VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

BEZPEČNOSTNÍ ANALÝZA BEZDRÁTOVÝCH WI-FI SÍTÍ

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

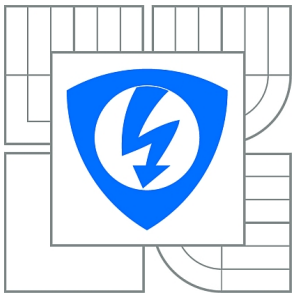
AUTOR PRÁCE
AUTHOR

Bc. JIŘÍ PASSINGER

BRNO 2012

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

BEZPEČNOSTNÍ ANALÝZA BEZDRÁTOVÝCH WI-FI SÍTÍ

SECURITY ANALYSIS OF WIRELESS WI-FI NETWORK

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

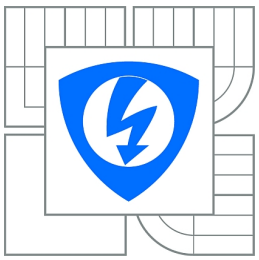
AUTOR PRÁCE — Bc. JIŘÍ PASSINGER

AUTHOR

VEDOUCÍ PRÁCE — Ing. MILAN BARTL

SUPERVISOR

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Jiří Passinger	***ID:***	112054
Ročník:	2	***Akademický rok:***	2011/2012

NÁZEV TÉMATU:

Bezpečnostní analýza bezdrátových Wi-Fi sítí

POKYNY PRO VYPRACOVÁNÍ:

Prouzkoumat úroveň zabezpečení bezdrátových Wi-Fi sítí. Provést pokus o narušení bezpečnosti. Popsat příčinu případného selhání bezpečnostních prvků. Navrhnout způsob implementace bezpečnostní záplaty. Pokusit se vytvořit bezpečnostní záplatu a implementovat ji na vybraném Wi-Fi zařízení.

DOPORUČENÁ LITERATURA:

[1] BURDA, K. Bezpečnost informačních systémů. 1. Brno: FEKT VUT Brno, 2005. s. 1-104.

[2] BURDA, K.; PŘINOSIL, J.; STRAŠIL, I. Bezpečnost rádiových kanálů pro místní informační systémy. In Bezpečnost světa a domoviny. Brno: Univerzita obrany, Brno, 2010. s. 1-6. ISBN: 978-80-7231-728-8.

Termín zadání:	6.2.2012	***Termín odevzdání:***	24.5.2012

Vedoucí práce: Ing. Milan Bartl
Konzultanti diplomové práce:

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Tato práce pojednává o bezpečnosti Wi-Fi sítí. Definuje bezpečnost a uvádí její specifika pro oblast Wi-Fi sítí. Dále popisuje principy některých bezpečnostních mechanismů s následným návodem na jejich prolomení. Z toho plyne podstata bezpečnostích chyb. Největší důraz klade na aktuální bezpečnostní problém technologie Wi-Fi Protected Setup (WPS). Následně se zabývá zprovoznění této technologie v GNU/Linuxové distribuci OpenWrt na Wi-Fi směrovači TP-LINK TL-WR1043ND. V závěru uvádí návrhy na opravu této bezpečnostní chyby.

KLÍČOVÁ SLOVA

bezpečnost, Wi-Fi, BackTrack, OpenWrt, WPS

ABSTRACT

This project is concerned with the security of Wi-Fi network. It defines security and introduces the principles of some security systems which are consequently instructed for its breakthrough, out of which follows the nature of security failures. The main emphasis is put on the current security issue of Wi-Fi Protected Setup (WPS) technology. Consequently, it is concerned with the putting into service of this technology in GNU/Linux distribution OpenWrt on Wi-Fi router TP-LINK TL-WR1043ND. The project is concluded with the suggestions for the correction of the security failure.

KEYWORDS

security, Wi-Fi, BackTrack, OpenWrt, WPS

PASSINGER, Jiří *Bezpečnostní analýza bezdrátových Wi-Fi sítí*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2012. 64 s. Vedoucí práce byl Ing. Milan Bartl.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Bezpečnostní analýza bezdrátových Wi-Fi sítí“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu práce Ing. Milanu Bartlovi za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce. Dále děkuji všem, kteří vznik této práce umožnili.

V Brně dne ....

(podpis autora)

SIX research centre
sensor, information and communication systems

Faculty of Electrical Engineering
and Communication

Brno University of Technology
Purkynova 118, CZ-61200 Brno, Czechia

http://www.six.feec.vutbr.cz

Výzkum popsaný v této diplomové práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007–13
OP Výzkum a vývoj pro inovace

OBSAH

SEZNAM OBRÁZKŮ

ÚVOD

Wi-Fi sítě patří k velmi rozšířeným a tento trend má stále stoupající úroveň. Je velmi snadné a pohodné pořídit si Wi-Fi směrovač, připojit ho k Internetu a mít možnost se připojit se svým bezdrátovým zařízením kdekoliv v dosahu signálu.

Méně potěšující je fakt, že možnost odposlouchávat komunikaci a v případě slabého zabezpečení ji snadno číst, má v dosahu signálu libovolný útočník. Proto je u Wi-Fi sítí důležité neopomíjet důkladné zabezpečení.

Cílem této práce je prozkoumání úrovně zabezpečení Wi-Fi sítí a provést pokus o narušení jejich bezpečnosti. Pro útoky byla využívána GNU/Linuxová distribuce BackTrack jenž byla v práci stručně popsána.

Jsou popsány možnosti odposlechu, útok na odpojení vybraného klienta, zjištění skrytého SSID, útok na technologie WEP a WPS. V práci je popsán i princip funkce těchto technologií, na základě čehož je zřejmé co je příčinou selhání bezpečnostního mechanismu.

Za účelem možnosti implementace záplaty je popsána a využita GNU/Linuxová distribuce OpenWrt, jenž funguje na Wi-Fi směrovači. V ní byla zprovozněna technologie WPS, na niž je v této práci kladen největší důraz, protože jde o aktuální bezpečnostní problém. V práci je podrobně rozebrán princip fungování WPS, z nějž plyne i známá bezpečnostní chyba a princip útoku. V závěru práce jsou navrženy způsoby opravy této chyby.

1 BEZPEČNOST WI-FI SÍTÍ

1.1 Bezpečnost

Bezpečnost lze definovat jako „stav, kdy ztráty aktiv nepřekračují stanovenou míru“ [7], přičemž aktiva představují „vše, co je majitelem považováno za cenné“ [7]. O bezpečnosti nelze hovořit v absolutních hodnotách [5], protože může dosahovat mnoha různých úrovní. Jde o jistý kompromis mezi ztrátou aktiv, která není vyloučená, proti úsilí a hlavně nákladům obětovaným na zabezpečení aktiv, což musí stanovit majitel aktiv.

Úroveň zabezpečení lze vyjádřit pouze s ohledem na určité časové období. Protože postupem času dochází k technickému pokroku, čímž je snadnější některé zabezpečovací mechanizmy překonat. Mohou být objeveny dříve neznámé techniky pro jejich překonání, atd. Na druhé straně dochází ke zlepšování stávajících a vývoji nových možností zabezpečení. To ale většinou vyžaduje neustále investice a vzdělávání lidí, kteří se o bezpečnost starají, ale i nutnost zaškolování všech, kteří mají k aktivům přístup. Jedná se o nekonečný souboj mezi obránci aktiv a útočníky, kteří se jich snaží z různých důvodů zmocnit.

Nelze také vyloučit, že neexistuje někdo, komu se podařilo úspěšně překonat některý bezpečnostní mechanizmus, tuto informaci nepublikoval a tudíž je tento bezpečnostní mechanizmus všeobecně dál považovaný za důvěryhodný.

Je třeba mít na paměti, že úroveň zabezpečení sítě odpovídá úrovni nejméně zabezpečeného prvku této sítě (včetně koncových stanic).

1.1.1 Lidský faktor

Bezpečnost nezávisí pouze na bezpečnostních technologiích či technických zařízeních, ale z velké míry se na ní podílejí také lidé [25]. Může jít např. o odborníky, kteří zabezpečení navrhli, implementovali a nakonfigurovali, dále také o běžné uživatele, ale o všechny, kteří mají příležitost do zabezpečení úmyslně či nevědomě zasáhnout. Tito lidé mohou znát principy zabezpečení, znají své autentizační údaje a mohou mít fyzický přístup k technickému vybavení.

Znalosti těchto údajů, svého postavení a možnosti přístupu mohou tito lidé zneužít sami, ale mohou je také vědomě, nebo nevědomě sdělit či poskytnout neoprávněné osobě. Útočníci používají pro zjištění takovýchto informací velmi účinné metody sociálního inženýrství [22]. Proto je důležité pečlivé vytvoření bezpečnostních pravidel, která budou sepsána s patřičným nadhledem nad možnými bezpečnostními úskalími. Tato pravidla musí výborně ovládat a dodržovat všichni, kteří by mohli přijít do styku se zabezpečením aktiv, popř. se samotnými aktivy.

1.2 Specifika bezpečnosti Wi-Fi sítí

Wi-Fi (Wireless Fidelity) sítě patří do skupiny bezdrátových sítí. Jejich signál je šířen prostorem a je velmi obtížné omezit dosah tohoto signálu na vymezené území (hranice pozemku, budovy, místnosti, apod.) [6].

Možnost použít bezdrátové zařízení a pracovat s Wi-Fi síti kdekoliv v dosahu signálu přináší uživatelům mnohé výhody. Zároveň má ale tu samou možnost i útočník, což předurčuje jistá bezpečností rizika.

Útočník v dosahu signálu může např. [25]:

- komunikaci na Wi-Fi odposlouchávat (zaznamenávat a následně zpracovávat).
- znemožňovat komunikaci rušením přenosového pásma.
- zahltit síť uměle generovaným provozem, což může vést k jejímu zpomalení až vyřazení z provozu.

Pokud se mu podaří do sítě připojit může ještě např.:

- modifikovat přenášené zprávy.
- pokusit se o editování nastavení sítě.
- získat přístup k Internetu.
- provádět mnoho další typů útoků, včetně využití sítě k útokům na jiné cíle.

Obecně lze typy útoků rozdělit na pasivní a aktivní. U pasivních útočník neprovádí žádnou aktivitu, kterou by oběť mohla zjistit (typicky třeba odposlouchávání). Při aktivním útoku již útočník aktivně vyvíjí nějakou činnost, která může být detekována a klasifikována jako útok.

1.3 Vícestupňová ochrana

Pro zvýšení bezpečnosti je nutné síť zabezpečit vhodnou kombinací více bezpečnostních opatření. Tím vznikne více stupňů ochrany a když se útočníkovi podaří některý z nich překonat, narazí na další. Tento vícestupňový způsob ochrany lze aplikovat na různých aspektech zabezpečení, může jít např. o zabezpečení fyzických prvků sítě, zabezpečení možnosti připojení k síti, zabezpečení přenášených dat, atd.

Při zabezpečování přenášených dat lze implementovat bezpečnostní mechanizmy na úrovních jednotlivých vrstev referenčního komunikačního modelu ISO/OSI (International Standards Organization / Open System Interconnection).

Technologie Wi-Fi pracuje na prvních dvou vrstvách síťového modelu ISO/OSI, tj. fyzická a spojová (linková) vrstva [6].

Aby mohla být Wi-Fi síť považována za důvěryhodnou musí spolehlivě vyhovovat všem následujícím kritériím.

- Autentizace – ověření identity (totožnosti) entity. Může jít o entity fyzické (např. síťové prvky, počítače), lidské (např. správci, uživatelé) a logické (např. procesy) [8]. Je vhodné když se vzájemně autentizují všechny zúčastněné entity.
- Autorizace – jedná se o řízení přístupu, kdy je subjekt identifikován a na základě oprávnění přidělených autoritou může vykonávat to k čemu je oprávněn (autorizován). Autorita je majitel, respektive správce aktiv, jenž může rozhodnout, kdo dostane oprávnění k aktivům přistupovat a v jakém rozsahu [7].
- Utajení (důvěrnost) – jde o zabezpečení před neautorizovaným únikem informací [23].
- Integrita dat – poskytuje záruku před neautorizovanou modifikací dat, data jsou stále identická (nedotčená) [8, 23].
- Nepopiratelnost – jde o jednoznačné určení odpovědnosti subjektu za provedenou činnost nebo událost. Např. určení toho, že byla daná zpráva odeslána, kdo ji odeslal, že byla přijata a kdo ji přijal [23].

1.4 Obecný postup návrhu zabezpečení Wi-Fi sítě

Zabezpečení Wi-Fi sítě je potřeba navrhnout ještě před jejím vytvořením a aplikovat před jejím uvedením do provozu. Tím se lze vyhnout plýtvání za pořizování komponent nevyhovujících navržené bezpečnostní koncepci a zbytečnému riziku ztráty nezabezpečených aktiv.

Nejprve je velmi důležité, aby si majitel aktiv ujasnil jakými aktivy disponuje, jakou mají hodnotu, proč by je měl chránit, jaká jsou hrozící rizika, co by znamenala ztráta aktiv, jaké úsilí a náklady je ochoten na jejich ochranu vynaložit.

