3.5. Szolgáltatások biztonsági szintjei

Három biztonsági szint került definiálásra a Bluetooth eszközök által nyújtott szolgáltatások eléréséhez.

- **Service level l:** a szolgáltatás eléréséhez hitelesítésre és authorizációra van szükség. Ennél a biztonsági szintnél csak a megbízható eszközök kaphatnak automatikus hozzáférést, a nem megbízható eszközök esetén mindig manuális authorizációra van szükség.

[9] Lu, Meier és Vaudenay: *„The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption”* (CRYPTO 2005, forrás: http://lasecwww.epfl.ch/pub/lasec/doc/LMV05.pdf)

- **Service level 2:** a szolgáltatás csak hitelesítést igényel, authorizációra nincs szükség. A hozzáférés csak a hitelesítési folyamat befejezése után engedélyezett.
- **Service level 3:** nincs szükség se hitelesítésre, se authorizációra, a szolgáltatáshoz történő hozzáférés automatikusan biztosított.

A Bluetooth architektúrája lehetővé teszi olyan hozzáférési politikák definiálást, amelyek a megbízható eszközök számára is csak bizonyos szolgáltatásokat tesznek hozzáférhetővé. A Bluetooth biztonsági megoldásai transzparensen működnek az alkalmazási réteg felé, ezért lehetséges felhasználó szintű hitelesítést és részletes hozzáférés-szabályozást megvalósítani a Bluetooth biztonsági keretrendszerén belül az alkalmazási rétegben.

2.3.6. Bluetooth specifikus fenyegetettségek

Létezik néhány olyan biztonsági fenyegetettség, amely a Bluetooth technológiát használó mobil eszközök jellegzetességeit vagy implementációs hiányosságait használja ki.

2.3.6.1. Bluejacking

A bluejacking anonim üzenetek küldését teszi lehetővé Bluetooth-on keresztül olyan eszközök felé, amelyek támogatják a névjegyek (vCard) küldését.
Ez nem nevezhető igazi támadásnak, mivel nem jár sem adatmódosítással, sem adatvesztéssel. Olyan készülékek ellen használható, ahol az Object Push Profile (OPP) implementációja lehetővé tesz annak hitelesítés nélküli használatát. A rejtett (non-discoverable) módban lévő eszközökkel szemben nem működik.

2.3.6.2. Bluebugging

A bluebugging egy biztonsági rést kihasználva lehetővé teszi, hogy AT parancsokat adjanak ki egy eszközön annak felhasználójának engedélye nélkül egy rejtett csatornán. Ez a sebezhetőség lehetővé teszi a támadó számára, hogy például egy telefonról hívásokat kezdeményezzen, vagy azokat lehallgassa, szöveges üzeneteket küldjön és fogadjon, olvassa és írja a telefonkönyvet, illetve hogy az Internetre csatlakozzon.

2.3.6.3. Bluesnarfing

A bluesnarfing az Object Exchange (OBEX) protokoll implementációjának hibáját kihasználó támadás. A támadó az engedélyezett objektum feltöltés (push) helyett letöltés (pull) parancsot

is kiadhat, ami lehetővé teszi, hogy a felhasználó tudta nélkül hozzáférjen a telefonon tárolt adatokhoz (telefonkönyv, naptárbejegyzések, SMS-ek, IMEI szám stb.). Nem szükséges hozzá az eszközök párosítása.
A Blooover nevű Java ME alkalmazással ez a támadás akár egy mobiltelefonról is végrehajtható.

2.3.6.4. Car Whisperer

A Car Whisperer nevű alkalmazás a Bluetooth autós készletek egy implementációs gyengeségét kihasználva lehetővé teszi a támadó számára, hogy a hívásokat lehallgassa, illetve hogy hangot továbbítson az autós készlet felé.
Ezek az eszközök általában valamilyen egyszerű, rögzített PIN kóddal (pl. 1234, 0000) kapcsolódnak a telefonhoz. A támadás ezt a gyenge PIN kód beállítást használja ki.

