Primerjava varnostnih mehanizmov brezžičnih tehnologij Bluetooth in Wireless LAN 802.11 WPA

Marko Hölbl, Boštjan Brumen, Tatjana Welzer
Fakulteta za elektrotehniko, računalništvo in informatiko, Univerza v Mariboru, Smetanova 17, 2000 Maribor
{marko.holbl, bostjan.brumen, welzer}@uni-mb.si

Povzetek

Brezžične tehnologije se vedno bolj uveljavljajo in izpodrivajo klasične kabelske povezave. Vedno večji pomen pridobiva področje mobilnih aplikacij v informatiki in s tem tudi brezžične tehnologije. Mednje sodita tudi tehnologiji Bluetooth in Wireless LAN (WLAN) družine standardov IEEE 802.11. Bluetooth je vodilna brezžična tehnologija na področju mobilnih aplikacij, WLAN pa predstavlja alternativno obliko povezovanja računalniških omrežij in informacijskih sistemov. Pomemben vidik brezžičnega povezovanja je zagotavljanje varnosti. Tehnologiji implementirata varnostne mehanizme, tj. overjanje in šifriranje podatkov. V članku analiziramo varnostne mehanizme obeh tehnologij in ju primerjamo s stališča varnostnih mehanizmov. Kriterije smo določili na podlagi varnostnih načel (zaupnost, overjanje in celovitost). Potem smo po zastavljenih kriterijih primerjali obe tehnologiji. Bluetooth ima višjo stopnjo varnosti in bolj izpopolnjen mehanizem varnosti, vendar tudi WLAN WPA ne zaostaja veliko.

Abstract

Comparison of security mechanisms of Bluetooth and Wireless LAN 802.11 WPA

Wireless technologies are establishing their role in the market and are replacing classical cable connections. Mobile application and wireless connection technologies are gaining a significant role in modern IT. The two wireless technologies Bluetooth and Wireless LAN (WLAN) belong to the family of standards IEEE 802.11. Bluetooth is the leading wireless technology from the field of mobile applications, whereas WLAN is an alternative technology for connecting computer networks and information systems. An important aspect of wireless connectivity is security assurance. Both technologies implement security mechanisms, e.g. authentication and encryption. This paper deals with the analysis and comparison of WLAN WPA with Bluetooth (from the security mechanisms perspective). We have defined certain criteria on the basis of the security principles (confidentiality, authentication and integrity). We conducted a comparison of security mechanisms on the basis of the above criteria. Bluetooth offers a higher security level and more improved security mechanisms. Nevertheless, WLAN WPA does not fall behind.

1 Uvod

V sodobnem svetu smo priča razmahu brezžičnega povezovanja različnih naprav – od računalnikov do mobilnih telefonov. Množica tehnologij brezžičnega povezovanja nadomešča žično povezovanje. Mednje sodijo tehnologije kot so Bluetooth, Wireless LAN (angl. Local Area Network) ali tehnologije podatkovnega prenosa prek GSM omrežij (GPRS, EDGE ipd.). Ker je medij, po katerem se prenašajo podatki, prosto dostopen, moramo biti pozorni na varnostne vidike prenosa. Brezžično povezovanje se uveljavlja tudi na področju mobilnih aplikacij in informacijskih sistemov. V članku bomo analizirali varnostne mehanizme tehnologije Bluetooth (Bluetooth specifikacija 1.2) [3] in Wireless LAN z varovalnim mehanizmom WPA (angl. WI-Fi Protected Access) [6]. Pod terminom Wireless LAN (WLAN) razumemo brezžično tehnologijo za povezovanje družine standardov IEEE 802.11. Na podlagi izbranih primerjalnih kriterijev bomo primerjali varnostne mehanizme obeh tehnologij. Pri tem se bomo omejili na varnostne mehanizme specifikacije Bluetooth 1.2 in specifikacije WLAN WPA, ki je namenjen zaščiti povezav WLAN. Pri tehnologiji WLAN je tudi moč zaslediti nove standarde varovanja kot sta WPA2 oz. standard 802.11i, vendar je WPA najbolj razširjen in široko podprt od proizvajalcev brezžične mrežne opreme.

Tehnologija WPA omogoča dva načina delovanja glede na področje uporabe:

- varovanje v srednjih in velikih organizacijah ter
- varovanje v domačih brezžičnih omrežjih in malih podjetjih.

Za vsako področje uporabe so definirani drugi načini oz. mehanizmi varovanja. V prvem primeru uporabljamo standard 802.1X in strežnike RADIUS, ki so namenjeni overjanju in upravljanju s ključi. V drugem primeru pa se uporablja način PSK (angl. Pre-Shared

Key). V okviru slednjega uporabnik ročno vnese vnaprej definiran ključ v vse mrežne naprave. Ker je področje uporabe Bluetootha primerljivo s področjem uporabe WLAN v domačih okoljih in malih podjetjih, bomo izvedli primerjavo varnostnih mehanizmov tehnologije Bluetooth po specifikaciji 1.2 in varovanje WLAN WPA v načinu PSK.

Kljub temu, da je bila pred kratkim sprejeta specifikacija Bluetooth 2.0 [4], le-ta ne bo zajeta v članku, saj definira enake varnostne mehanizme kot specifikacija 1.2.

Članek ne obravnava tehnologij za prenos podatkov po omrežjih GSM oz. UMTS, saj so tehnologije in njihovi varnostni vidiki vezani na infrastrukturo omrežja in dejavnost operaterja. Prav tako nista namenjeni povezovanju naprav v domačih oz. poslovnih okoljih.

Članek je razdeljen v pet delov. Uvodu, v katerem je opisana metodologija, ki jo bomo kasneje uporabili za primerjavo, sledi obravnava tehnologij Bluetooth in WLAN ter primerjava varnostnih mehanizmov.

1.1 Metodologija

Zaradi boljšega pregleda in razumljivosti varnostnih mehanizmov obeh tehnologij bomo naredili kratek splošen pregled tehnologije Bluetooth in WLAN, nato se bomo osredinili na varnostne mehanizme, ki jih posamezna tehnologija vsebuje.

Na področju varnostnih informacijsko-komunikacijskih tehnologij veljajo varnostni principi, ki jih želimo izpolniti [20]:

- overjanje (angl. Authentication),
- zaupnost (angl. Confidentiality),
- celovitost (angl. Integrity) in
- nezanikanje (angl. Non-repudiation).

Pri primerjanju bomo zajeli principe overjanja, celovitosti in zaupnosti. Princip ne-zanikanja bomo izpustili, saj se uporablja na višji komunikacijski ravni.

Primerjava kakovosti varnostne tehnologije je možna prek tehnologij, ki zagotavljajo izpolnjevanje določenega varnostnega principa. Zaupnost zagotavljamo s pomočjo šifriranja in ustreznih algoritmov. Zato bo del primerjave varnostnih mehanizmov primerjava šifrirnega algoritma in njegovih parametrov, ki vplivajo na raven zaščite. Pomemben parameter je dolžina ključa; daljši je ključ, manj verjetno je, da je mogoče izvesti napad z grobo silo (angl. Brute-force Attack) in tako pridobiti podatke. Kot primerjalni kriterij bomo definirali dolžino ključa. Kakovost posameznega algoritma vpliva na odpornost na različne napade. Algoritem ne sme vsebovati varnostnih lukenj, prek katerih je napadalcu omogočen nepooblaščen dostop do podatkov. Zato so drugi primerjalni kriterij morebitni obstoječi napadi ali druge pomanjkljivosti, ki so bile odkrite in objavljene. Tudi zelo kakovosten algoritem ne daje zaščite, če ga naprava ne uporablja. Zato bomo v sklop primerjave vključili kriterij o obveznosti uporabe šifriranja.

Overjanje je zagotavljanje verodostojnosti entitet, udeleženih v komunikaciji. Tudi v primeru overjanja se uporabljajo algoritmi za overjanje in pripadajoči ključi. Kakor pri šifriranju podatkov lahko tudi kakovost overjanja določimo s pomočjo dolžine ključa, karakteristik algoritma (odpornost na napade, varnostne luknje) in obveznosti uporabe overjanja.

Tretji princip, celovitost, zagotavlja, da spreminjanje podatkov ne ostane neopaženo. Če torej napadalec spremeni podatke med prenosom, je to mogoče zaznati. Primerjali bomo algoritme, ki jih oba standarda predvidevata za zagotavljanje celovitosti – ali so znane pomanjkljivost oz. varnostne luknje. Tudi pri tem principu bo kriterij obveznost uporabe tehnologij za zagotavljanje celovitosti.