V této chvíli by měl odborník na bezpečnost Wi-Fi sítí na základě zjištěných potřeb a možností navrhnout odpovídající komplexní řešení. To bude zahrnovat všemožné aspekty, od výběru a umístění hardwarových komponent, přes výběr a aplikování bezpečnostních opatření, až po vytvoření pravidel, soupisů, postupů pro různé situace, školení osob a další.

Tímto může být Wi-Fi síť uvedena do provozu, ale práce na její bezpečnosti nekončí. Nadále je třeba sledovat vývoj v oblasti bezpečnosti Wi-Fi sítí a dělat patřičné inovace. Dál je nutné systematicky a s danou četností prověřovat celistvost sítě a bezchybnou funkci bezpečnostních mechanizmů. Zároveň je potřeba provádět detekci útoků, pokusů o ně a na základě zjištěných skutečností provádět příslušná opatření. Je dobré rozlišovat mezi náhodně provedenými a cíleně mířenými útoky.

2 BACKTRACK

BackTrack je distribuce operačního systému GNU/Linux (GNU – GNU's Not Unix), která se zaměřuje na penetrační testování. Obsahuje velké množství vybraných a vyzkoušených bezpečnostních nástrojů, které pokrývají různé oblasti bezpečnosti informačních systému. Proto představuje rychlý a poměrně snadný způsob, jak mohou začátečníci i zkušení uživatelé testování bezpečnosti informačních systémů provádět. [4].

Tuto distribuci lze stáhnout z oficiálních webových stránek, viz [4], kde se také nachází různé návody a diskuzní fórum. Je na výběr pro 32 i 64 bitovou architekturu a s prostředími GNOME (GNU Network Object Model Environment) nebo KDE (K Desktop Environment). BackTrack může být nainstalován nebo může být provozován z Live DVD (Digital Versatile Disc) či USB (Universal Serial Bus) flash disku.

V této práci byla využívána 32 bitová verze distribuce BackTrack 5 R2 s GNOME, ukázka viz obrázek 2.1. Nástroje pro útoky na Wi-Fi sítě se nacházejí v několika podnabídkách ze zobrazených nabídek. Jsou roztříděné podle účelu použití.

Obr. 2.1: Ukázka distribuce BackTrack a její základní nabídky.

Pro nastartování systému do grafického rozhraní je nutné při startu nechat výchozí volbu „BackTrack Text – Default Boot Text Mode“ a po nastartování textového režimu napsat a potvrdit `startx` .

3 POUŽÍVANÝ WI-FI SMĚROVAČ

Aby mohlo být na Wi-Fi směrovači implementováno jakékoliv bezpečnostní řešení, je nutné použít Wi-Fi směrovač, který implementaci vlastního řešení ve firmwaru umožňuje, popř. je u něj možné nahradit původní firmware jiným. S ohledem na to byl pro řešení této práce vybrán Wi-Fi směrovač TP-LINK TL-WR1043ND, viz obrázek 3.1.

Ten umožňuje nahradit originální proprietární firmware alternativním, který je poskytován včetně zdrojových kódů, má dobrou dokumentaci a implementaci vlastního řešení umožňuje.

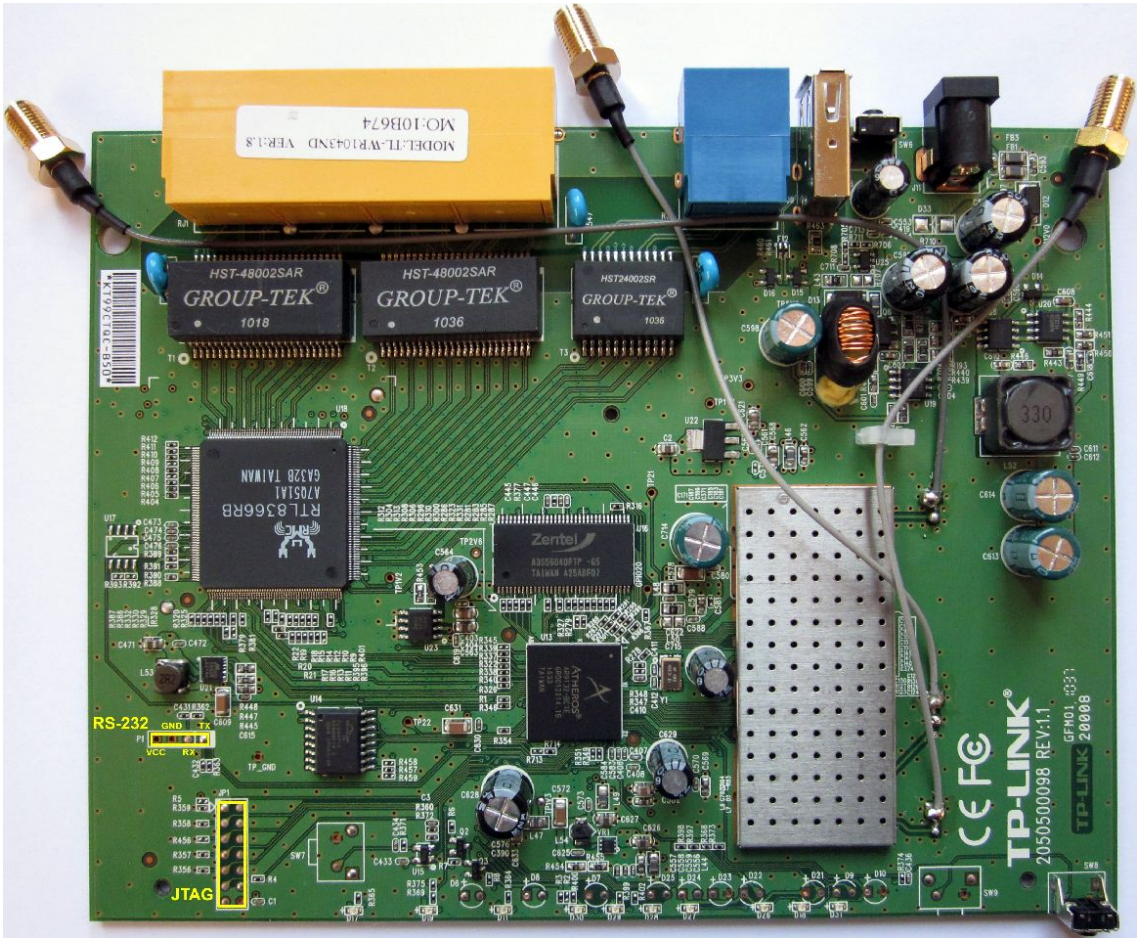
Obr. 3.1: Wi-Fi směrovač TP-LINK TL-WR1043ND, převzato z [26].

Při pokusech o narušení bezpečnosti v kapitolách 6, 7 a 8 byl použit Wi-Fi směrovač Netgear WPN824 v2 s originálním firmwarem.

3.1 Přehled základních parametrů TP-LINK TL-WR1043ND

- **Procesor** – Atheros AR9132 rev 2 (MIPS 24Kc V7,4), 400 MHz, (více lze zjistit v OpenWrt, které bude popsáno dále, z výpisu po zadání `dmesg` a `cat /proc/cpuinfo`).
- **Operační paměť** – 32 MB [27].
- **Flash paměť** – 8 MB, ST 25P64V6P [27].
- **Zavaděč** – U-Boot (Universal Bootloader) [27].
- **Ethernetový čip** – RealTek RTL8366RB pěti portový gigabitový přepínač [27].

- **Rozhraní** – 4x LAN (10/100/1 000 Mbit/s) (LAN – Local Area Network), WAN (10/100/1 000 Mbit/s) (WAN – Wide Area Network), USB 2.0, RS-232[1], JTAG[1] (Joint Test Action Group) [26, 27].
- **Bezdrátový čip** – Atheros AR9103 2,4 GHz [27].
- **Wi-Fi standardy** – IEEE 802.11b (IEEE - Institute of Electrical and Electronics Engineers), IEEE 802.11g, IEEE 802.11n [26].
- **Antény** – 3 odnímatelné všesměrové, každá 3 dBi [26].
- **Výchozí údaje** – IP adresa: 192.168.1.1, uživatelské jméno: admin, heslo: admin.
- **Tlačítka** – reset, QSS (Quick Security Setup).
- **Napájení** – stejnosměrné, 12 V, 1,5 A.



Obr. 3.2: Deska plošných spojů směrovače TP-LINK TL-WR1043ND s vyznačenými rozhraními RS-232 a JTAG [28, 27].

[1]Rozhraní RS-232 a JTAG jsou dostupná po rozkrytování na desce plošných spojů. Vyznačeno na obrázku 3.2.

4 OPENWRT

Jako náhrada za původní firmware ve Wi-Fi směrovači byl zvolen firmware vytvořený pomocí OpenWrt. Ten velmi dobře umožní funkčnost Wi-Fi směrovače, implementaci vlastního řešení i jeho otestování.

OpenWrt je GNU/Linuxová distribuce, která je určena pro vestavěné minimalistické systémy, nebo-li zařízení s velmi omezenými výpočetními prostředky. Mezi výhody tohoto řešení patří využívání propracovanosti a filozofie systému GNU/Linux. Distribuce je poskytována pod licencí GPLv2 [1] (GPL – General Public License), z čehož plyne, že je vše poskytováno včetně zdrojových kódů.

OpenWrt obsahuje balíčkovací systém opkg (Open PacKaGe management), který umožňuje do systému přidat či odebrat vybranou aplikaci, bez nutnosti vytvářet a přepisovat celý firmware. Neomezuje se pouze na výrobu předpřipraveného firmwaru, ale umožňuje si vytvořit firmware dle vlastních požadavků a pomocí balíčkovacího systému ho dále upravovat. K dispozici jsou již tisíce připravených balíčků, které se nacházejí v repozitáři a další jsou poskytovány komunitou. To pro tuto distribuci představuje velké možnosti použití a široký potenciál. [1].

Konfiguraci OpenWrt lze provádět pomocí příkazového řádku (např. přes SSH (Secure SHell)), nebo pomocí webového rozhraní (projekty LuCi (Lua Unified Configuration Interface) nebo X-Wrt).

Na webových stránkách OpenWrt, viz [18], lze najít dokumentaci, fórum, wiki, lze si distribuci v požadované verzi stáhnout a také se zde nachází část věnovaná vývoji.

Verze OpenWrt jsou číslované a zároveň mají svůj slovní název. Ten vychází z názvu koktejlů a návod k jejich přípravě se nachází v úvodním logu po přihlášení přes SSH. Pro tuto práci byla využita distribuce OpenWrt ve verzi Backfire 10.03.1.

4.1 Postup instalace OpenWrt

Nejprve je nutné si obstarat OpenWrt firmware a v další fázi ho nahrát do Wi-Fi směrovače.

4.1.1 Získání firmwaru OpenWrt

Pro získání OpenWrt firmwaru existují 4 možnosti [27]:

- Stáhnout si předpřipravený firmware. Pro mnoho podporovaných zařízení je na webových stránkách OpenWrt již takovýto firmware připraven ke stažení. Jedná se o nejrychlejší a nejsnadnější možnost, která je doporučována.

- Druhou možností je stáhnutí a použití produktu „Image Generator“, s jehož pomocí si lze firmware vytvořit.
- Dále použití SDK (Software Development Kit) a křížové kompilace.
- Poslední a zřejmě nejsložitější možností je využití „OpenWrt Buildroot“.

V této práci bylo použita první možnost, jenž je dostačující, byla ale vyzkoušena i možnost poslední, která představuje kompletní vytvoření firmwaru ze zdrojových kódů.

Předpřipravený firmware OpenWrt ve verzi Backfire 10.03.1 pro směrovač TP-LINK TL-WR1043ND lze stáhnout z [11]. Zároveň se zde nacházejí ve složce „package“ balíčky, které jsou poskytovány a mohou být nainstalovány. Jelikož jsou tu firmwary pro všechny zařízení se stejnou architekturou, je třeba vybrat správný. Názvy souborů mají následující podobu:

```
openwrt-architektura-zarizeni-souborovy-system-typ.bin
```

V tomto případě je správný název:

```
openwrt-ar71xx-tl-wr1043nd-v1-squashfs-factory.bin
```

Souborové systémy mohou být squashfs nebo jffs2. Vhodnější a v tomto případě jediný poskytovaný je squashfs.

Typ může být factory nebo sysupgrade. Factory slouží pro nahrazení jiného firmwaru a sysupgrade pro nahrazení OpenWrt novější verzí. [12].

Velikost staženého souboru je 8 126 464 B a bude nahráván do paměti s celkovou velikostí 8 388 608 B, ve které je pro firmware vyhrazeno 8 192 000 B.

4.1.2 Nahrání firmwaru OpenWrt do směrovače

V této fázi by při přerušení procesu mohlo dojít ke zničení směrovače. Proto je dobré proces nepřerušovat a žádné ze zařízení neodpojovat od napájení. Je lepší, když jsou zařízení připojeny k záložnímu zdroji napájení.