2.3.7. Rendelkezésre állás

Mint bármely más vezeték nélküli hálózati technológia, a Bluetooth is érzékeny a szolgáltatás megtagadási támadásokra. A rendelkezésre állás kérdése leginkább az ad hoc szervezésű hálózatoknál kritikus, mivel a kommunikációban résztvevő eszközök üzeneteket kell továbbítaniuk más eszközök felé.

- A legegyszerűbb lehetőség DoS támadás indítására a Bluetooth esetében is az általa használt ISM frekvenciasáv zavarása.
- Egy másik, kevésbé valószínű helyzet, amikor a támadó a mobil Bluetooth eszköz akkumulátorának lemerítésével próbálja azokat képtelenné tenni a hálózaton belüli kommunikációra. Ezt úgy éri el, hogy folyamatosan kéréseket indítanak az eszköz felé, így az nem képes energiatakarékos állapotra váltani.
- Léteznek olyan alkalmazások, amelyek segítségével a Bluetooth szolgáltatást zavarni lehet hibás formátumú vagy más, nem szabványos csomag küldésével. Ezzel elérhető, hogy az eszköz lassabban vagy egyáltalán ne legyen képes válaszolni. Ezen alkalmazásokat a Bluetooth implementáció hibáinak feltárásához fejlesztették, de támadások is indíthatóak velük. Ilyen támadási lehetőség volt például egy nagy méretű (jellemzően több mint 600 kB hosszúságú) L2CAP ping kéréssel.

2.4. IrDA

Az Infrared Data Association (IrDA) egy nonprofit szervezet, aminek célja, hogy olcsó, kis hatótávolságú, infravörös fénnyel történő kommunikációhoz szabványokat fejlesszen. 1993. június 28-án kezdte meg működését a HP infravörös ajánlását alapul véve.
Az IrDA két fő szabványt hozott létre: az IrDA Data-t nagysebességű adatátvitelhez és az IrDA Control-t vezeték nélküli lassú perifériákhoz (billentyűzetek, mutatóeszközök stb.).

2.4.1. Az IrDA Data specifikáció

2.4.1.1. IrPHY (IrDA Physical Layer)

Az IrPHY tartalmazza az optikai adó-vevő, a jelkódolás, a keretezés és az átvitel jellemzőinek leírását.
A kommunikáció half-duplex, pont-pont típusú. A full-duplex átvitelt az elsődleges eszköz vezérlésével, a kommunikáció irányának váltogatásával lehet szimulálni.
Az IrPHY folyamatos működés esetén a hatótávolságot 1 méterben (kis energiafogyasztású eszközök között 0,2 méterben), a rálátás nyílásszögét ±15º-ban határozza meg.
A Serial Infrared (SIR, 1994) 115,2 Kb/s, a Fast Infrared (FIR, 1995) 4 Mb/s, a Very Fast Infrared (VFIR, 1999) ajánlás 16 Mb/s maximális adatátviteli sebesség eléréséhez ad specifikációt.

2.4.1.2. IrLAP (IrDA Link Access Protocol)

Az IrLAP az IrDA Data adatkapcsolati rétege. IrLAP végzi az egymással kommunikálni képes eszközök felderítését, a kapcsolat létrehozását és fenntartását, a hibajavítást (CRC-16 1,152 Mb/s-ig, e fölött CRC-32), illetve az elsődleges/másodlagos szerepkör megállapítását a két eszköz között.
Az elsődleges eszköz vezérli a másodlagos eszközt, utóbbi csak akkor küldhet adatot, ha az elsődleges eszköz erre kérést küld.

2.4.1.3. IrLMP (IrDA Link Management Protocol)

IrLMP két komponenst definiál: a Link Management Information Access Service-t (LM-IAS) és a Link Management Multiplexer-t (LM-MUX). Az LM-IAS teszi lehetővé az információcserét a kapcsolatban résztvevő eszközökről és az általuk nyújtott

szolgáltatásokról, míg az LM-MUX biztosítja egy eszköz számára, hogy ugyanazon az IrLAP kapcsolaton keresztül több alkalmazás kommunikáljon.