Za zagotavljanje varnosti je pomembno opredeliti, ali se za overjanje, šifriranje in zagotavljanje celovitosti uporabljajo različni ključi. S tem ko uporabljamo različne ključe pri šifrirnih oz. overitvenih algoritmih, lahko zagotovimo višjo raven varnosti, saj ob pridobitvi enega izmed ključev ne moremo zaobiti vseh mehanizmov varovanja.

Zadnji primerjalni kriterij, ki ga bomo uporabili, so karakteristike gesel/skupnih skrivnosti in postopek generiranja ključev iz gesel. Obravnavali bomo postopke za generiranje ključev na podlagi gesel.

Tabela 1: **Primerjalni kriteriji**

#	Primerjalni kriterij
1.	Razlikovanje med ključi za šifriranje in overjanje
2.	Dolžina ključa
3.	Karakteristike gesel/skupnih skrivnosti
4.	Pomanjkljivost in luknje v uporabljenih algoritmih
5.	Obveznost uporabe overjanja
6.	Obveznost uporabe šifriranja
7.	Obveznost uporabe zagotavljanja celovitosti

Zaradi težavnosti shranjevanja in pomnjenja dolgih ključev tehnologiji nudita mehanizem, ki s pomočjo gesla generira ključ. Ker pomembno vpliva na raven varnosti, ga bomo uporabili za primerjalni kriterij.

V tabeli 1 so strnjeni vsi primerjalni kriteriji, ki jih bomo uporabili.

Za boljšo preglednost bomo strnili ugotovitve v tabelo in na podlagi rezultatov primerjave podali ugotovitve glede ravni varnosti obeh tehnologij.

V nadaljevanju si bomo ogledali tehnologijo Bluetooth in njene varnostne mehanizme.

2 Tehnologija Bluetooth

Bluetooth je tehnologija, ki je bila zasnovana z namenom povezovanja perifernih naprav, mobilnih telefonov, prenosnikov in drugih mobilnih naprav. Za tehnologijo skrbi skupina Bluetooth SIG (Special Interest Group) [1], [14].

Leta 1999 je bila sprejeta prva verzija specifikacije Bluetooth 1.0B. Sledila je vpeljava specifikacije 1.1 [2] in kasneje še 1.2 [3]. Večina današnjih naprav s podporo tehnologiji Bluetooth uporablja specifikacijo 1.2. Nedavno pa je bila sprejeta tudi specifikacija 2.0 [4]. Tehnologija se uporablja za povezovanje različnih brezžičnih naprav. Veliko novejših prenosnih računalnikov je opremljenih s potrebno strojno in programsko opremo za povezovanje s pomočjo Bluetootha.

Bluetooth naprave lahko kategoriziramo na različne načine. Na podlagi porabe električne energije in dosega jih kategoriziramo v tri razrede [5]:

- 3. razred – naprave z močjo signala 1 mW in dosegom od 0.1 do 10 m,
- 2. razred – naprave z močjo signala 1 do 2.5 mW in dosegom 10 m in
- 1. razred – naprave z močjo 100 mW in dosegom do 100 m.

Naprave komunicirajo v frekvenčnem pasu 2.45 GHz in imajo največjo prepustnost 1,4 Mb/s. Zaradi dodatnih storitev, ki so potrebne za vzpostavitev in nadzor povezave in se prenašajo skupaj s podatki prek brezžične povezave, je dejanska prepustnost manjša. Bluetooth naprave se povezujejo v omrežja, ki jih imenujemo piconet. V piconet je lahko povezanih do osem naprav, izmed katerih je ena glavna (angl. Master Device), druge pa so odvisne (angl. Slave Device).

Glede na varnostne mehanizme naprave uvrščamo v tri načine [5]:

- varnostni način 1 (angl. No-security) – naprave se povezujejo in nikoli ne zahtevajo uporabe varnostnih mehanizmov (overjanja in šifriranja);
- varnostni način 2 (angl. Service Level Enforced Security) – naprave, ki se povezujejo v tem načinu vzpostavijo varnostne mehanizme na ravni kanala (naloga je prepuščena višjim ravnem komunikacijskega protokola ali aplikacijam);
- varnostni način 3 (angl. Link Level Enforced Security). Varnostni mehanizmi se vzpostavijo pred vzpostavitvijo povezave. Možni sta dve različni varnostni politiki: vedno zahtevaj overjanje in vedno zahtevaj overjanje in šifriranje.

Razlika med drugim in tretjim načinom je v tem, da pri varnostnem načinu 3 naprave Bluetooth inicializirajo varnostne mehanizme pred vzpostavitvijo povezave. Varnost prenosa je prepuščena Bluetoothu. V varnostnem načinu 2 je varovanje predano višji ravni, ki mora poskrbeti zanj.

Vzpostavitev komunikacijskega kanala med dvema napravama imenujemo vzpostavitev povezave (angl. Pairing). Razlikujemo dva scenarija:

- vzpostavitev povezave med dvema napravama poteka prvič,
- ponovna vzpostavitev povezave dveh naprav (ki sta že vzpostavili povezavo).

Ker je Bluetooth brezžična tehnologija, so pomemben del specifikacije tudi varnostni mehanizmi, ki jih bomo opisali v nadaljevanju. Obravnavali bomo ključe, ki jih definira Bluetooth pri svojih varnostnih mehanizmih in postopke overjanja ter šifriranje.

2.1 Varnostni mehanizmi

2.1.1 Ključi

Varnostni koncept tehnologije Bluetooth vključuje ključe, ki se uporabljajo pri overjanju in šifriranju. Specifikacija definira dve vrsti ključev:

- ključi povezave (angl. Link Key),
- šifrirni ključ (angl. Encryption Key).

Vlogo ključa povezave lahko prevzamejo različni ključi. Ključ povezave se ne uporablja samo pri overjanju, ampak tudi za generiranje šifrirnega ključa. Napravi si izmenjata ključ povezave v procesu vzpostavitve povezave.

Šifrirni ključ, ki je izpeljan iz ključa povezave, uporabljamo za šifriranje podatkov pri prenosu. Po specifikaciji [3] se šifrira samo vsebina paketov (angl. Payload), ne pa tudi režijski podatki (angl. Overhead

data). Pri generiranju ključev se uporablja naslov Bluetooth naprave (angl. Bluetooth Device Address), ki je izviren za vsako napravo.

Ključi povezave

Ključ povezave je rezultat vzpostavitve povezave. Specifikacija predvideva dva tipa ključev glede na trajnost [11]:

- poltrajni ključ (angl. Semi-permanent Key) in
- začasni ključ (angl. Temporary Key).

Med poltrajne ključe povezave prištevamo [3]:

- ključ naprave (angl. Unit Key) in
- kombinacijski ključ (angl. Combination Key).

Prav tako razlikujemo dva tipa začasnih ključev [3]:

- glavni ključ (angl. Master Key) in
- vzpostavitveni ključ (angl. Initialization Key).

Inicializacijski ključ se uporablja za vzpostavitev komunikacije med napravami in obstaja samo za čas vzpostavljanja povezave. Pri vzpostavitvi povezave se v napravi, ki se povezuje, vnese geslo (PIN). Inicializacijski ključ se generira po naslednji enačbi:

$$K_{vzp} = geslo, l_{gesla}, RAND, BD\_ADDR,$$

pri čemer je *PIN* (angl. Personal Identification Number) geslo, l_{gesla} dolžina gesla, *RAND* 128-bitno naključno število in *BD_ADDR* 128-bitni naslov Bluetooth naprave. Parametra geslo in l_{gesla} pridobimo na naslednji način:

$$geslo' = \begin{cases} geslo \cup BD\_ADDR & l_{gesla} \leq 10 \\ geslo \cup BD\_ADDR[0...(15-L)] & 10 < l_{gesla} \leq 15 \\ geslo & l_{gesla} = 16 \end{cases}$$

$$l_{gesla}' = \min(l_{gesla} + 6,16)$$

$\cup$ označuje konkatenacijo dveh nizov. Če je dolžina gesla krajša od 16 zlogov, se izvede bitno zapolnjevanje (angl. Padding) po zgornjem postopku. Inicializacijski ključ se uporablja za izmenjavo drugih ključev povezave.