Způsobů pro nahrání firmware je několik [27]:

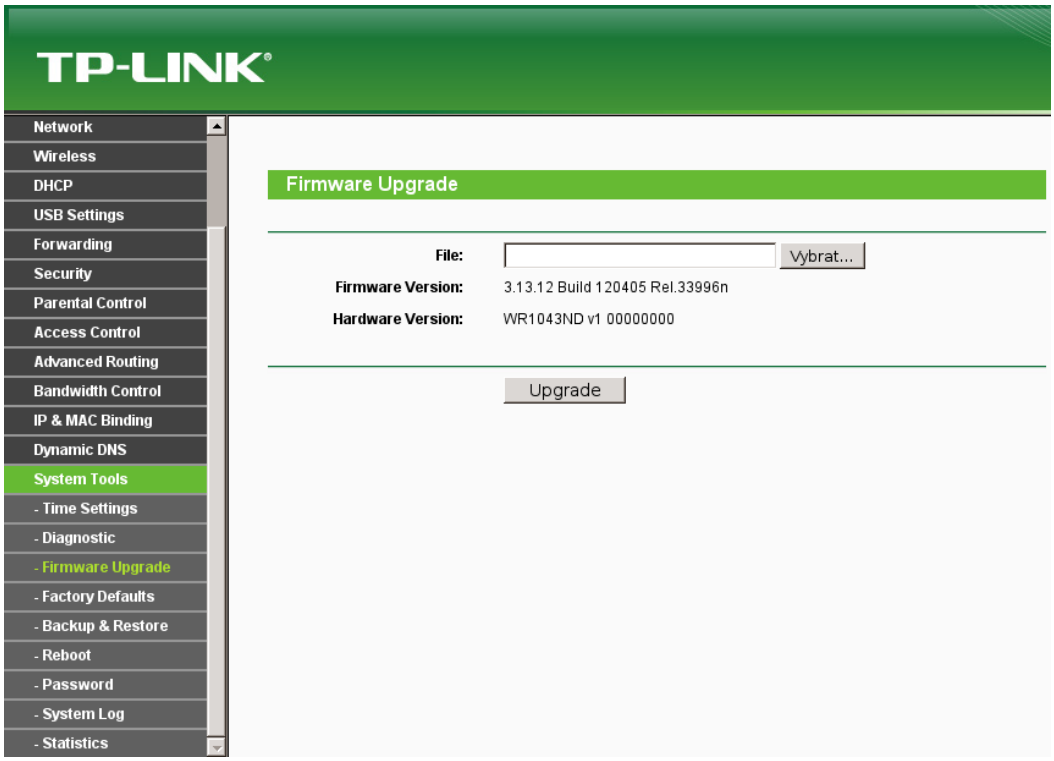
- Nejjednodušší metodou je nahrání pomocí webového rozhraní z předešlého firmwaru jako jeho aktualizace.
- Pomocí zavaděče a LAN portu.
- Pomocí zavaděče a sériového portu (RS-232).
- Přes rozhraní JTAG.
- A další.

V této práci bylo provedeno nahrání firmware přes webové rozhraní. Při tom je potřeba propojit síťovým kabelem síťovou kartu počítače s LAN portem směrovače a nechat si přiřadit síťovou adresu a masku od DHCP (Dynamic Host Configuration

Protocol), nebo je nastavit ručně. Výchozí adresa směrovače je 192.168.1.1 s maskou 255.255.255.0, proto musí být na počítači nastavena stejná maska a adresa ze stejné podsítě. U směrovače TP-LINK TL-WR1043ND může být někdy nutné připojení k Internetu na portu WAN, pokud tato podmínka není splněna k nahrání nového firmwaru nedojde a po restartu naběhne původní [27].

Po splnění uvedených podmínek se ve webovém prohlížeči zadá IP adresa směrovače (výchozí 192.168.1.1). Naběhne webové rozhraní, které žádá vyplnění uživatelského jména a hesla (ve výchozím stavu je oboje admin).

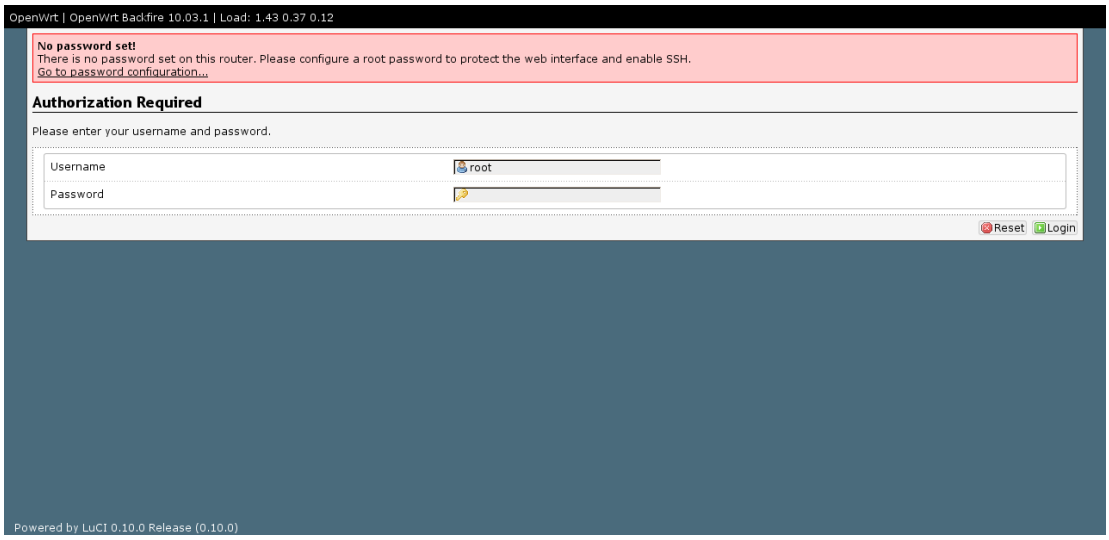
Dále je potřeba v levém sloupci kliknout na „System Tools“ a objeví se nabídka „Firmware Upgrade“, na niž je třeba opět kliknout a nyní již naběhne požadované okno, viz obrázek 4.1.



Obr. 4.1: Nahrání firmwaru ve webovém rozhraní originálního firmwaru.

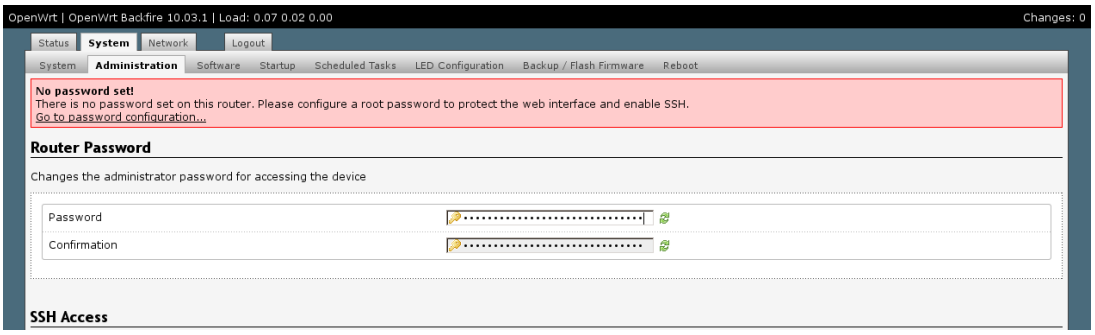
Po kliknutí na tlačítko „Vybrat“ se potřeba zadat umístění připraveného OpenWrt firmwaru. Když je cesta zadána stačí kliknout na tlačítko „Upgrade“ a čekat než se nový firmware nahraje. Celý proces trvá cca 2 minuty.

Po automatickém restartování naběhne již webové rozhraní OpenWrt, jak je vidět na obrázku 4.2. V tuto chvíli není nastaveno žádné heslo a systém proto žádá o jeho nastavení. Uživatelské jméno je standartní jméno superuživatele z prostřední GNU/Linux – root.



Obr. 4.2: První přihlášení do OpenWrt.

Stačí kliknout na tlačítko „Login“. Nastavení hesla je možné najít pod záložkami „System“, „Administration“ v oblasti „Router Password“ jak je vidět na obrázku 4.3.



Obr. 4.3: Změna hesla v OpenWrt.

První přihlášení lze provést i pomocí telnetu. V GNU/Linuxových systémech zadáním příkazu:

```
telnet 192.168.1.1
```

Ovšem jak upozorňuje následující výpis, je třeba pomocí příkazu `passwd root` zadat heslo. Následně bude telnet vypnut (půjde použít pouze v záchranném módu) a zapnuto SSH.

4.2 Základní příprava a konfigurace OpenWrt

Základní konfiguraci lze dělat pomocí webového rozhraní. Veškerou konfiguraci lze provádět připojením přes konzolu pomocí SSH. Tato druhá možnost byla z praktic-

kých a názornějších důvodů zvolena v této práci pro veškerou další konfiguraci.

Dále je nutno předeslat, že veškerá konfigurace bude prováděna z operačního systému GNU/Linux Ubuntu.

Většina konfigurační souborů se v OpenWrt nachází v /etc/config. Konfiguraci lze také provádět pomocí nástroje pro snadnější konfiguraci UCI (Unified Configuration Interface).

4.2.1 Připojení přes SSH

Pro přihlášení přes SSH s uživatelským jménem root na adresu 192.168.1.1 je potřeba zadat:

```
ssh root@192.168.1.1
```

Následně je požadováno schválení veřejného klíče a pokračování v procesu přihlašování. Veřejný klíč bude uložen (v Ubuntu) v ∼/.ssh/known_hosts. Dále je požadováno heslo pro přihlášení. Po jeho správném zadání je přihlášení úspěšné a naběhne úvodní výpis:

```
BusyBox v1.15.3 (2011-11-24 00:44:20 CET) built-in shell (ash)
Enter 'help' for a list of built-in commands.


 _______                     ________        __
|       |.-----.-----.-----.|  |  |  |.----.|  |_
|   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
|_______||   __|_____|__|__||________||__|  |____|
         |__| W I R E L E S S   F R E E D O M
Backfire (10.03.1, r29592) ------------------------
 * 1/3 shot Kahlua    In a shot glass, layer Kahlua
 * 1/3 shot Bailey's  on the bottom, then Bailey's,
 * 1/3 shot Vodka     then Vodka.
---------------------------------------------------
```

4.2.2 Práce s balíčky

Před začátkem instalování balíčků z repozitáře je nezbytné stáhnou jejich seznam. Cesta k repozitáři je uvedena v /etc/opkg.conf. Stažení seznamu dostupných balíčků se provede pomocí:

```
opkg update
```

Zobrazení dostupných balíčků včetně krátkého popisu lze získat zadáním:

```
opkg list
```

Seznam nainstalovaných balíčků včetně závislostí a dalších podrobností lze najít v /usr/lib/opkg/status. Instalace dalších balíčků se spustí příkazem:

```
opkg install nazev_balicku
```

K odstranění balíčků slouží:

```
opkg remove nazev_balicku
```

5 ODPOSLECH PŘENÁŠENÝCH DAT NA WI-FI SÍTI

Odposlouchávání přenosu u Wi-Fi sítí vyžaduje umístění antény v dosahu signálu. A to nejen v dosahu signálu přístupového bodu AP (Access Point), ale i jednotlivých stanic, mají-li být taktéž odposlouchávány. Při použití vysoce směrové antény a zesilovače může útočník zachytit signál i ve značné vzdálenosti [5]. Dále stačí na zařízení, ke kterému je tato anténa připojena, zapnout příslušný program, který bude přenášená data zaznamenávat (např. Wireshark).

Pokud není zachycená komunikace zabezpečená, může být rovnou čitelná. Když zabezpečená je (typicky šifrováním), lze tuto komunikaci uložit a zpětně provádět pokusy na prolomení ochrany.

5.1 Monitorovací mód

Aby bylo možné monitorovat veškerý Wi-Fi provoz, který je v dosahu antény, je třeba přepnout Wi-Fi adaptér do monitorovacího módu. K tomu bude využit program Airmon-ng, který se nachází v balíku Aircrack-ng. Manuál k tomuto balíku, včetně syntaxe příkazů lze najít v [3]. Pro ovládání monitorovacího módu slouží příkaz:

```
airmon-ng <start|stop|check|check kill> <rozhrani> [kanal|frekvence]
```

V konkrétním příkladu lze pro zapnutí monitorovacího režimu na rozhraní `wlan0` (název rozhraní a jeho vztah k Wi-Fi lze zjistit z výpisu po zadání příkazu `iwconfig`) použít příkaz:

```
airmon-ng start wlan0
```

Tím dojde k vytvoření rozhraní v monitorovacím módu s názvem `mon0`. Rozhraní `mon0` lze po ukončení monitorovací činnosti zrušit zadáním:

```
airmon-ng stop mon0
```

Stav rozhraní je možné zjistit pomocí `iwconfig`. Zkrácený výpis pro rozhraní `wlan0` bez monitorovacího módu (`Mode:Managed`) a `mon0` v monitorovacím módu (`Mode:Monitor`) může vypadat následovně:

```
wlan0   IEEE 802.11bg  ESSID:off/any
        Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
        Retry  long limit:7   RTS thr:off   Fragment thr:off
        Power Management:off
```

```
mon0    IEEE 802.11bg  Mode:Monitor  Tx-Power=20 dBm
        Retry  long limit:7   RTS thr:off   Fragment thr:off
        Power Management:on
```

5.2 Obrana proti odposlechu

Proti odposlechu se lze bránit potlačením úniku rádiového signálu mimo vymezenou oblast. Toto opatření lze realizovat obložením daných prostor materiálem s vysokou pohltivostí, který rádiový signál nepropustí. Praktická realizace je ale velmi náročná technicky i finančně.