2.4.2. Az IrDA Data biztonsága

Az IrDA Data szabvány nem biztosít semmilyen kapcsolatszintű védelmet, nincs hitelesítés, authorizáció és a kommunikáció titkosítás nélkül zajlik. Ha ezekre szükség lenne, azt az alkalmazási rétegben kell megvalósítani.

Elméletben lehetséges az adatforgalom lehallgatása a visszavert infravörös fény észlelésével és a környezeti zajokat kiszűrve, de mivel a kommunikáló eszközöknek igen kis szögben közvetlen rálátással kell rendelkezniük egymásra, továbbá az átvitel hatótávolsága is igen rövid, és a terepakadályok is gátolják, ezért annak ellenére, hogy maga a szabvány nem nyújt semmilyen védelmet, viszonylag biztonságos technológiának tekinthető.

3. Összefoglalás

A vezeték nélküli hálózatok kezdetben számos biztonsági hiányossággal küzdöttek. A vezeték nélküli lokális hálózatok legelterjedtebb szabványa az IEEE 802.11. Ennek első verziójában került definiálásra a WEP, amely a vezetékes hálózatokkal összehasonlítható biztonságot ígért. Azonban ennek rövid időn belül számos hiányosságára derült fény, amelyek az alkalmazott kriptográfiai algoritmusok gyengeségeire vezethetőek vissza, így helyes konfiguráció esetén sem nyújt kellő biztonságot és a paraméterek erősítésével sem javítható jelentős mértékben. A WEP alkalmazása ma már nem javasolt, viszont ennek ellenére a legtöbb otthoni felhasználásra szánt vezeték nélküli hálózati eszköz még mindig ezt ajánlja fel alapértelmezett beállításként. A szabvány 802.11i kiegészítésében definiált RSN megoldást kínál a WEP összes ismert gyengeségére egy olyan biztonsági keretrendszer definiálásával, ami lehetővé teszi a felhasználók fejlett hitelesítését, az alkalmazott kriptográfiai kulcsok menedzsmentjét, erős titkosítás alkalmazását és lehetőséget nyújt arra, hogy a szervezetek a számukra legmegfelelőbb biztonsági politikát alakíthassák ki. Azonban ügyelni kell arra, hogy az implementáció során az RSN szabadon választható elemei (például a hitelesítéshez használt EAP metódus vagy a hitelesítő szerver implementációja) is kellően biztonságos legyen. Otthoni felhasználásra a WPA2 előre kiosztott kulcsokat alkalmazó változatának használata ajánlott.

A vezeték nélküli személyi hálózati szabványok megjelenése későbbre tehető, így már a tervezés során figyelembe vették WLAN-ok biztonságával kapcsolatos tapasztalatokat, így a Bluetooth specifikációt is már úgy tervezték meg, hogy a felhasználásának megfelelően erős biztonsági megoldásokat tartalmazzon. A Bluetooth specifikációnak jelenleg nincs ismert hiányossága, azonban a biztonsági szint nagymértékben függ az implementáció minőségétől és az alkalmazott beállításoktól. Például konfiguráció során kerülni kell a statikus vagy gyenge PIN kódok használatát, érdemes korlátozni az eszközök láthatóságát, illetve kikapcsolni a Bluetooth-t, ha nincs rá szükség.

A WPAN-okban használt IrDA Data az átvitelhez használt infravörös fény tulajdonságai és a kis hatósugár miatt kellően biztonságos, annak ellenére is, hogy nem nyújt semmilyen biztonsági funkcionalitást. De az alkalmazás szinten megvalósítható itt is hitelesítés és tikosítás a biztonság növelésére.

A fentieket figyelembe véve mára már a vezeték nélküli hálózatok kellően biztonságos alternatíváinak tekinthetőek a vezetékes hálózatoknak.