Ključ naprave nastopa v vlogi ključa povezave in ga kreira naprava samo pri povezovanju z drugimi napravami. Zato je ključ naprave poznan množici naprav. Generira se s pomočjo algoritma E21 ob namestitvi nove naprave:

$K_A = E_{22}$ *(RAND, BD_ADDR)*, pri čemer je *RAND* 128-bitno naključno število in *BD_ADDR* 128-bitni naslov Bluetooth naprave. Med vzpostavljanjem povezave se napravi dogovorita, kateri ključ naprave se bo uporabljal. Ponavadi se uporablja ključ naprave, ki ima manjše pomnilniške kapacitete. Po generiranju se ključ naprave ne prenese neposredno na drugo napravo, marveč se uporabi operacija XOR $K'_A = K_A \oplus K_{vzp}$

Prejemnik lahko pridobi prvotni ključ s pomočjo naslednje enačbe:

$$ključ\_enote'_A \oplus vzpostitve\_ključ =$$
$$= ključ\_enote'_A \oplus vzpostitve\_ključ \oplus vzpostitve\_ključ =$$
$$= ključ\_enote'_A$$

Ključ naprave je varen, če obstaja zaupanje med napravami, ki se povezujejo. Slabost pristopa je možnost, da lahko vsaka naprava, ki ima isti ključ naprave, pooseblja drugo napravo. Specifikacija Bluetooth 1.2 uporabo ključa naprave odsvetuje, vendar zaradi kompatibilnosti za nazaj, ta tip ključev še ni bil odstranjen iz specifikacije.

Kombinacijski ključ se kreira s pomočjo dveh naprav. Za razliko od ključa naprave je ta ključ poznan samo napravama, ki sta ga kreirali. Daje visoko stopnjo varnosti, njegova slabost pa je potreba po pomnilniku, saj mora naprava shraniti kombinacijski ključ za vsako napravo, s katero se povezuje.

Kombinacijski ključ za napravi A in B se generira s pomočjo algoritma E21.

$K_A = E_{21}$ *(*$RAND_A$*,* BD_ADDR_A*)* in
$K_B = E_{21}$ *(*$RAND_B$*,* BD_ADDR_B*)*

Skupni, torej kombinacijski ključ K_{AB}, se izračuna kot $K_{AB} = K_A \oplus K_B$. Seveda je treba pred združevanjem ključev poskrbeti za prenos ključa K_A k napravi B in ključa K_B k napravi A. Ker je postopek prenosa zapleten, lahko bralec podrobnosti prouči v [3], [5].

Prvi začasni ključ povezave je glavni ključ, ki ga kreira glavna naprava pri vzpostavljanju šifrirane povezave z več odvisnimi napravami. Uporablja se za prenos podatkov med odvisno napravo in glavno napravo. Ključ generira glavna naprava s pomočjo algoritma E22:

$K_G = (RAND1, RAND2)$, kjer sta *RAND1* in *RAND2* dve naključi števili. Glavni ključ se na odvisno napravo ne prenese neposredno, ampak odvisni napravi pošlje tretje (javno znano) naključno število RAND3 in $K_{AB} = K_{glavni} \oplus K_{izr}$, pri čemer je K_{AB} kombinacijski ključ, K_{izr} pa izračunamo po naslednjem postopku:

$K_{izr} = E_{22}$ *(K,RAND3,16)*; *K* je trenutni ključ povezave. Odvisna naprava, ki pozna *K* in *RAND3* lahko izračuna glavni ključ kot:

$K_{AB} \oplus E_{22}(K,RAND3,16)$
$= K_{AB} \oplus K_{izr}$
$= K_{glavni} \oplus K_{izr} \oplus K_{izr}$
$= K_{glavni}$

Proceduro je treba opraviti za glavno napravo in vse odvisne naprave, ki se povezujejo z njo.

Šifrirni ključi

Ob ključih povezave predvideva specifikacija Bluetooth tudi tri šifrirne ključe [3]:

- šifrirni ključ K_c (angl. Encrpytion Key),
- omejeni šifrirni ključ (angl. Constrained Encryption Key) in
- ključ vsebine K_p (angl. Payload Key).

Ker je lahko šifrirni ključ daljši od dogovorjene maksimalne dolžine, se ga ne uporablja neposredno. Namesto njega se uporablja omejeni šifrirni ključ, ki je lahko dolg 8 do 128 bitov. Pomembno je omeniti, da ni priporočljivo uporabljati ključev z dolžino manj kot 128 bitov. Krajše dolžine ključev so bile predvidene zaradi omejitev izvoza kriptografije v nekaterih državah. Omejeni šifrirni ključ pridobimo s pomočjo šifrirnega ključa K_c, ključ vsebine K_p pa pridobimo s pomočjo omejenega šifrirnega ključa K_c.

Šifrirni ključ je izpeljan iz ključa povezave in se generira s pomočjo algoritma E_3 na naslednji način:

$K_c = E_3(K_{pov}, COF, RAND)$;

COF (angl. Cipher Offset Number) je nadomestno šifrirno število, E_3 je naključno število in K_{pov} je ključ povezave. *COF* izračunamo kot [3]:

$$COF = \begin{cases} naslov\_naprave \parallel naslov\_naprave \\ \\ ACO \end{cases}$$

Prvi primer velja le, če je ključ povezave enak glavnemu ključu, drugi pa v ostalih primerih. ACO (angl. Authentication Ciphering Offset) je število, ki ga pridobimo v fazi overjanja, ki jo bomo obravnavali v naslednjem razdelku.

Novejše verzije specifikacije ne priporočajo uporabe omejenega šifrirnega ključa oz. priporočajo, da je dolžina omejenega šifrirnega ključa 128 bitov.

Za šifriranje in dešifriranje podatkov se uporablja ključ vsebine K_p, ki ga pridobimo s pomočjo omejenega šifrirnega ključa:

$K_p = E_0(K_c, CLK, RAND, DB\_ADDR)$

K'_c je omejeni šifrirni ključ, *CLK* je 26 bitov trenutne ure naprave, *RAND* je 128-bitno naključno število in *DB_ADDR* je 128-bitni naslov Bluetooth naprave.

V tabeli 2 je pregled vseh ključev, ki jih predvideva specifikacija Bluetooth.

Tabela 2: **Pregled ključev specifikacije Bluetooth**

Namen	Poltrajni	Začasni
Overjanje	▪ Ključ enote ▪ Kombinacijski ključ	▪ Vzpostavitveni ključ ▪ Glavni ključ
Šifriranje		▪ Šifrirni ključ ▪ Omejeni šifrirni ključ ▪ Ključ vsebine

2.2 Overjanje

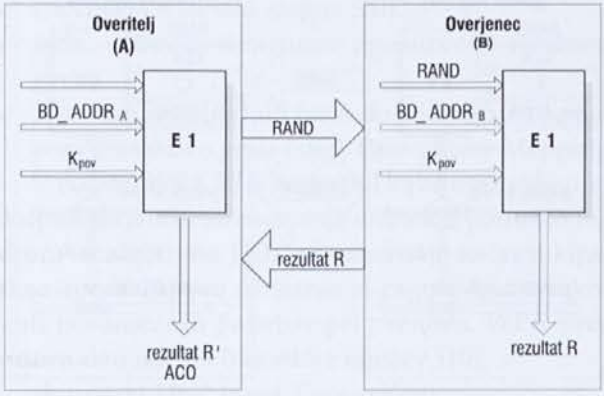
Varnost tehnologije Bluetooth je sestavljena iz dveh delov, ki sta med seboj povezana. Prvi del, ključi, je bil podrobneje obravnavan v prejšnjem razdelku. Drugi del je postopek overjanja in šifriranja. Uspešen zaključek overjanja entitet v komunikaciji je pogoj za uporabo šifriranja.

Overjanje poteka enosmerno, torej ena stran overja drugo ali obratno – ena entiteta v postopku nastopa kot overitelj in druga kot overjenec. Vloge dodeli uporabnik oz. gostitelj pred začetkom postopka overjanja. Slika 1 prikazuje postopke overjanja, kjer je naprava A overitelj in naprava B overjenec.

Najprej stran, ki želi overiti drugo stran, tej pošlje naključno število *RAND*. Algoritem *E1* sprejme naslednje parametre:

- 128-bitno naključno število *RAND*,
- 128-bitna naslova Bluetooth naprav BD_ADDR_A in BD_ADDR_B ter
- ključe povezave K_{pov}.

S pomočjo teh parametrov in algortima *E1* napravi izračunata števili R' (overitelj) in *R* (overjenec). Nato overitelj pošlje število *R* overjencu. Overitelj primerja *R'* z *R*.