Jako jednodušší, ovšem méně účinnější řešení lze aplikovat následující [5]:

- Umístit AP uvnitř budovy tak, aby co nejlépe pokrýval signálem potřebný prostor a naopak příliš zbytečně nezasahoval mimo něj.
- U AP které to umožňují, snížit vysílací výkon na nejnižší možnou hodnotu, která bude dostatečná pro obsloužení všech stanic v dané oblasti.
- Použít směrové antény, které budou mířit dovnitř požadovaného prostoru.

6 PŘERUŠENÍ SPOJENÍ MEZI PŘÍSTUPOVÝM BODEM A KLIENTY

Cílem útoku může být znemožnění komunikace mezi klientem popř. více klienty a AP. U jistých typů útoků se očekává, že po odpojení se bude chtít klient znovu k přístupovému bodu připojit, což poskytuje možnost zachytit některé důležité informace, jenž jsou při přihlašování přenášeny. Jedná se o aktivní typ útoku, který je možné detekovat.

6.1 Deautentizace

Pro přerušení spojení pomocí deautentizace lze použít program Aireplay-ng, jenž je obsažen v balíku Aircrack-ng.

Nejprve je třeba přepnout Wi-Fi rozhraní do monitorovacího módu a to na stejném kanálu, na němž probíhá komunikace mezi AP a klienty. Číslo kanálu na kterém probíhá spojení lze zjistit např. pomocí programu Wireshark z odposlechnutého rámce beacon (viz hodnota Current Channel na obrázku 7.1). (Pro odposlechnutí rámce beacon je již nutné mít Wi-Fi rozhraní přepnuté v monitorovacím módu. Ten lze následně vypnout a znovu zapnout na zjištěném kanálu.) Monitorovací mód je popsán v kapitole 5.1. V tomto konkrétním případě (pro kanál 6) bude použit příkaz: `airmon-ng start wlan0 6`

Dále může následovat spuštění deautentizačního útoku. Jeho syntaxe v konkrétním i obecném případě spolu s vysvětlením následuje.

```
aireplay-ng -0 1 -a 00:14:6C:CF:00:00 -c 00:1A:73:68:00:00 mon0
```

```
aireplay-ng -0 <pocet_poslanych_deautentizaci> -a <BSSID>
[-c <MAC_adresa_klienta>] <rozhrani>
```

kde [3]:

- -0 – znamená deautentizační útok. Místo `-0` lze též napsat `--deauth`
- pocet_poslanych_deautentizaci – číselné vyjádření kolik deautentizaci bude posláno. Pokud je použita 0, bude deautentizace posílána neustále. Pro úspěšné zrušení spojení mezi AP a klientem je někdy potřebné odeslání většího množství deautentizací.
- a – označuje, že bude následovat MAC (Media Access Control) adresa přístupového bodu.
- BSSID – vyjadřuje použití konkrétního BSSID (Basic Service Set IDentifier), nebo-li MAC adresy AP.

- -c – předurčuje zadání MAC adresy klienta, který má být odpojen. Pokud by nebyl klient takto specifikován, došlo by k odpojení všech klientů daného AP v dosahu vysílání deautentizace.
- MAC_adresa_klienta – specifikuje konkrétní MAC adresu vybraného klienta.
- rozhrani – odpovídá názvu rozhraní, na němž je spuštěn monitorovací mód.

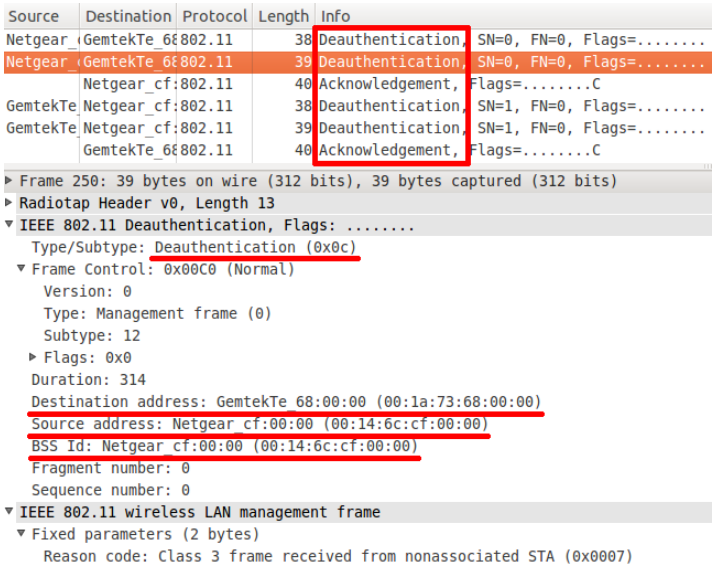
Výstup z odesílání jedné deautentizace může vypadat následovně:

```
Waiting for beacon frame (BSSID: 00:14:6C:CF:00:00) on channel 6
Sending 64 directed DeAuth. STMAC: [00:1A:73:68:00:00] [60|61 ACKs]
```

Nejprve se čeká na příjem rámce beacon od AP. Dále je při každé jednotlivé deautentizaci posíláno 64 rámců na přístupový bod a 64 rámců zadanému klientovi. Část [60|61 ACKs] označuje kolik bylo přijatých potvrzujících odpovědí ACK (ACKnowledgment) a to ve tvaru [ACK od klientů|ACK od AP]. [3].

Pokud je odpovědí méně než 64, došlo ke ztrátě některých rámců. Větší počet odpovědí než 64 může být způsoben právě probíhající aktivní komunikací, popř. vícenásobným příjmem rámců, k čemuž může při aktivovaném monitorovacím módu docházet. [3].

Na obrázku 6.1 je zobrazen zkrácený průběh deautentizace, který byl zachycen v programu Wireshark. Nejprve je odesílána deautentizace od AP Netgear ke klientovi GemtekTE. Následuje potvrzení a posílání deautentizace od klienta k AP, jenž je opět potvrzeno. Podrobněji je ukázán rámec deautentizace od AP ke klientovi, důležité údaje jsou v něm vyznačeny. U deautentizačního rámce v opačném směru jsou na rozdíl od zobrazeného opačně cílová a zdrojová adresa.

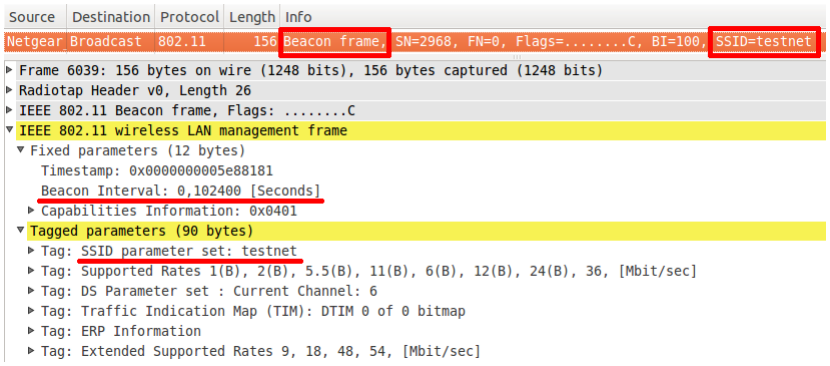


Obr. 6.1: Průběh deautentizace a zobrazení detailu rámce.

7 ZÁKLADNÍ METODY ZABEZPEČENÍ WI-FI

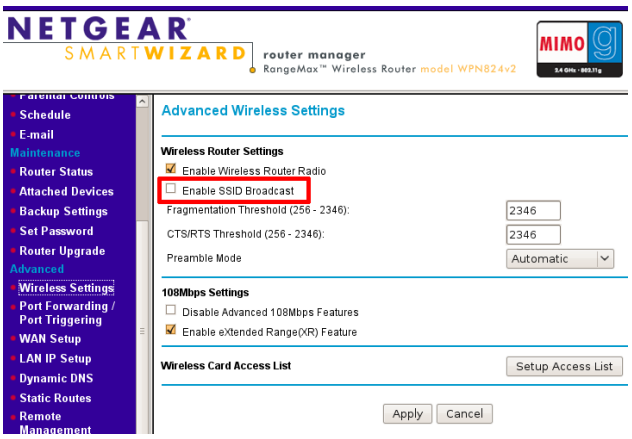
7.1 Skrytí SSID

Aby stanice měly informace o Wi-Fi sítích, které mají ve svém dosahu, ohlašují přístupové body AP svou přítomnost. Dělají to pravidelně opakujícím se vysíláním rámce beacon, např. každých 100 ms. Tento rámec obsahuje mimo jiné i SSID (Service Set IDentifier), nebo-li název sítě (viz obrázek 7.1 z programu Wireshark). Znalost SSID je pro připojení se do požadované Wi-Fi sítě nutná. [5].

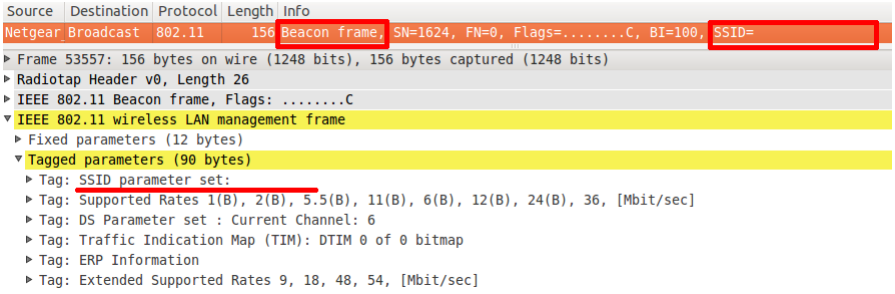


Obr. 7.1: Rámec beacon s vyznačeným SSID a intervalem posílání.

Z bezpečnostního hlediska je vhodnější SSID nevysílat. Tuto volbu nemusí podporovat všechna zařízení, protože není dána normou IEEE 802.11 (Institute of Electrical and Electronics Engineers) [10]. Ukázka volby vypnutí vysílání SSID je znázorněna na obrázku 7.2. Pokud je vysílání SSID vypnuté, posílá AP v rámcích beacon hodnotu SSID jako prázdnou. To lze vidět na obrázku 7.3.



Obr. 7.2: Vypnutí rozesílání SSID u Wi-Fi směrovače.



Obr. 7.3: Rámec beacon se skrytým SSID.

Pro znesnadnění práce potenciálnímu útočníkovi je dobré jako SSID nepoužívat nic, co by prozrazovalo majitele, umístění, či jiné informace o dané síti. A to ani když je SSID skryté.

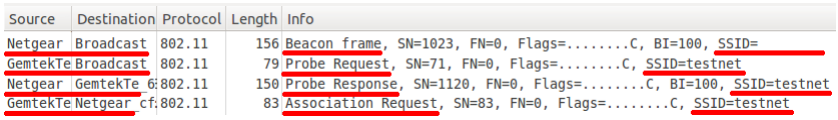
7.1.1 Zjištění skrytého SSID s připojenými klienty

Hodnota SSID je vždy přenášena v nešifrované podobě, takže ji lze monitorováním síťového provozu odposlechnout. Jedná se o pasivní způsob odposlechu, který není možné zjistit. Není proto bezpečné používat pouze tento typ ochrany.

Pro monitorování síťového Wi-Fi provozu je potřeba přepnout síťový adaptér do monitorovacího módu. Postup viz kapitola 5.1.

Nyní již stačí v programu Wireshark aktivovat zachytávání na vytvořeném rozhraní `mon0`.

Skryté SSID lze zjistit z komunikace mezi AP a klienty. Je posíláno v management rámcích association request, probe request a probe response. Viz obrázek 7.4, kde AP představuje zařízení Netgear a klienta zařízení GemtekTe.



Obr. 7.4: Zjištění skrytého SSID.

Pro rychlejší hledání lze v programu Wireshark použít filtry, které zobrazí pouze požadovaný typ rámců [20]:

- association request – `wlan.fc.type_subtype==0`
- probe request – `wlan.fc.type_subtype==4`
- probe response – `wlan.fc.type_subtype==5`

Dále lze zobrazení omezit na vybraný typ rámců (zde použit probe request) pro konkrétní přístupový bod, který je určen svým BSSID (Basic Service Set IDentifier).

A to filtrem `wlan.bssid==xx:xx:xx:xx:xx:xx and wlan.fc.type_subtype==4`, kde `xx:xx:xx:xx:xx:xx` musí být nahrazeno požadovaným BSSID [20].

Přistupuje-li útočník k již vytvořenému spojení a v síti by nebyly posílány rámce probe request a probe response, může se pokusit přerušit spojení mezi AP a vybranou stanicí, popř. i všemi připojenými stanicemi. Postup je uveden v kapitole 6.1. Je pravděpodobné, že se stanice pokusí znovu připojit. V tom případě stačí mít ve Wiresharku zapnuté odchytávání s nastaveným filtrem na association request. Z něho je možné skryté SSID snadno přečíst.