4. Irodalomjegyzék

Könyvek

1. M. Gast: *„802.11 Wireless Networks - The Definitive Guide”*
   (O'Reilly, 2005)
2. R. Flickenger: *„Building Wireless Community Networks (2nd Edition)”*
   (O'Reilly, 2003)
3. P. Mateti: *„Hacking Techniques in Wireless Networks”*
   (Wright State University, 2005, forrás:
   http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm
4. J. Geier: *„Vezeték nélküli hálózatok”*
   (Panem, 2005)
5. T. Karygiannis, L. Owens: *„Wireless Network Security, 802.11, Bluetooth and Handheld Devices”*
   (National Institute of Standards and Technology, 2002)
6. R. K. Nichols, P. C. Lekkas: *„Wireless Security - Models, Threats, and Solutions”*
   (McGraw-Hill, 2002)

Szabványok

1. *IEEE Std 802.11-2007: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*
   (IEEE, 2007)
2. *IEEE Std 802.1X-2004: Port-Based Network Access Control*
   (IEEE, 2004)

Cikkek

1. T. Vainio: *„Bluetooth Security”*
   (Helsinki University of Technology, 2000, forrás: http://www.mowile.com/bluesec.pdf)
2. G. Lamm et al.: *„Bluetooth Wireless Networks Security Features”*
   (University of Virginia, 2001, forrás:
   http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.121.5042&rep=rep1&type=pdf)

3. T. Macaulay: *„Hardening IEEE 802.11 Wireless Networks”*
(EWA Canada, 2002, forrás: http://magnoliaroad.net/downloads/hardening_802.11.pdf)
4. N. Mavrogiannopoulos: *„On Bluetooth Security”*
(HELLUG.gr, 2005, forrás: http://members.hellug.gr/nmav/papers/other/Bluetooth%20security.pdf)
5. K. M. J. Haataja: *„Security in Bluetooth, WLAN and IrDA - A Comparison”*
(University of Kuopio, 2006, forrás: http://www.cs.uku.fi/research/publications/reports/A-2006-1.pdf)
6. C. Low: *„Understanding Wireless Attacks and Detection”*
(SANS.org, 2005, forrás: http://www.sans.org/reading_room/whitepapers/detection/understanding-wireless-attacks-detection_1633)
7. G. Deckerd: *„Wireless Attacks from an Intrusion Detection Perspective”*
(SANS.org, 2006, forrás: http://www.sans.org/reading_room/whitepapers/honors/wireless-attacks-intrusion-detection-perspective_1681)

Jegyzetek, órai jegyzetek

1. *Kriptográfia 1. órai jegyzet*, 2006, Dr. Pethő Attila előadásai alapján
2. *Kriptográfiai protokollok órai jegyzet*, 2008, Dr. Huszti Andrea előadásai lapján
3. *Hálózatok órai jegyzet*, 2009, Dr. Almási Béla előadásai alapján
4. *Számítógép-hálózatok*, előadás segédlet, 2006. Dr. Almási Béla

Prezentációk

1. Krasznay Cs.: *„Vezetéknélküli hálózatok (WiFi, Bluetooth) biztonsága”*
(Kancellár.hu, PTE Szakhét 2007, forrás: http://krasznay.hu/presentation/pte2007_krasznay.ppt)
2. Jákó A.: *„Wireless LAN”*
(BME EISzk, Networkshop 2003, forrás: http://splash.eik.bme.hu/papers/wlan.pdf)
3. Horváth T.: *„WLAN hálózatok a támadó szemszögéből”*
(HUWICO, Hacktivity 2005 Konferencia, forrás:
http://hacktivity.hu/portal/archivum/folia/2005/wlan.pdf)

5. Függelék: rövidítések jegyzéke

AAAK – Authentication, Authorization and Accounting Key

ACL (Asynchronous Connectionless Link) – aszinkron kapcsolat nélküli link

ACO – Authenticated Ciphering Offset

AES – Advanced Encryption Standard

AP (Access Point) – hozzáférési pont

AR_ADDR (Access Request Address) – hozzáférés kérési cím

AS (Authentication Server) – hitelesítő szerver

AU_RAND (Authenticated Random) – hitelesített véletlen érték

BSS (Basic Service Set) – alapszolgáltatás készlet

BD_ADDR (Bluetooth Device Address) – Bluetooth eszköz fizikai címe

CBC-MAC – Cipher Block Chaining Message Authentication Code Protocol

CCMP – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CHAP – Challenge Handshake Authentication Protocol