Slika 1: **Postopek overjanja pri Bluetoothu**

Če se ujemata ($R = R'$), je postopek overjanja uspel, drugače ne. V primeru, da je postopek overjanja uspel, se izvrši še postopek overjanja v nasprotno smer – vlogi overitelja in overjanca se zamenjata. Naključno število se pri ponovnem overjanju zamenja.

Poleg overitev naprav je rezultat postopka overjanja tudi t. i. *ACO*, ki se uporablja pri generiranju šifrirnega ključa. Vrednost *ACO* se generira sočasno z vrednostjo *R*. Podrobnosti v zvezi z algoritmom *E1* in generiranje *ACO* so v [3], [5].

2.3 Šifriranje podatkov in zagotavljanje celovitosti

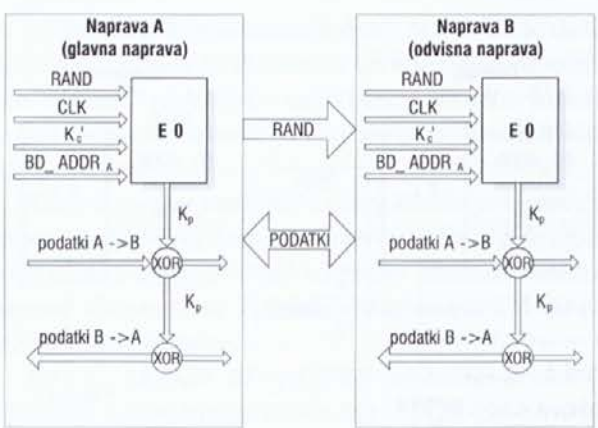
Šifriranje podatkov zagotavlja zaupnost prenesenih podatkov. Ob uporabi šifriranja se ključ samodejno generira. Ob ponovni vzpostavitvi povezave se šifrirni ključ zamenja. Podrobnosti delovanja postopka šifriranja prikazuje slika 2.

Šifriranje poteka s pomočjo algoritma E0 in parametrov [3]:

- 128-bitnega naslova glavne naprave Bluetooth *BD_ADDR*,
- 8–128-bitnega omejenega šifrirnega ključa K_c',
- 128-bitnega naključnega števila *RAND* in
- časovne značke naprave *CLK*.

Algoritem *E0* generira binarni niz ključev (angl. Binary Keystream), ki se po modulu 2 dodajo podatkom (operacija *XOR*). Šifrirani podatki se nato prenesejo k napravi B. Dešifriranje podatkov poteka po enakem postopku [5].

Tehnologija Bluetooth ne vsebuje mehanizma za zagotavljanje celovitosti s stališča varnostnih principov (s pomočjo ključa). Zagotavljanje celovitosti glave poslanega paketa je realizirano s pomočjo kontrolnika napak glave (angl. Header-Error-Check) HEC, ki je velikosti 8 bitov [3]. Vsak paket vsebuje tudi vrednosti CRC (angl. Cyclic Redundancy Check) za zaznavanje napak [3]. Kljub temu pa mehanizma nista namenjena zagotavljanju celovitosti s stališča varnosti, saj samo preverjata, ali je prišlo do napake v paketu, ki je posledica motenj pri prenosu. Prav tako mehanizem zagotavljanja celovitosti ni vezan na ključ. Če pride do napake, je treba paket poslati ponovno.



Slika 2: **Šifriranje pri Bluetoothu**

Bluetooth ni edina tehnologija za brezžično povezovanje. V nadaljevanju bomo obravnavali tehnologijo WLAN, ki je prav tako namenjena brezžičnemu povezovanju.

3 Tehnologija Wireless LAN

Tehnologija Wireless LAN je namenjena povezovanju naprav v omrežja. Nadomešča žična lokalna omrežja (angl. Wired Local Area Network). Kratica WLAN označuje družino standardov IEEE 802.11. Tehnologija je trenutno v velikem razvoju, saj močno olajša vzpostavitev lokalnih omrežij. Uporablja frekvenčni pas 2.4 GHz (IEEE 802.11, IEEE 802.11b, IEEE 802.11g) in 5 Ghz (IEEE 802.11a). Maksimalni prenos variira od 1 Mbit/s (IEEE 802.11) do 54 Mbit/s (IEEE 802.11a in g).

V skupini 802.11 so ključni naslednji standardi [10]:

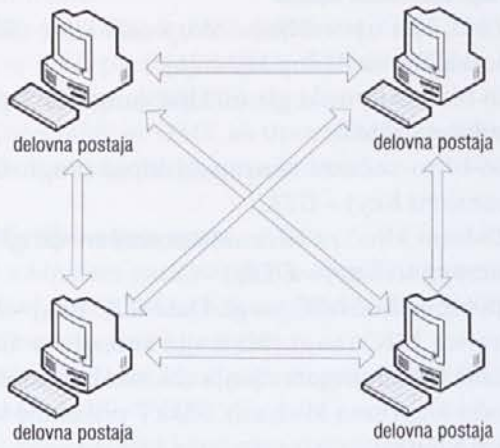
- 802.11 – prvotni standard, ki omogoča prenos podatkov 1 oz. 2 Mbit/s, frekvenčni pas 2.4 GHz, sprejet leta 1999,
- 802.11a – omogoča prenos do 54 Mbit/s, frekvenčni pas 5 Ghz, sprejet leta 1999,
- 802.11b – omogoča prenos do 11 Mbit/s, frekvenčni pas 2.4 Ghz, sprejet leta 1999,
- 802.11d – spremembe, potrebne zaradi omejitev v nekaterih državah,
- 802.11e – nadgraditev ravni *MAC* za zagotovitev storitev kakovosti (angl. Quality of Service),
- 802.11h – spremembe, potrebne zaradi omejitev v Evropi,
- 802.11i – definira dodatne varnostne mehanizme.

Tehnologija WLAN omogoča postavitev dveh tipov omrežij [10]:

- začasna omrežja (angl. Ad-hoc Network),
- infrastrukturna omrežja (angl. Infrastucture Network).

Večina omrežij WLAN je infrastrukturnega tipa (angl. Infrastucture Network). Druga vrsta omrežij so začasna omrežja (angl. Ad-hoc Network), pri katerih ne potrebujemo dostopnih točk (angl. Access Point).

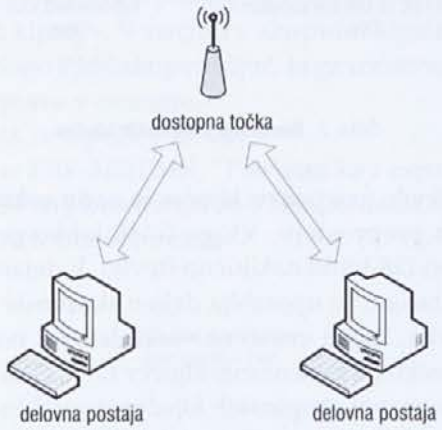
Arhitektura omrežja je bistveno preprostejša, saj ne vsebuje dodatnih omrežnih naprav, ampak samo delovne postaje, ki se povezujejo. Vsaka delovna postaja v omrežju neposredno komunicira z drugimi delovnimi postajami (slika 3).



Slika 3: **Struktura začasnega omrežja**

Varnost v začasnih omrežjih je na nizki ravni; omrežja namreč niso trajna in zato ni potrebe po varnosti.

Drugi tip omrežij so infrastrukturna omrežja, kjer potrebujemo dodatne omrežne naprave, imenovane dostopne točke. Vsaka delovna postaja komunicira z drugo postajo prek dostopne točke (slika 4).



Slika 4: **Shema infrastrukturnega omrežja**

Dostopna točka poskrbi, da se podatkovni paketi ustrezno usmerjajo proti distribucijskemu sistemu (angl. Distribution System), npr. usmerjevalniku.

Vsako omrežje vsebuje identifikacijo množice storitev SSID (angl. Service Set Indentifier), ki ga imenujemo tudi ime omrežja. Namen SSID je identifikacija podatkov glede na omrežje, tj. kateri podatki pripadajo kateremu omrežju.

Ker je medij, po katerem se prenašajo podatki zrak, je treba v omrežjih WLAN poskrbeti tudi za varnost. V nadaljevanju si bomo ogledali vse dejavnike, ki so povezani z varnostjo pri tehnologiji WLAN.