7.1.2 Zjištění skrytého SSID bez připojených klientů

Pokud nejsou k AP připojení žádní klienti, není skryté SSID přenášeno a nelze ho tudíž odposlechnout. Jedinou možností, jak SSID zjistit je útok hrubou silou, kdy se útočník zkouší AP postupně ptát na všechny možné varianty, až do nalezení správné. To provádí posíláním rámců probe request. Popř. slovníkový útok, kdy zkouší stejným způsobem jednotlivá slova z vybraného slovníku. V okamžiku kdy se zeptá na správné SSID, odpoví mu AP rámcem probe response.

Jedná se o aktivní typ útoku, při kterém je posíláno zvýšené množství rámců probe request, což může být monitorováno a vyhodnoceno jako útok.

Když bude posíláno velké množství rámců probe request za sekundu, může se už jednat o útok typu DoS (Denial of Service), protože dojde k zahlcení sítě a ta začne odepírat služby klientům.

Pro tento útok bude využit program MDK3, k němuž lze získat nápovědu zadáním `mdk3 --fullhelp`. Útok může být spuštěn následujícím konkrétním příkazem. Jeho obecná podoba s vysvětlením následuje.

```
mdk3 mon0 p -b m -c 6 -t 00:14:6C:CF:00:00
```

```
mdk3 <rozhrani> p -b <a|l|u|n|c|m> -c <cislo_kanalu> -t <BSSID>
[-s <pakety_za_sekundu>]
```

kde:

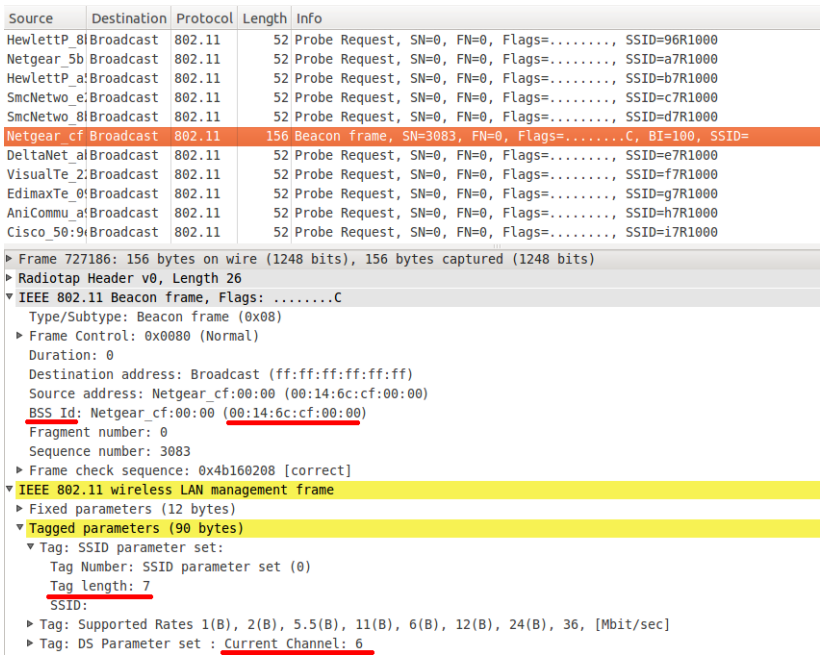
- rozhrani – znamená název rozhraní, na kterém je spuštěn monitorovací mód, viz kapitola 5.1.
- p – označuje mód útoku pro zjištění SSID hrubou silou.
- -b – slouží k aktivaci režimu útoku hrubou silou.
- a – říká, že budou použity všechny kombinace všech tisknutelných znaků, bez ohledu na zjištěnou délku SSID.
- l – určuje použití pouze malých znaků.
- u – značí použití jen velkých znaků.

- n – vyjadřuje použití pouze čísel.
- c – umožní použít malé a velké znaky.
- m – nastaví použití malých znaků, velkých znaků i čísel.
- -c – udává zadání čísla kanálu.
- cislo_kanalu – představuje skutečné číslo kanálu, na kterém AP vysílá (viz obrázek 7.5).
- -t – předesílá zadání BSSID.
- BSSID – oznamuje hodnotu BSSID, AP na které se má útočit, viz obrázek 7.5.
- -s – předchází uvedení frekvence odesílání paketů.
- pakety_za_sekundu – definuje, kolik paketů má být odesláno za sekundu, standartně nastaveno 300.

Na obrázku 7.5 z programu Wireshark je vidět několik rámců probe request, které vysílá program MDK3, při útoku hrubou silou na zjištění skrytého SSID. Aby byl útok rychlejší, zjistí si MDK3 na základě znalosti BSSID cíle útoku počet znaků skrytého SSID. Tuto hodnotu vysílá AP v rámcích beacon. Pak se útok omezí pouze na zjištěný počet znaků.

Jak je dále na obrázku 7.5 vidět, program MDK3 nastavuje pro každý rámec probe request jiného odesílatele. Tím jednak skrývá pravého odesílatele a zároveň vytváří dojem, že dotazy neposílá jedna stanice, ale je jich v okolí velké množství.

Z obrázku 7.5 je patrné, že z rámců beacon, které AP vysílá, lze snadno vyčíst BSSID, počet znaků SSID a číslo kanálu.



Obr. 7.5: BSSID, délka SSID, kanál a útok hrubou silou s MDK3.

Pro slovníkový útok může být použit opět program MDK3. Pro jeho spuštění může sloužit následující konkrétní příkaz. Za ním je uveden jeho obecný tvar a dovysvětleny rozdíly od příkazu k útoku hrubou silou.

```
mdk3 mon0 p -f slovnik.txt -c 6 -t 00:14:6C:CF:00:00
```

```
mdk3 <rozhrani> p -f <umisteni_a_nazev_slovníku>
-c <cislo_kanalu> -t <BSSID> [-s <pakety_za_sekundu>]
```

kde:

- -f – slouží k aktivaci režimu slovníkového útoku, zároveň očekává zadání umístění a název slovníku.
- umisteni_a_nazev_slovníku – vyjadřuje konkrétní umístění a název slovníku, umístění je vyjádřeno vůči domovské složce. Jako slovník je očekáván textový soubor, kde každé slovo je umístěno na novém řádku.

Z útoku hrubou silou je patrné, že z hlediska bezpečnosti je dobré dávat dlouhá SSID (může mít až 32 znaků [10]), protože jejich rozluštění bude trvat mnohem delší dobu. Zároveň je dobré se vyvarovat používání slov, která se vyskytují ve slovníku, aby se zabránilo úspěchu při použití slovníkového útoku.

Použití skrytého SSID může utajit existenci sítě před zcela nezkušeným útočníkem. Použití této ochrany je vhodné zejména u sítí s velmi malým využitím.

8 WEP

WEP (Wired Equivalent Privacy) je standard pro zabezpečení bezdrátových sítí. Jeho cílem je zabezpečit síť na úrovni ekvivalentní s kabelovými sítěmi. Ke své funkci používá symetrickou proudovou šifru RC4 (Ron's Code no. 4). [24].

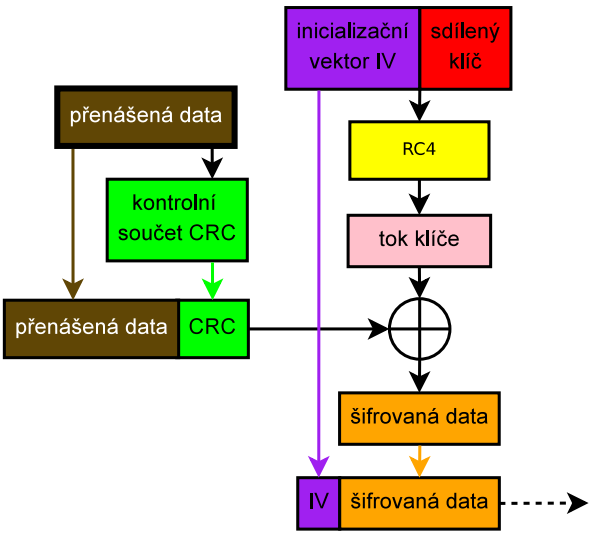
Pro své nedostatky není WEP považován za bezpečný.

8.1 Šifrování zpráv

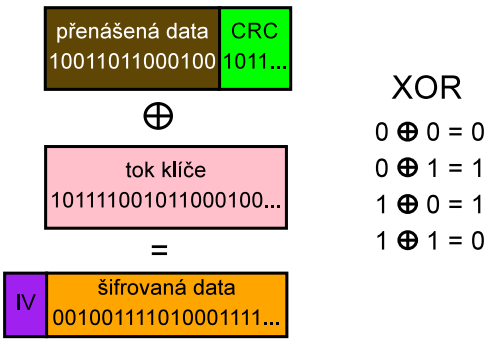
Postup šifrování přenášených dat je ukázán na obrázku 8.1. Z dat, která mají být přenesena, je nejprve vypočítán 32 bitový cyklický redundantní součet CRC (Cyclic Redundancy Check), který bude sloužit pro kontrolu integrity přenesených dat. Hodnota CRC se přidá za přenášená data. Dále je vygenerován inicializační vektor IV (Initialization Vector), který je dlouhý 24 bitů.

Hodnota IV se přidá k tajnému sdílenému klíči a jsou odeslány do generátoru pseudonáhodných čísel RC4. Ten vytvoří proud bitů (tok klíče), který bude stejné délky jakou má IV + sdílený klíč. Tento proud bitů bude použit k šifrování.

Nyní se pomocí operace XOR (exkluzivní disjunkce) spojí přenášená data + kontrolní součet a proud bitů z RC4. Tím jsou data zašifrována. Před přenosem se před ně ještě přidá hodnota IV a mohou se poslat. Zjednodušenou podobu s konkrétními hodnotami lze vidět na obrázku 8.2. [5, 24].



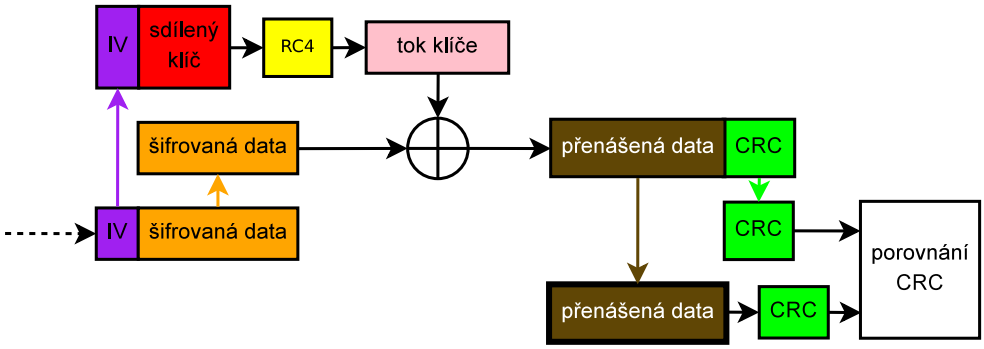
Obr. 8.1: Proces šifrování protokolem WEP [5, 34].



Obr. 8.2: Zjednodušený proces šifrování, XOR [5].

8.2 Dešifrování zpráv

Dešifrování zprávy u příjemce probíhá opačným postupem. Od zašifrovaných dat se oddělí IV, který se přidá ke sdílenému klíči. Společně projdou stejným generátorem pseudonáhodných čísel jako při šifrování. Tím je získán stejný tok bitů, jakým byla zpráva zašifrována. Tento tok bitů je přiveden spolu se šifrovanými daty na operaci XOR. Výsledkem jsou původní data. Pro ověření jejich neporušenosti se vypočítá jejich kontrolní součet CRC, který se porovná s vytvořeným před zašifrováním. Celý postup je možno vidět na obrázku 8.3. [24].



Obr. 8.3: Proces dešifrování protokolem WEP [10].

8.3 Autentizace

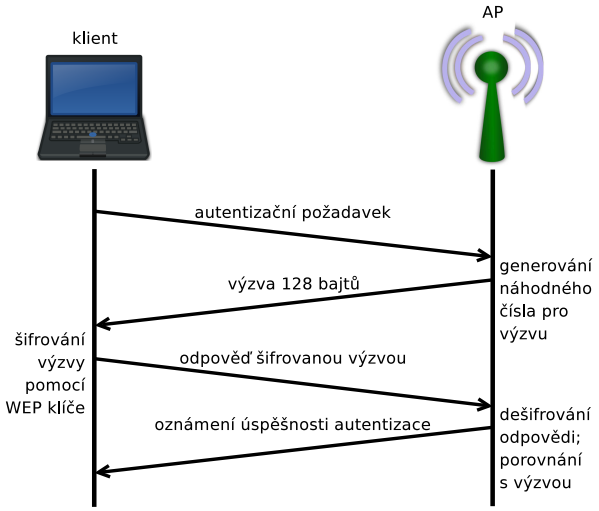
Specifikace 802.11 umožňuje při používání WEP dva způsoby autentizace. Jde o otevřený systém a systém se sdíleným klíčem. Jedná se pouze o jednosměrné autentizování stanic. Přístupový bod se neautentizuje. [6, 34].

8.3.1 Otevřený systém

Otevřený systém autentizace je výchozí volbou 802.11. Přihlašovaný klient není v tomto případě nijak prověřován. Klient pošle autentizační rámec, ve kterém je obsaženo SSID. AP tento rámec bez ověřování přijme a odpoví potvrzením. [21, 34].