CRC, CRC-32 – Cyclic Redundancy Check, Cyclic Redundancy Check 32 bit

DoS (Denial of Service) – szolgáltatás megtagadás

DS (Distribution System) – elosztó rendszer

DSSS (Direct Sequence Spread Spectrum) – közvetlen sorozatú szórt spektrum

EAP – Extensible Authentication Protocol

eSCO (Extended Synchronous Connection Oriented) – kibővített szinkron kapcsolatorientált (link)

ESS (Extended Service Set) – kiterjesztett szolgáltatáskészlet

FEC (Forward Error Correction) – előremutató hibajavítás

FHSS (Frequency Hopping Spread Spectrum) – frekvenciaugrásos szórt spektrum

GTK (Group Temporal Key) – csoportszintű ideiglenes kulcs

HCI – Host Controller Interface

HIPERLAN – High Performance Radio Local Area Network

HMAC – Hash-based Message Authentication Code

IBSS (Independent Basic Service Set) – független alapszolgáltatás készlet

ICV (Integrity Check Value) – integritás ellenőrzési érték

ISM – Industrial, Scientific and Medical

IV (Initialization Vector) – inicializáló vektor

KGD (Key Generation and Distribution) – kulcs generálás és kiosztás

L2CAP – Logical Link Control and Adaptation Protocol

LAP – Link Access Protocol

LFSR (Linear Feedback Shift Register) – lineáris visszacsatolású shift-regiszter

LM-IAS – Link Management Information Access Service

LM-MUX – Link Management Multiplexer

LMP – Link Manager Protocol

LT_ADDR – Logical Transport Address

MAC (Medium Access Control) – közeghozzáférés-vezérlés

MAC (Message Authentication Code) – üzenet hitelesítési kód

MIC (Message Integrity Code) – üzenet integritási hitelesítő kód

MIMO – Multiple Input - Multiple Output

MSK – Master Session Key

MTU (Maximum Transmission Unit) – maximális átviteli egység

NFC – Near Field Communication

OBEX – Object Exchange Protocol

OFDM (Orthogonal Frequency Division Multiplexing) – ortogonális frekvenciaosztásos multiplexelés

OOB – Out of Band

OPP – Object Push Profile

OTP – One Time Password

PAP – Password Authentication Protocol

PHY (Physical Layer) – fizikai réteg

PIN (Personal Identification Number) – személy azonosító szám

PM_ADDR (Parked Mode Address) – park üzemmód cím

PMK (Pairwise Master Key) – páronkénti mester kulcs

PPP (Point-to-Point Protocol) – Pont-Pont Protokoll

PSK (Pre-shared Key) – előre kiosztott kulcs

PTK (Pairwise Transient Key) – páronkénti átmeneti kulcs

QoS (Quality of Service) – szolgáltatás-minőség biztosítás

RADIUS – Remote Authentication Dial In User Service

RC4 – Rivest Cipher 4

RSN – Robust Security Network

RSNA – Robust Security Network Association

SCO (Synchronous Connection Oriented) – szinkron kapcsolatorientált (link)

SDP - Service Discovery Protocol

SM 1, 2, 3, 4 – Security mode 1, 2, 3, 4

SSID – Service Set Identifier

SSP (Secure Simple Pairing) – biztonságos egyszerű párosítás

STA (Station) – állomás

TDM (Time Division Multiplexing) – időosztásos multiplexelés

TKIP - Temporal Key Integrity Protocol

TSN (Transition Security Network) – átmeneti biztonsági hálózat

UNII – Unlicensed National Information Infrastructure

WEP – Wired Equivalent Privacy

WLAN (Wireless Local Area Network) – vezeték nélküli lokális hálózat

WPA – Wi-Fi Protected Access

WPA2 – Wi-Fi Protected Access 2

WPAN (Wireless Personal Area Network) – vezeték nélküli személyi hálózat

Ezúton is szeretnék köszönetet mondani témavezetőmnek, Dr. Krausz Tamásnak a diplomamunkám elkészítéséhez nyújtott támogatásáért és bizalmáért és Dr. Huszti Andreának, aki a kriptográfiai protokollokkal kapcsolatos szakmai észrevételeivel és tanácsaival segítette munkámat.