3.1 Varnostni mehanizmi

Analizirali bomo tehnologijo, imenovano WPA (angl. Wi-Fi Protected Access), v načinu PSK (angl. Preshared Key). Standard vsebuje protokol TKIP (angl. Temporal Key Integrity Protocol) za šifriranje podatkov in algoritem Michael za preverjanje celovitosti. WPA je bil vpeljan kot okrnjena različica standarda IEEE 802.11i. Namen WPA je bil povečati raven varnosti in hkrati omogočiti, da se rešitev vpelje samo s programsko nadgraditvijo obstoječih naprav. Zato je WPA samo začasna rešitev, ki jo bo kasneje nadomestil standard IEEE 802.11i, znan pod imenom WPA2 [6].

3.2 Ključi

Varnostni mehanizem WPA v načinu WPA-PSK uporablja t. i. skupni ključ. Skupni ključ se generira na podlagi gesla, saj bi bilo za uporabnika težko, da bi si zapomnil 256 bitov dolgo geslo. V ta namen se uporablja mehanizem, ki uporabnikovo geslo razširi v 256-bitni skupni ključ [9]:

PSK = PBKDF2(geslo, ssid, ssidLength, 4096, 256).

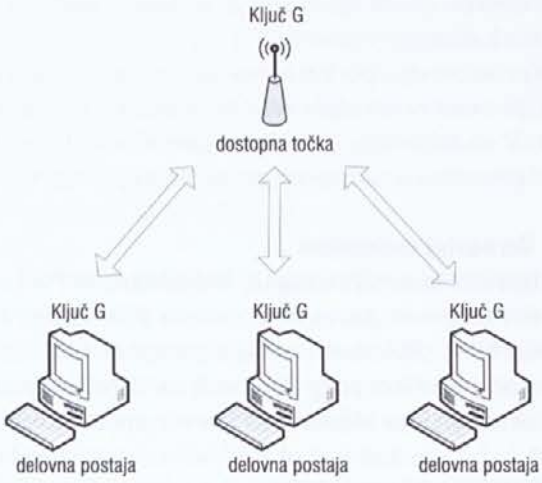
Pri čemer je:

- *geslo* – geslo, ki ga vnese uporabnik, sestavljeno iz ASCI znakov, dolžine 8 do 63 znakov,
- *ssid* – je SSID omrežja, v katerem se nahajajo naprave, zapisan v obliki zlogov,
- *ssidLength* – število zlogov SSID,
- *4096* – število izračunov zgostitvene vrednosti gesla,
- *256* – število izhodnih bitov, ki jih izračuna funkcija za preslikavo gesla (angl. Pass-phrase Mapping).

V načinu WPA PSK je skupni ključ uporabljen kot skupna skrivnost za overjanje entitet. S pomočjo tega ključa in algoritma TKIP se generirajo začasni ključi, ki se uporabljajo za šifriranje in zagotavljanje celovitosti posameznih paketov pri prenosu. WPA predvideva dva načina hierarhije ključev [10]:

- skupinski ključ (angl. Group Key),
- ključ para naprav (angl. Pairwise Key).

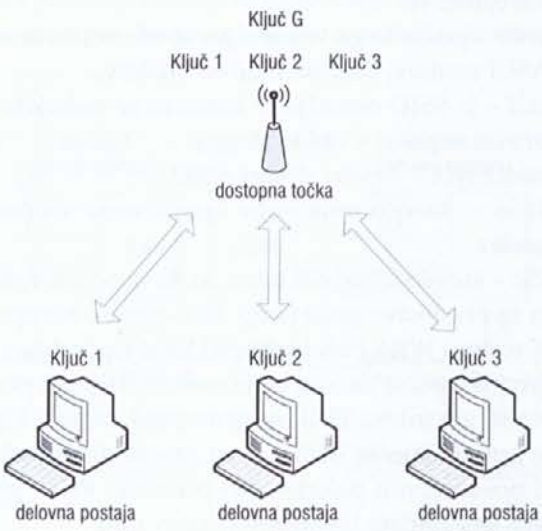
V prvem načinu uporabljajo vse delovne postaje in dostopna točka isto množico ključev (slika 5).



Slika 5: **WPA s skupinskim ključem**

Ta način je primeren za okolja, kjer razpršeno prenašamo podatke (angl. Broadcast). Način je bolj preprost s stališča upravljanja s ključi, a ne omogoča overjanja delovnih postaj, saj je skupni ključ naključno število. Skupinski ključ se v dejanskih implementacijah generira za tem, ko so že generirani posamezni ključi parov naprav.

V drugem načinu uporablja vsak par delovna postaja – dostopna točka različen ključ.



Slika 6: **WPA s ključi parov naprav**

Glede na način delovanja WPA definira več ključev. V nadaljevanju bomo obravnavali vse ključe, ki se uporabljajo v okviru varnostih specifikacij WPA.

Izpeljava ključev oz. vrste le-teh so odvisne od hierarhije ključev, ki jo uporabljamo.

Hierarhija skupinskih ključev

V načinu, kjer uporabljamo skupinski ključ (slika 6), se uporabljajo naslednji ključi [6]:

- 128-bitni skupinski glavni ključ (angl. Group Master Key) – *GMK*,
- 256-bitni začasni skupinski ključ (angl. Group Transient Key) – *GTK*,
- 128-bitni ključ za šifriranje podatkov (angl. Data Encryption Key) – *DEK*,
- 128-bitni ključ MIC (angl. Data *MIC* Key) – *DMK*.

Kratica MIC (angl. Message Intergirty Check) označuje termin zagotavljanja celovitosti podatkov (s pomočjo algoritma Michael). Slika 7 prikazuje hierarhijo teh ključev.

Slika 7: **Hierarhija skupinskih ključev**

Po številu in izpeljavi ključev je način s skupinskim ključem preprostejši. Vlogo *GMK* lahko prevzame poljubno 128-bitno naključno število. V dejanskih implementacijah se uporablja deljen skupinski ključ, ki ga je treba ročno vnesti na vsaki delovni postaji/dostopni točki. Za generiranje ključev *GTK, DEK* in *DMK* se pri hierarhiji skupinskih ključev uporablja *GMK*. S pomočjo *GTK* generiramo ostale tri ključe kot [9]:

GTK = PRF-256(GMK, "Group key expansion" || AA || GNonce),

pri čemer je:

- *PRF-256* generator psevdonaključnih števil, ki generira 256-bitno izhodno vrednost,

- *GMK* 128-bitni skupinski glavni ključ,
- *Group key expansion* niz znakov,
- *AA – MAC* naslov overitelja,
- *GNonce* naključno ali psevdonaključno število in
- || označuje konkatenacijo.

S pomočjo funkcije L lahko nato iz *GTK* pridobimo *DEK* in *DMK*:

DEK = L(GTK, 0, 128), DMK = L(GTK, 128, 256).

Torej je *DEK* prvih 128 bitov *GTK* (0–127) in *DMK* drugih 128 bitov (128–255).

Ključa *DEK* in *DMK* se uporabljata za šifriranje podatkov in zagotavljanje celovitosti.

Hierarhija ključev para naprav

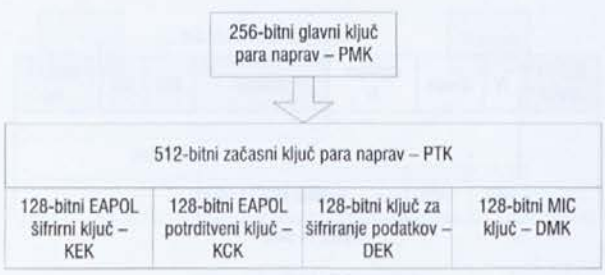
Način s ključem para naprav je s stališča generiranja in upravljanja ključev bolj zapleten (slika 6). Opravka imamo s šestimi ključi [10]:

- 256-bitni glavni ključ para naprav (angl. Pairwise Master Key) – *PMK*,
- 512-bitni začasni ključ para naprav (angl. Pairwise Transient Key) – *PTK*,
- 128-bitni EAPOL šifrirni ključ (angl. EAPOL Key Encryption Key) – *KEK*,
- 128-bitni EAPOL potrditveni ključ (angl. EAPOL Key Confirmation Key) – *KCK*,
- 128-bitni ključ za šifriranje podatkov (angl. Data Encryption Key) – *DEK*,
- 128-bitni *MIC* ključ (angl. Data *MIC* Key) – *DMK*.

Hierarhijo prikazuje slika 8. Zaradi dejstva, da se ključi v parih generirajo za vsaki dve napravi, ki se povezujeta (delovna postaja in dostopna točka), obstaja več ključev. V načinu s skupnim ključem prevzame vlogo *PMK* skupen ključ, ki ga ročno vnesemo v vse naprave v omrežju.