8.3.2 Sdílený klíč

Postup autentizace pomocí sdíleného klíče je ukázán na obrázku 8.4. Stanice, která se chce připojit, pošle přístupovému bodu autentizační požadavek. Na to AP odpoví náhodně vygenerovanou výzvou. Klient tuto zprávu s pomocí WEP klíče zašifruje a pošle zpět na AP. Přístupový bod zprávu dešifruje a porovná s poslanou výzvou. Když se zprávy shodují, pošle klientovi zprávu o úspěšné autentizaci, v opačném případě o neúspěšné. [5].



Obr. 8.4: Autentizace sdíleným klíčem [5, 6, 15].

Autentizace je založena na znalosti WEP klíče, který je uložen na AP a případně i na klientské stanice. Nejde tedy o ověření osoby uživatele [21].

Nevýhodou autentizace se sdíleným klíčem je, že si útočník může odposlechnout nezašifrovanou výzvu a posléze i zašifrovanou odpověď. Provede-li útočník XOR těchto zpráv, získá šifrovací sekvenci. Když nyní útočník požádá AP o autentizaci a k zašifrování výzvy použije získanou šifrovací sekvenci, bude rovněž úspěšně autentizován. [5].

8.4 Útok na WEP

Nejprve je potřeba si odchytit dostatečné množství dat. K tomu bude použit program Airodump-ng a balíku Aircrack-ng. Manuál je k dispozici v [3]. Dostupné sítě se zobrazením všech potřebných parametrů si lze najít zadáním následujícího příkazu.

```
airodump-ng <rozhrani_v_monitorovacim_modu>
```

V konkrétní možné podobě:

```
airodump-ng mon0
```

Zde se vybere vhodná síť na kterou bude proveden útok. Parametrem -w se specifikuje název souboru, do kterého se budou ukládat zachycená data. Dále se uvede za parametrem -c číslo kanálu, na kterém AP vysílá. Poslední před názvem rozhraní v monitorovací modu, přes které se bude zachytávat se specifikuje za parametrem --bssid konkrétní BSSID.

```
airodump-ng [-c <cislo_kanalu>] [-w <nazev_souboru>]
[--bssid <MAC_adresa_AP>] <rozhrani_v_monitorovacim_modu>
```

Např. takto:

```
airodump-ng -c 6 -w zaznamenana_data --bssid 00:14:6C:CF:BA:0C mon0
```

V novém okně terminálu lze zkoušet, jestli odchycené množství dat již není dostatečné (to většinou bývá kolem jednotek až desítek tisíc odchycených IV). Stačí spustit program Aircrack-ng ze stejnojmenného balíku a zadat mu jako parametr název souboru se zachycenými daty. Za zadaný název souboru se přidává -01 a koncovka .cap.

```
aircrack-ng <nazev_souboru-01.cap>
```

```
aircrack-ng zaznamenana_data-01.cap
```

Po krátké chvíli program buď ohlásí nedostatečné množství dat, nebo oznámí úspěch a správný WEP klíč.

Program Aircrack-ng je velmi efektivní. Ke své činnosti používá kombinaci více metod útoků. Jedná se o metody: PTW (Pychkine, Tews, Weinmann), FMS (Fluhrer, Mantin, Shamir) – statistické metody, korek – statistické metody a hrubou silou [3].

9 WPS

WPS (Wi-Fi Protected Setup) je certifikační program od Wi-Fi aliance (nezisková organizace složená ze stovek firem působících v oblati Wi-Fi technologií), který započal na začátku roku 2007. Jeho hlavním cílem je zjednodušení konfigurace zabezpečení Wi-Fi sítí. Zaměřuje se při tom na oblast domácích a malých firemních Wi-Fi sítí. [32].

WPS má co nejjednoduším způsobem zajistit, aby i člověk zcela neznalý problematiky zabezpečení Wi-Fi sítí mohl provozovat svou Wi-Fi síť s vysokou úrovní zabezpečení. Takový uživatel pomocí jednoduchých úkonů spustí proces automatického nastavení bezpečnosti a nemusí dále nikde nic nastavovat. Proto bývá WPS ve výchozím stavu zapnuté, aby daný uživatel nemusel dělat ani tento úkon.

Motivací pro zavedení technologie WPS je snadná dostupnost a vysoká rozšířenost Wi-Fi zařízení, jenž se dostávají k lidem, kteří mají o jejich zabezpečení minimální nebo nulové znalosti. Takoví uživatelé potom provozují svou Wi-Fi síť nezabezpečenou nebo se zabezpečením na nedostatečné úrovni. Čímž se ocitají v ohrožení, o němž a jeho možných následcích často nemají tušení.

Aby mohla technologie WPS fungovat, musí být podporována na přístupovém bodu i klientské stanici. Zařízení, která tuto podporu nemají, mohou být nakonfigurována ručně.

9.1 WPS na TP-LINK TL-WR1043ND

Tento směrovač obdržel certifikát od Wi-Fi aliance 30.11.2009 [31]. Nicméně certifikaci na WPS neobsahuje. Technologii WPS ovšem používá a označuje svým vlastním názvem QSS.

9.2 Princip fungování WPS

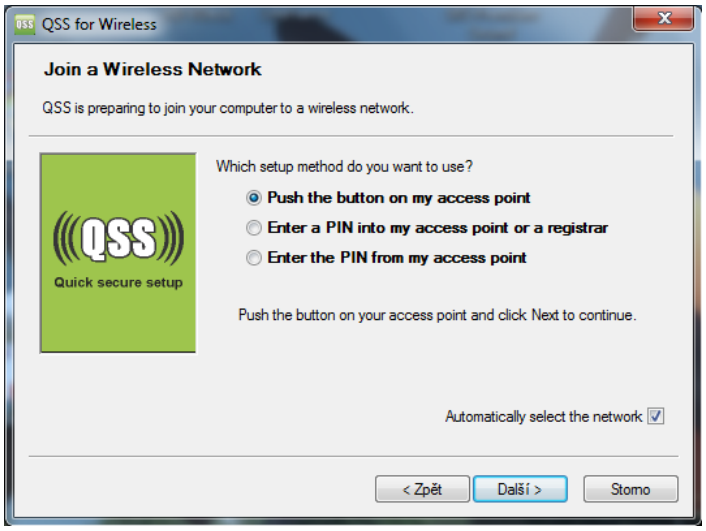
9.2.1 Role zařízení

WPS definuje 3 možné role v jakých se zařízení nacházejí [29, 13]:

- **Žadatel** – jde o nové zařízení, které nezná údaje potřebné pro přihlášení k Wi-Fi síti a snaží se k ní připojit.
- **Registrátor** – je zařízení, jehož úkolem je prověřit žadatele a když vyhoví, poskytnout mu údaje nutné pro přihlášení do dané Wi-Fi sítě.
- **Přístupový bod** (AP) – představuje zařízení, které slouží jako prostředník mezi žadatelem a registrátorem. Žadatel se pomocí něj může připojit k Wi-Fi síti. V praxi bývá registrátor často součástí přístupového bodu.

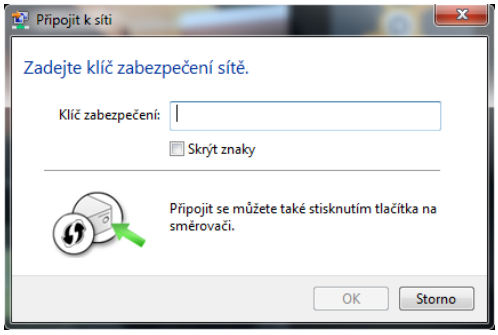
9.2.2 Metody přihlašování

Používají se v podstatě 3 metody, pomocí kterých se může žadatel připojit k Wi-Fi síti, viz obrázek 9.1, který je z programu QSS dodávaný firmou TP-LINK, [29]:



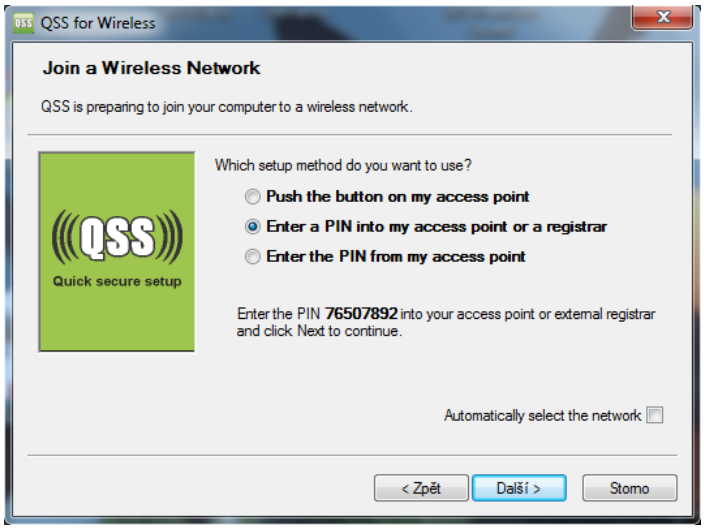
Obr. 9.1: Výběr metod WSP v programu QSS.

- **PBC** (Push Button Configuration) – je metoda, která využívá stisku tlačítek. Uživatel musí stisknout tlačítko na stanici, která se má připojit (žadatel) a na přístupovém bodu (eventuálně na registrátorovi). Tlačítka mohou být na zařízení přítomna fyzicky nebo mohou být realizována softwarově (např. v operačním systému). Fyzické a softwarové tlačítko je možno vidět na obrázcích: 3.1, 9.1, 9.2, 9.4. Po stisknutí tlačítka na AP bude funkce aktivní po omezenou dobu (např. 2 minuty) nebo než bude žadatel ověřen.

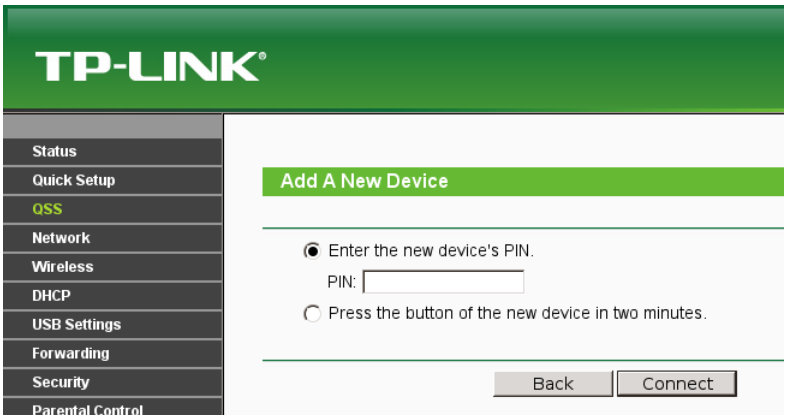


Obr. 9.2: Funkce softwarové tlačítka ve Windows 7.

- **PIN** (Personal Identification Number) – **interní registrátor** – PIN se může nacházet napsaný fyzicky přímo na žadateli, nebo může být generován softwarově, viz obrázek 9.3 Je třeba ho zapsat do přístupového bodu (např. pomocí webového rozhraní), jak ukazuje obrázek 9.4.



Obr. 9.3: Ukázka softwarově vygenerovaného PINu žadatele, jenž je třeba zadat do AP.

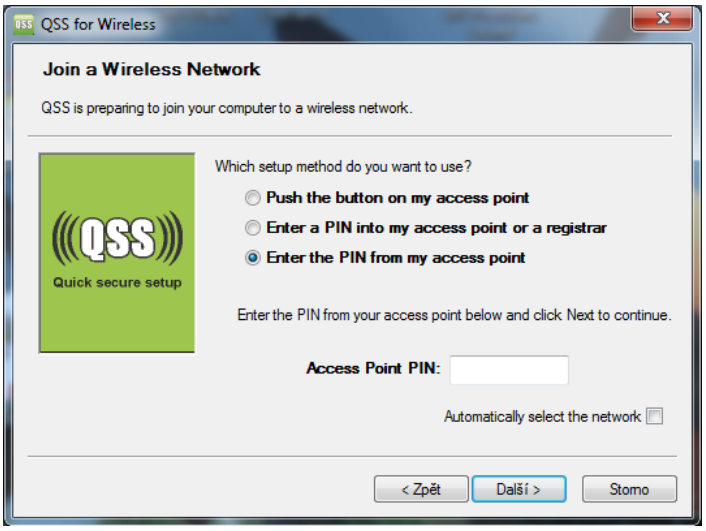


Obr. 9.4: Funkce interního registrátoru a softwarového tlačítka ve webovém rozhraní směrovače.

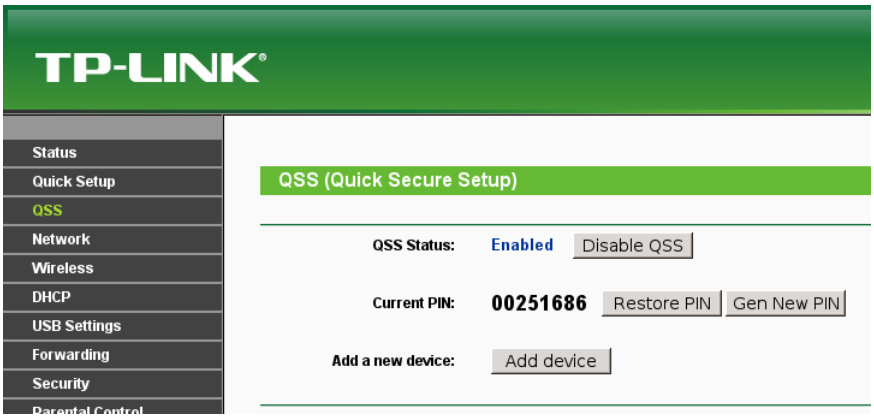
- **PIN – externí registrátor** – PIN který je fyzicky napsán nebo generován (např. přes webové rozhraní) na přístupovém bodu, jak ukazují obrázky 9.5 a 9.7, se zapíše do žadatele, viz obrázek 9.6.