Iz *PMK* se izpelje *PTK* kot:

PTK = PRF-512(PMK, "Pairwise key expansion", Min(AA,SPA) || Max(AA,SPA) || Min(ANonce,SNonce) đđ Max(ANonce,SNonce)),



Slika 8: **Hierarhija ključev para naprav**

pri čemer je:

- *PRF-512* generator psevdonaključnih števil, ki generira 512-bitno izhodno vrednost,
- *PMK* 256-bitni glavni ključ para naprav,
- *Pairwise key expansion* niz znakov,
- *Min in Max* operacija, ki izbere minimalno oz. maksimalno vrednost izmed parametrov, tj. *AA* in *SPA* ter *ANonce* in *SNonce*,
- *AA – MAC* naslov overitelja,
- *SPA – MAC* naslov overjenca,
- ANonce – naključno ali psevdonaključno število overitelja in
- SNonce – naključno ali psevdonaključno število overjenca.

S pomočjo funkcije *L* lahko nato iz *PTK* pridobimo ostale štiri ključe [6], [10]:

KCK = L(PTK, 0, 128),
KEK = L(PTK, 128, 256),
DEK= L(PTK, 256, 384) in
DMK = L(PTK, 384, 512).

KCK je torej 0. do 127. bit, *KEK* 128. do 255. bit, *DEK* 256 do 383 bit in *DMK* 384 do 511 bit.

Ko se postopek izpeljave ključev zaključi, nadaljujemo s postopki overjanja, šifriranja in zagotavljanja celovitosti.

3.3 Overjanje

Overjanje je mehanizem, ki zagotavlja pristnost sistema ali osebe. WPA v načinu PSK predvideva dva načina overjanja [17], [16]:

- odprti sistemi (angl. Open Systems),
- skupni ključ (angl. Pre-shared Key).

Pri odprtih sistemih ni overjanja. Vsakdo lahko dostopa do sistema, saj dostopna točka vsaki omrežni napravi dovoli povezavo v omrežje. Zato tudi ni mogoče uporabljati šifriranja in zagotavljanja celovitosti.

Pri overjanju s skupnim ključem se v vsako delovno postajo in dostopno točko vnese skupni ključ. Overjanje poteka v štirih korakih, v katerih obe napravi druga drugi dokažeta, da poznata skupno skrivnost (skupni ključ). Overjanje poteka v obe smeri (angl. Mutual Authentication). V procesu overjenja se uporabljajo EAPOL sporočila in ključi, ki smo jih omenili v prejšnjem poglavju. Overjanje poteka po štirismernem protokolu. Najprej morata overitelj in overjenec generirati dve naključni števili. Vsaka stran generira svojo naključno vrednost:

- *ANonce* generira overitelj in
- *SNonce* generira overjenec.

Vrednosti *ANonce* in *SNonce* ne smeta biti povezani.

Nato sledi izmenjava štirih sporočil po štirismernem protokolu [10]:

1. Overitelj pošlje sporočilo A, ki vsebuje naključno število ANonce in *AA* (*MAC* naslov overitelja). Sporočilo je poslano nešifrirano in brez mehanizmov za zagotavljanje celovitosti. Po prejetju ima overjenec vse potrebne parametre za izračun *PTK*.
2. Overjenec pošlje sporočilo B, ki vsebuje naključno število SNonce, *SAP* (*MAC* naslov overjenca) in *MIC* za zagotavljanje celovitosti. Izračun *MIC* je mogoč, saj je overjenec v prejšnjem koraku generiral *PTK*. Overitelj uporabi SNonce in *SAP* za generiranje *PTK* in preverjanje vrednosti *MIC*.
3. Overitelj pošlje sporočilo C, ki vsebuje vrednost *MIC*, in začetno zaporedno število, ki označuje, da je overitelj pripravljen začeti s šifriranjem.
4. Overjenec pošlje sporočilo D, ki vsebuje vrednost *MIC* in začetno zaporedno število, ki označuje, da je overjenec pripravljen začeti s šifriranjem.

Celoten postopek je pregledno prikazan na sliki 9.

Po končani izmenjavi in overjanju sta obe strani pripravljeni za pošiljanje in sprejem šifriranih podatkov. Po končani vzpostavitvi hierarhije ključev para naprav je treba izvesti še distribucijo skupinskega ključa. Le-ta se uporablja za t. i. razpršeno pošiljanje podatkov po omrežju. Razpršeno pošiljanje je dovoljeno samo dostopni točki, vendar lahko vsaka delovna postaja »poda zahtevo« dostopni točki za razpršeno pošiljanje. Če želimo uporabljati tudi način skupinskega ključa, je treba še distribuirati skupinski ključ med vsemi delovnimi postajami. Ker je že vzpostavljen varen komunikacijski kanal (varovan s ključi parov naprav), je distribucija skupinskega ključa preprosta:

1. Generiramo *GTK*, s pomočjo katerega bomo generirali vse ostale začasne ključe.
2. Po vzpostavitvi varne povezave s pomočjo ključa para naprav:
   a) pošljemo *GTK* in trenutno zaporedno število vsaki delovni postaji,
   b) počakamo na potrdilo o prejemu.

Podrobnosti v zvezi s hierarhijami ključev, overjanjem in distribucijo ključev dajeta [9] in [10].

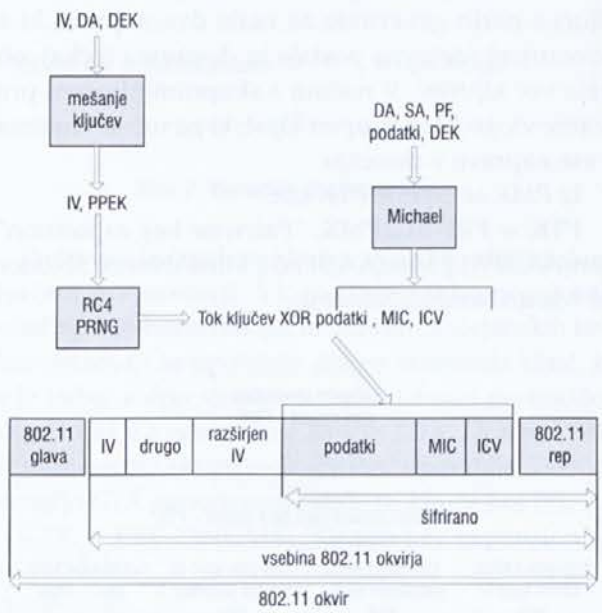
3.4 Šifriranje in zagotavljanje celovitosti

Za zagotavljanje zaupnosti WPA definira šifriranje podatkov. Šifrira se le dejanska vsebina. Potrebni so naslednji parametri za šifriranje:

1. 48-bitni inicializacijski vektor *IV* (angl. Initialization Vector), katerega začetna vrednost je 0 in se povečuje za vsak okvir,
2. *DEK* za šifriranje povezave,
3. naslov pošiljatelja *SA* (angl. Source Address) in naslov prejemnika *DA* (angl. Destination Address),
4. vrednost prednostnega polja *PF* (angl. Priority Field) z začetno vrednostjo 0,
5. *DMK* za zagotavljanje celovitosti.