Obr. 9.5: PIN fyzicky nalepený na štítku AP.

Existují i další metody, které si zajišťují výměnu přihlašovacích údajů jinou cestou než přes Wi-Fi. Ty se ovšem nepoužívají.



Obr. 9.6: Místo pro zadání AP PINu v žadateli.



Obr. 9.7: AP PIN vygenerovaný ve webovém prostředí směrovače.

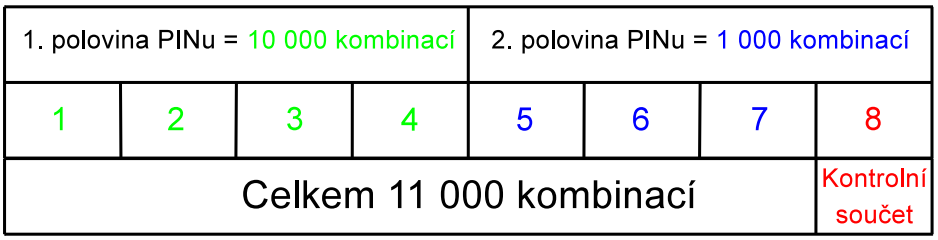
Z hlediska přístupového bodu musí mít při metodě PBC uživatel k AP fyzický přístup, u metody PIN – interní registrátor se musí uživatel dostat k webovému rozhraní v AP a u metody PIN – externí registrátor stačí mít znalost AP PINu [29].

9.3 Útok na AP PIN

Na konci roku 2011 byla publikována bezpečnostní slabina v přihlašování pomocí metody PIN – externí registrátor. PIN je složen z 8 číslic, což představuje $10^8 = 100\,000\,000$ možných kombinací. Při útoku hrubou silou, kdy se zkouší postupně všechny možnosti než se najde správná, by prolomení mohlo trvat velmi dlouho. Při ideálních podmínkách (bez rušení pásma, ztrátovosti, ...) by při průměrné rychlosti 1 pokus za sekundu trvalo vyzkoušení všech kombinací přibližně 3,17 roku. [33].

Objevená bezpečnostní chyba značným způsobem snižuje počet možných kombinací. Když přístupový bod obdrží špatný PIN, informuje o tom žadatele. Z této odpovědi je ovšem patrné jestli 1. nebo 2. polovina PINu byla správná. Zároveň má poslední číslice význam kontrolního součtu předchozích číslic. To je znázorněno na obrázku 9.8. 1. polovina představuje 10^4 možných kombinací a 2. polovina 10^3, což v součtu dává 11 000 možností.

To při stejném modelu útoku hrubou silou (1 pokus za sekundu) činí přibližně 3,06 hodin, nicméně ve skutečnosti vychází doba trvání jednoho pokusu asi na 3 sekundy, tj. přibližně 9,17 hodin na otestování všech možností, což ovšem nemusí být potřeba.

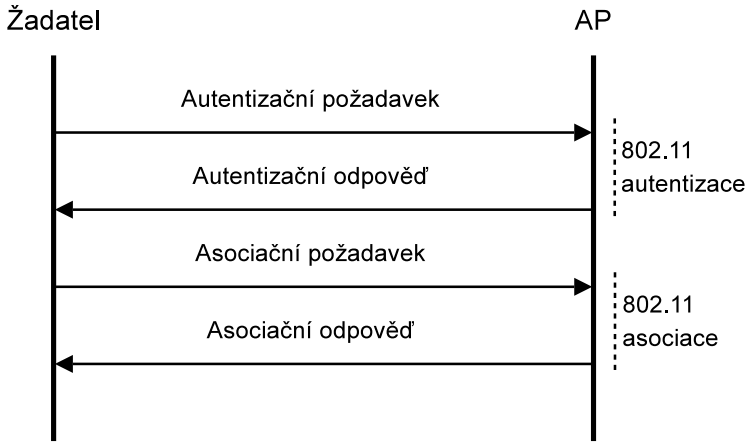


Obr. 9.8: Struktura AP PINu [29].

K provádění útoku hrubou silou slouží skript wpscrack.py (autor Stefan Viehböck) a program Reaver (autor Craig Heffner).

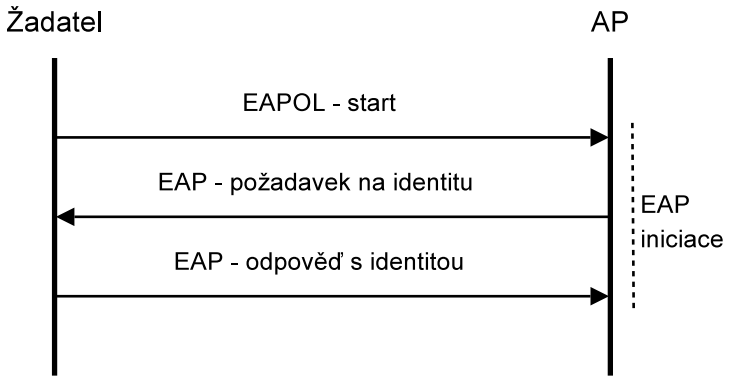
9.3.1 Princip přihlašování metodou PIN – externí registrátor

Na základě uživatelova podnětu na připojení k síti je zahájena následující výměna zpráv mezi zúčastněnými stranami. Nejprve dojde k autentizaci a asociaci podle IEEE 802.11, viz obrázek 9.9.



Obr. 9.9: Autentizace a asociace dle 802.11 [29].

Následuje zahájení výměny EAP (Extensible Authentication Protocol) zpráv jak je vidět na obrázku 9.10.



Obr. 9.10: Zahájení EAP výměny [29].

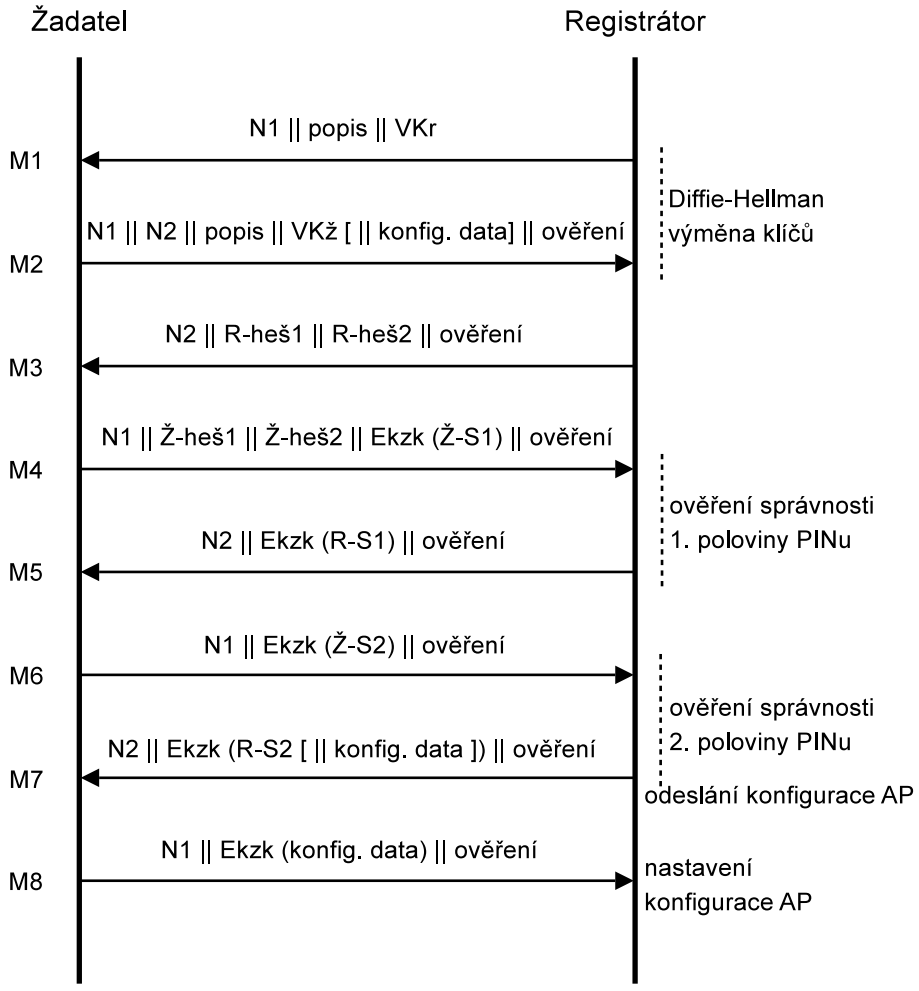
Poslední fází je výměna EAP zpráv podle WPS. Tato komunikace je rozdělena do 8 zpráv, M1 až M8. Na obrázku 9.11 je ukázán průběh této výměny a co je obsahem jednotlivých zpráv. Obrázek vychází z implementace WPS společností Microsoft v mechanizmu Windows Connect Now [2].

Všechny zprávy M1 až M8 obsahují typ registračního protokolu, to nebylo pro zjednodušení v obrázku 9.11 zaznamenáno. Znaky || představují spojení parametrů, které utvářejí danou zprávu. [30].

Význam jednotlivých parametrů zpráv z obrázku 9.11 je následující [30, 29]:

- **N1** – představuje 128 bitový náhodný řetězec (nonce), jenž vygeneroval registrátor.
- **popis** – obsahuje údaje popisující dané zařízení (např. výrobce, model, MAC adresu, ...).
- **VKr** – veřejný Diffie-Hellman klíč registrátora.
- **N2** – představuje 128 bitový náhodný řetězec (nonce), jenž žadatel vygeneroval.
- **VKž** – veřejný Diffie-Hellman klíč žadatele.
- **konfig. data** – obsahují informace o nastavení a zabezpečení sítě.
- **ověření** – představuje ověřovací atribut, který obsahuje hešovací funkci HMAC-SHA-256 prováděnou nad předchozí a aktuální zprávou s využitím autentizačního klíče. HMACaut.klíč(předchozí zpráva || aktuální zpráva).
- **auth.klíč** – je odvozen z Diffie-Hellmanova $g^{AB} \mathrm{mod}\ p$, N1, N2 a MAC adresy.
- **R-hešl** – doložení znalosti 1. poloviny **svého** PINu.
  R-hešl = HMACaut.klíč(R-S1 || PSK1 || VKž || VKr), kde **R-S1** = 128 náhodných bitů a **PSK1** = prvních 128 bitů z HMACaut.klíč(1. poloviny PINu).

- **R-hešŽ** – doložení znalosti 2. poloviny **svého** PINu.
  R-hešŽ = HMACaut.klíč(R-S2 || PSK2 || VKž || VKr), kde **R-S2** = 128 náhodných bitů a **PSK2** = prvních 128 bitů z HMACaut.klíč(2. poloviny PINu).
- **Ž-hešŽ1** – doložení znalosti 1. poloviny **registrátorova** PINu od žadatele.
  Ž-hešŽ1 = HMACaut.klíč(Ž-S1 || PSK1 || VKž || VKr), kde **Ž-S1** = 128 náhodných bitů.
- **Ž-hešŽ2** – doložení znalosti 2. poloviny **registrátorova** PINu od žadatele.
  Ž-hešŽ2 = HMACaut.klíč(Ž-S2 || PSK2 || VKž || VKr), kde **Ž-S2** = 128 náhodných bitů.
- **Ekzk** () – je šifrovaní hodnot uvedených v závorkách symetrickou blokovou šifrou AES-CBC (Advanced Encryption Standard) (Cipher-Block Chaining).