Postopek šifriranja je prikazan na sliki 10:

Slika 9: **Štirismerni protokol za overjanje in izmenjavo začasnih ključev**

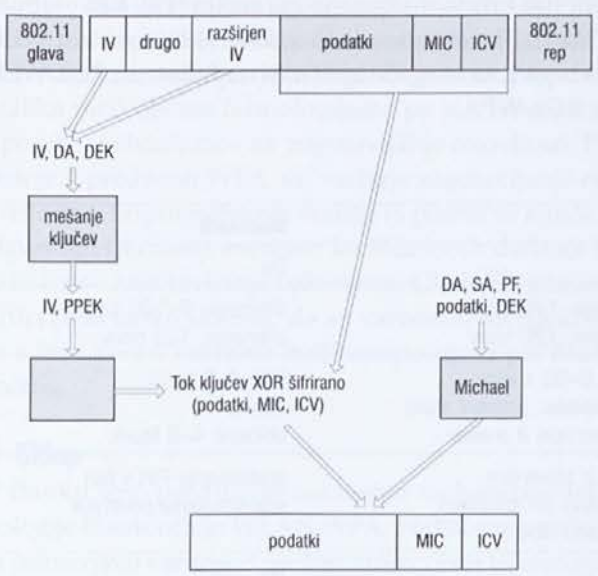


Slika 10: **WPA šifriranje**

1. IV, DA in DEK so vhodni parametri v funkcijo za mešanje ključev KMF (angl. Key Mixing Function), s pomočjo katere izračunamo šifrirne ključe za posamezen paket *PPK* (angl. Per-packet Key).
2. *DA, SA, PF*, podatki in *DMK* so vhodni parametri v algoritem za zagotavljanje celovitosti Michael, s pomočjo katerega izračunamo vrednost *MIC*.
3. Vrednost za preverjanje celovitosti *ICV* (angl. Integrity Check Value) izračunamo s pomočjo *CRC* vrednost (angl. cyclic redundancy check).
4. IV in šifirini ključi za posamezen paket so vhodni parametri za *RC4 PRNG* funkcijo. Ta generira tok ključev, ki je enake dolžine kot podatki, *MIC* in *ICV*.
5. Tok ključev je s pomočjo operacije *XOR* (ekskluzivni-ali) kombiniran s podatki, *MIC* in *ICV*.
6. K šifrirani vsebini paketov dodamo v polji imenovani *IV* polje in razširjeno *IV* polje (angl. IV field), vrednost *IV*. Rezultat nato ovijemo z glavo in repom 802.11.

Dešifriranje poteka podobno in je prikazano na sliki 11.

1. *IV* pridobimo iz *IV* polja in razširjenega *IV* polja. *IV, DA* in *DEK* so vhodni parametri v *KMF*, s pomočjo katere izračunamo *PPK*.
2. *IV* in *PPK* sta vhodna parametra v funkcijo *RC4 PRNG*, ki generira izhodni tok ključev enake dolžine kot šifrirani podatki, *MIC* in *ICV*.
3. Tok ključev je *XOR* kombiniran s podatki, *MIC* in *ICV*. S pomočjo te operacije pridobimo dešifrirane podatke, *MIC* in *ICV*.
4. Za dešifriranje podatke izračunamo *ICV* in ga primerjamo z *ICV*, ki smo ga prejeli in dešifrirali. Če se ne ujemata, zavržemo podatke.
5. *DA, SA*, podatki in *DMK* so vhodni parametri v funkcijo Michael, ki izračuna *MIC*.
6. Izračuna se vrednost *MIC* in se jo primerja z dešifriranim *MIC*. Če se vrednosti ne ujemata, podatke zavržemo. V nasprotnem primeru so podatki predani višji omrežni ravni za nadaljnjo procesiranje.



Slika 11: **WPA dešifriranje**

Mehanizmi za varovanje so pri WLAN enako pomembni kot pri Bluetoothu. Sledi primerjava varnosti obeh tehnologij glede na definirane primerjalne kriterije.

4 Primerjava varnostnih mehanizmov

Primerjali bomo varnosti obeh tehnologij (WLAN in Bluetooth). Pri izvedbi bomo uporabili tabelo kriterijev (tabela 1).

Obe tehnologiji, tako WLAN WPA (na kratko WPA) kot Bluetooth, uporabljata različne ključe za overjanje in šifriranje podatkov. Bluetooth uporablja štiri ključe povezave, WPA pa specificira tri različne ključe glede na hierarhijo ključev:

- DMK, ki je enake bitne dolžine za obe hierarhiji ključev in
- KCK, ki se uporablja v štirismernem protokolu za overjanje in izmenjavo ključev.

Ključe DMK se uporablja pri šifriranju in overjanju. Postopek generiranja DMK je različen glede na to, ali gre za šifriranje ali overjanje.

Bluetooth v fazi vzpostavitve in overjanja uporablja več različnih ključev povezave, ki so namenjeni tako vzpostavitvi povezave (vzpostavitveni ključ) kot kasnejšemu overjanju (ključ enote, glavni ključ in kombinacijski ključ). Pri WPA tehnologiji skupni ključ vnesemo ročno v vse naprave omrežja, zato ne potrebujemo posebnih ključev za fazo vzpostavljanja povezave. Overjanje WPA temelji na skupnem ključu – skupni skrivnosti, postopek overjanja pri Bluetoothu pa temelji na poznavanju gesla naprave (PIN). Pri Bluetoothu je PIN različen za vsako napravo. WPA definira skupni ključ, ki si ga delijo vse naprave. S stališča uporabe različnih ključev za overjanje in šifriranje sta tehnologiji enakovredni.

Pomemben dejavnik pri zagotavljanju varnosti je dolžina uporabljenih ključev. Kratki ključi omogočajo izvedbo napada z grobo silo. Bluetooth definira dolžino ključev med 8 in 128 biti. Ker je priporočena dolžina 128 bitov, sodobne implementacije uporabljajo dolžino 128 bitov. Uporaba variabilne dolžine ključa je pogojena z zgodovino tehnologije (npr. restrikcij nekaterih držav glede uporabe močne kriptografije). WPA specifikacija definira ključe dolžine 128 bitov. Zaradi variabilne dolžine ključa Bluetootha je WPA v prednosti, saj specifikacija definira 128-bitno dolžino ključa. Dolžina ključev pri Bluetoothu pa je odvisna od implementacije.

Tretji primerjalni kriterij so karakteristike gesel oz. skupnih skrivnosti. Tehnologiji predvidevata vnos gesel v naprave, iz katerih se nato generirajo ustrezni ključi. Bluetooth za vsako napravo predvideva svoje geslo oz. PIN. Dolžina PIN je lahko največ 16 števk. V praksi srečamo dolžine od 4 do 8 števk. WPA predvideva dolžino gesla med 8 in 63 znakov. Če uporabljamo kratka in enostavna gesla je WPA dovzeten za t. i. napade s slovarjem (angl. dictionary attack) [7]. Zato je priporočljivo, da so gesla ustrezno dolga in ne vsebujejo znanih besed. Priporočljivo je imeti gesla, ki so sestavljena iz črk, števk in posebnih znakov ali pa čisto naključne nize znakov. PIN, ki ga uporablja Bluetooth, je sestavljen iz števke in ne omogoča kombinacije črk, števk ter posebnih znakov. Priporočljivo je uporabljati vsaj osem števk dolge PIN, ki niso znane številke (npr. rojstni datumi). Glede na tretji kriterij je v prednosti Bluetooth, saj so gesla odvisna od naprave in jih je teže avtomatizirano iskati. To drži ob predpostavki, da uporabljamo PIN, daljši od štirih števk. WPA gesla lahko iščemo s pomočjo ustreznih programov, kar olajša iskanje. Slabost WPA je tudi v skupnem geslu, ki je enako za vse naprave v omrežju.

V kriteriju »pomanjkljivosti in luknje v uporabljenih algoritmih« so zajete znane šibke točke, luknje in druge napake, ki so bile odkrite v posameznih algoritmih ali postopkih določenega varnostnega mehanizma. Za varnostni koncept Bluetootha je bila do zdaj objavljena le ena pomanjkljivost. Napad omogoča pridobitev PIN v postopku vzpostavljanja povezave (angl. Pairing). Podrobnosti so opisane v [18]. Veliko hroščev v programski opremi nekaterih mobilnih telefonov je v praktični uporabi omajalo zaupanje v varnost Bluetootha [19]. Zaradi slabo zasnovanih mobilnikov, ki so podpirali Bluetooth, se je na spletu pojavila kopica programov, ki omogočajo zlorabo Bluetooth [19]. Ker ti napadi niso posledica pomanjkljivosti v specifikaciji Bluetooth, marveč napak in površnosti snovalcev mobilnih telefonov, jih v okviru primerjave ne bomo upoštevali. V zvezi s tehnologijo WPA je znana pomanjkljivost pri izbiri gesla. Možen je napad s slovarjem oz. uganjevanje gesla [11], [8], [7]. Prav tako so se pojavile varnostne pomanjkljivosti v algoritmu RC4, ki ga uporablja WPA [13]. Pomanjkljivosti algoritma RC4 so šibki ključi (angl. weak keys), vendar je mogoče pomanjkljivost izničiti z izločitvijo znanih šibkih ključev. RC4 v kombinaciji z WPA do sedaj še ni bil uspešno kriptoanaliziran in razbit, medtem ko je bila kombinacija WEP in RC4 uspešno kriptoanalizirana in razbita [13]. Ker vsebuje WPA daljši inicializacijski vektor (48 bitov) kot WEP (24 bitov), ni mogoče aplicirati napadov na RC4-WEP na RC4-WPA.

Tabela 3: **Primerjava varnostnih mehanizmov**

Kriterij	**WPA**	**Bluetooth**
Različni ključi za šifriranje in overjanje	Da	Da
Dolžine ključev	šifriranje: 128 bitov overjanje: 128 bitov	šifriranje: 8–128 bitov overjanje: 128 bitov
Karakteristike gesel/skupnih skrivnosti	geslo: 8–63 znakov črke, številke, posebni znaki običajno vsaj 8 znakov	PIN: 4–8 števk številke običajno 4–8 števk
Pomanjkljivost in luknje v uporabljenih algoritmih	napad s slovarjem šibki ključi pri šifrirnem algoritmu RC4	pridobivanje PIN v fazi vzpostavljanja povezave
Obvezna uporaba overjanja	Ne	Ne
Obvezna uporaba šifriranja	Ne	Ne
Obvezna uporaba mehanizmov za zagotavljanjE celovitosti	Ne	Ni na voljo

Glede na peti kriterij (obveznost uporabe overjanja) sta obe tehnologiji glede na specifikacijo, enakovredni. Nobena specifikacija, niti WPA niti Bluetooth, ne predvideva obvezne uporabe overjanja. Kljub temu pa je treba omeniti, da v praksi naprave Bluetooth zahtevajo vnos PIN, vsaj privzetega. Po drugi strani pa lahko uporabnik pri omrežnih napravah, ki podpirajo WPA, le-to izključi. V praktični uporabi ima torej prednost Bluetooth.

Glede na obveznost uporabe šifriranja (šesti kriterij) sta tehnologiji enakovredni s stališča specifikacije. Tehnologiji definirata, da šifriranje vključuje predhodno overjanje. Kljub temu pa je situacija enaka kot pri overjanju. Po specifikaciji sta tehnologiji enakovredni, vendar je v praksi bolj varen Bluetooth.

Zadnji primerjalni kriterij (obveznosti zagotavljanja celovitosti) je odvisen od uporabe šifriranja in overjanja. Bluetooth ne zagotavlja celovitosti s stališča varnosti. Pri tehnologiji WPA to funkcijo opravlja algoritem Michael. Zagotavljanje celovitosti, šifriranje in overjanje so pri tehnologiji WPA med seboj tesno povezani. Ob vnosu skupnega ključa samodejno uporabljamo vse tri. Glede na kriterij je WPA v prednosti pred Bluetoothom, ki nima kriptografskega zagotavljanja celovitosti.

V tabeli 4 je strnjena celotna primerjava. Tehnologiji sta enakovredni glede na dolžino ključa in uporabe različnih ključev za šifriranje in overjanje ter obvezne uporabe šifriranje in overjanja. Razlika je predvsem v karakteristikah gesel/skupnih skrivnosti in v pomanjkljivostih ter luknjah v uporabljenih algoritmih. Glede na te kriterije je boljši Bluetooth. Največja razlika med obema tehnologijama pa je v obveznost uporabe mehanizmov za zagotavljanje celovitosti. Pri tem je v prednosti WPA, saj vsebuje zagotavljanje celovitosti v kriptografskem smislu (s pomočjo ključa – algoritem Michael), medtem ko Bluetooth definira le »klasično« zagotavljanje celovitosti. Glede na izbrane kriterije bi lahko sklenili, da so varnostni mehanizmi in s tem raven varnosti bolj izpopolnjeni pri Bluetoothu.

5 Sklep

V članku smo predstavili varnostne mehanizme tehnologije Bluetooth in WLAN WPA. Podali smo analizo in primerjavo varnostih mehanizmov obeh tehnologij. Določili smo kriterije, ki smo jih izbrali na gesla in mehanizem za zagotavljanje celovitosti. Zato bi morali razvijalci identificirati slabosti v naslednjih revizijah varnostnih mehanizmov Bluetootha in WLAN. Naslednik standarda WPA pri omrežjih WLAN je WPA2 oz. standard IEEE 802.11i. Le-ta vsebuje številne izboljšave na področju varnosti [9], medtem ko Bluetooth verzija 2.0 ne prinaša izboljšav na področju varnosti [4]. Ker je specifikacija že sprejeta in se že implementira v praksi, bi bilo treba morda v naslednji reviziji specifikacije Bluetooth podrobneje analizirati nastale šibke točke in jih izboljšati. Prek obeh vrst brezžičnih tehnologij se namreč prenašajo občutljivi podatki, ki jih je treba dobro zaščititi. Že »narava« prenosnega medija (zrak) zahteva boljše varnostne mehanizme kot prenos prek kabla. Tega se morajo zavedati tudi uporabniki tehnologije.

6 Viri in literatura

[1] Bluetooth Special Interest Group, http://www.bluetooth.com/, nazadnje obiskano 1. 9. 2006.

[2] Bluetooth Specification Version 1.1, Bluetooth SIG, 2001.

[3] Bluetooth Specification Version 1.2, Bluetooth SIG, 2003.

[4] Bluetooth Specification Version 2.0 + EDR, Bluetooth SIG, 2004.

[5] C. Gehrmann, J. Persson, B. Smeets: Bluetooth Security, Artech House, 2004.

[6] D. Halasz: IEEE 802.11i and wireless security, Embedded.com, 2004, http://www.embedded.com/showArticle.jhtml?articleID=34400002, nazadnje obiskano 1. 9. 2006.

[7] G. Fleishman, R. Moskowitz: Weakness in Passphrase Choice in WPA Interface, Wi-Fi Networking News, 2003, http://wifinetnews.com/archives/002452.html, nazadnje obiskano 1. 9. 2006.

[8] G. Fleishman: WPA Cracking Proof of Concept Available, Wi-Fi Networking News, 2004, http://wifinetnews.com/archives/004428.html, nazdanje obiskano 1. 9. 2006.

[9] IEEE Standard 802.11i, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control, (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC), Security Enhancements, IEEE Computer Society, 2004.

[10] J. Edney, W. A. Arbaugh: Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison-Wesley, 2003.

[11] J. L. MacMichael: Auditing wi-fi protected access (WPA) pre-shared key mode, Linux Journal, Volume 2005 Issue 137, 2005.

[12] J. Walker, Part II: The Temporal Key Integrity Protocol (TKIP), 802.11 Security Series, Platform Networking Group, Intel Corporation, http://cache-www.intel.com/cd/00/00/01/77/17769_80211_part2.pdf, nazadnje obiskano 1. 9. 2006.

[13] S. Fluhrer, I. Mantin, A. Shamir: Weaknesses in the Key Scheduling Algorithm of RC4, Computer Science Department, The Weizmann Institute, Cisco Systems Inc., August 2001.

[14] The Official Bluetooth Membership Site, https://www.bluetooth.org/, nazadnje obiskano 1. 9. 2006.

[15] WiFi Protected Access (WPA) Overview, Windows Platform Design Notes, Microsoft Corporation, 2003.

[16] Wi-Fi Protected Access (WPA), Version 1.2, Wi-Fi Alliance, 2002.

[17] Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks, Wi-Fi Alliance, 2003, http://main.wi-fi.org/membersonly/getfile.asp?f=Whitepaper_Wi-Fi_Security4-29-03.pdf, nazadnje obiskano 1. 9. 2006.

[18] Y. Shaked, A. Wool: Cracking the Bluetooth PIN, In Proc. 3rd USENIX/ACM Conf. Mobile Systems, Applications, and Services (MobiSys), pages 39–50, 2005.

[19] Trifinite.stuff, trifinite.org – the home of the trifinite.group, http://trifinite.org/trifinite_stuff.html, nazadnje obiskano 1. 9. 2006.

[20] C. P. Pfleeger, S. L. Pfleeger: Security in Computing, 3rd Ed, Prentice Hall, 2002.

▪

Marko Hölbl je podiplomski študent računalništva in informatike na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Raziskovalno se ukvarja z zaščito in varovanjem podatkov, kriptografijo in zaupnostjo v omrežjih ter inteligentno obdelavo podatkov z metodami strojnega učenja.

▪

Boštjan Brumen je docent na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru. Na raziskovalnem področju se ukvarja s podatkovnimi bazami, podatkovnim rudarjenjem in varovanjem računalniških sistemov.

▪

Tatjana Welzer je redna profesorica na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru, kjer predava na dodiplomski in podiplomski stopnji in vodi laboratorij za podatkovne tehnologije. Na raziskovalnem področju se ukvarja predvsem s podatkovnimi bazami, kakovostjo podatkov, podatkovnim modeliranjem in varovanjem podatkov.