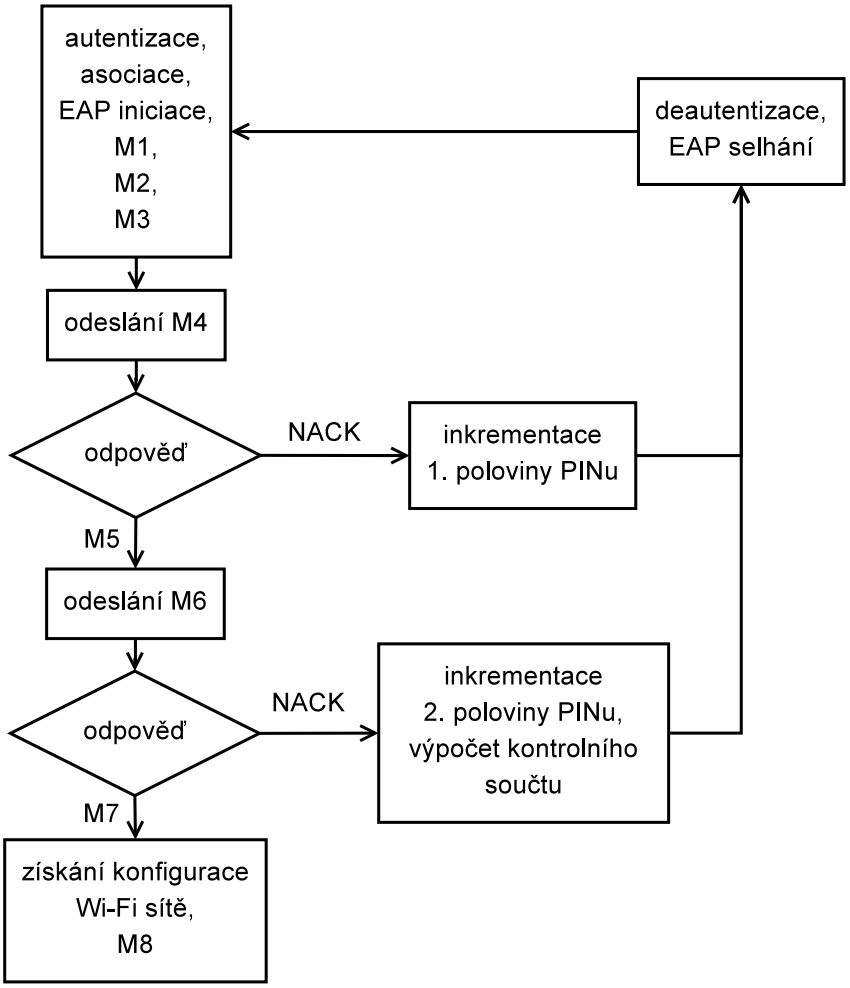


Obr. 9.11: Výměna EAP zpráv u WPS dle Windows Connect Now [30, 29].

9.3.2 Princip útoku na přihlašování metodou PIN – externí registrátor

Z obrázku 9.11 a jeho popisu je patrné, že z odpovědi, kterou pošle registrátor na zprávu M4, žadatel pozná jestli 1. polovina PINu, kterou žadatel odeslal byla správná – přijde M5, nebo špatná – přijde NACK (Negative ACKnowledgment). Když uhodne 2. polovinu přijde od registrátora odpověď M7. Celé to znázorňuje obrázek 9.12.

Na tom je postavený útok na tuto metodu. Útočník postupně zkouší uhodnout nejprve 1. polovinu PINu (10 000 možností) a následně 2. polovinu (1 000 možností).



Obr. 9.12: Schéma útoku na metodu PIN – externí registrátor [29].

9.3.3 Praktická realizace útoku

Tento útok byl vyzkoušen pomocí programu Reaver 1.4. Prvním krokem je přepnutí rozhraní do monitorovacího módu, postup viz kapitola 5.1. Pro spuštění je třeba

znát MAC adresu AP (BSSID). Tu lze zjistit vícero způsoby (odposlechnutím rámce beacon ve Wiresharku, pomocí balíku Aircrack-ng, ze síťového manažera Wicd, ...). Při zadání `reaver` vyběhne nápověda se syntaxí a možnostmi programu.

Útok lze spustit zadáním příkazu v minimálně tomto tvaru:

```
reaver -i <rozhrani_v_monitorovacim_modu> -b <BSSID>
```

Konkrétně byl použit následující příkaz, který provádí podrobné vypisování průběhu útoku:

```
reaver -i mon0 -b 74:EA:3A:A2:CA:C6 -vv
```

Začátek průběhu útoku je potom ukázán na následujícím výpisu. Je z něho patrný průběh komunikace, který byl popsán dříve. Význam jednotlivých řádků je z názvů a předchozího popisu zřejmý.

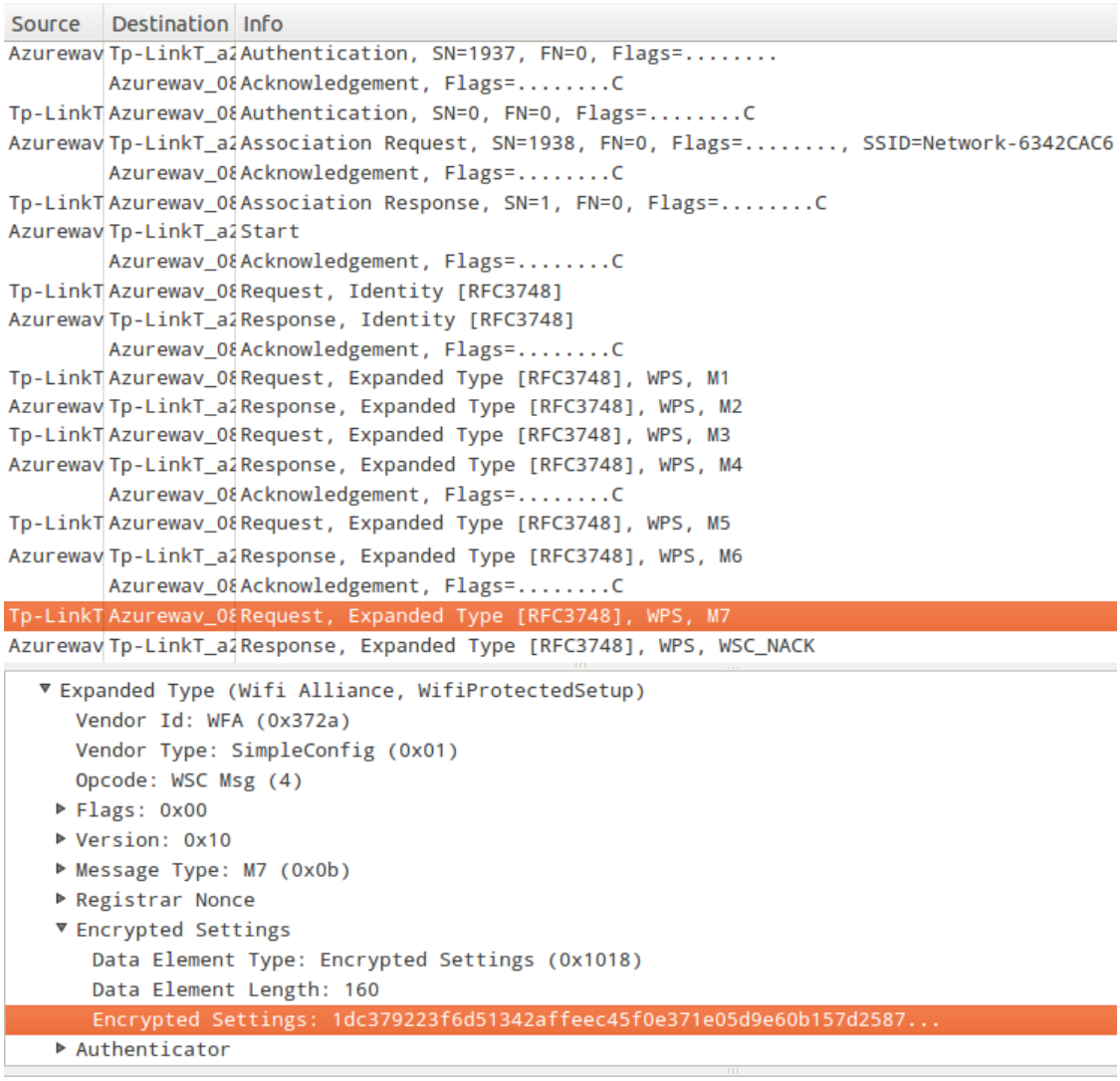
```
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner
<cheffner@tacnetsol.com>
[+] Waiting for beacon from 74:EA:3A:A2:CA:C6
[+] Switching mon0 to channel 4
[+] Associated with 74:EA:3A:A2:CA:C6 (ESSID: Network-6342CAC6)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00005678
```

Útok je možné kdykoliv přerušit pomocí ctrl+c, program si sám uloží dosavadní výsledky a po novém spuštění se zeptá, jestli má pokračovat od místa kde naposledy skončil.

Po dokončení útoku program vypíše zjištěné údaje, jak je ukázáno dále:

```
[+] Pin cracked in 856 seconds
[+] WPS PIN: '00251686'
[+] WPA PSK: '261FAA1467AD4B920CA204DEFB98170992C7EAAC9929A12974DDF23
39DCA3591'
[+] AP SSID: 'Network-6342CAC6'
```

Průběh útoku byl monitorován programem Wireshark a následující obrázek 9.13 ukazuje poslední úspěšnou výměnu. Na obrázku je Azurewav útočník a Tp-LinkT je AP a registrátor v jednom. Jelikož se útočník nechce připojit, po zprávě M7 zasílá žadatel zprávu NACK. Dole je ukázán obsah zprávy M7, který posílá přihlašovací údaje k síti (zvýrazněno). Z obrázku je zároveň patrný průběh celé komunikace, jak byla popsána dříve.



Obr. 9.13: Zkrácený záznam útoku zachycený programem Wireshark.

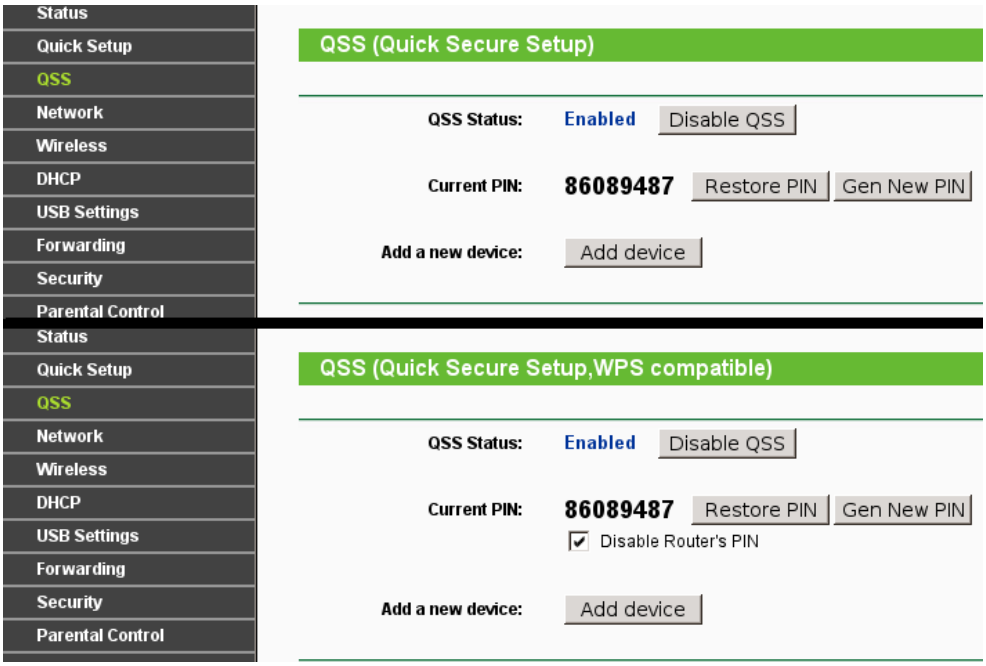
9.4 Obrana proti útoku na přihlašování metodou PIN – externí registrátor

Možnost tohoto útoku představuje poměrně velký bezpečnostní problém. WPS je implementováno na většině moderních Wi-Fi směrovačích určených pro domácí a malé firemní sítě. Většinou bývá ve výchozím stavu zapnuté a na některých modelech ani nejde vypnout.

Obranné mechanizmy je možno implementovat v nových firmwarech, nicméně z hlediska cílové skupiny pro tyto zařízení (lidé s minimálními a žádnými znalostmi v oblasti bezpečnosti Wi-Fi sítí), nelze příliš předpokládat, že si tito lidé budou sami do svých zařízení nahrávat nový firmware. Nesledují-li ani zprávy z této oblasti, nemají o této bezpečnostní chybě, která jim reálně hrozí, ani ponětí.

9.4.1 Obrana od TP-LINK na směrovači TL-WR1043ND

Společnost TP-LINK zareagovala na tuto bezpečnostní chybu, u tohoto směrovače, vydáním nového firmwaru 10.2.2012 s označením „TL-WR1043ND_V1_120210“. V něm přidala možnost vypnutí přihlašování pomocí AP PINu ve webovém rozhraní a dále omezila počet neúspěšných pokusů. Při více neúspěšných pokusech (asi 10) se přihlašování touto metodou vypne. Pro opětovné zapnutí je třeba navštívit webové rozhraní a volbu opět povolit. Ukázka změny oproti předešlému firmwaru z 6.5. 2011 „TL-WR1043ND_V1_110429“ je vidět na obrázku 9.14.



Obr. 9.14: Ukázka ve změně firmwaru, nahoře starší a dole novější verze.

10 ZPROVOZNĚNÍ WPS NA OPENWRT

Ve výchozím stavu, tj. po nahrání firmwaru staženého z [11], nejsou funkce technologie WPS k dispozici. Pro zprovoznění WPS je potřeba nainstalovat balíčky „wpad“ a „hostapd-utils“ [19]. Výchozí firmware obsahuje balíček „wpad-mini“, což je minimalistická verze balíčku „wpad“. Proto je nejprve nutno „wpad-mini“ odinstalovat. To lze provést příkazem:

```
opkg remove wpad-mini
```

Ovšem ani po nainstalování uvedených balíčků z repozitáře OpenWrt, čili zadáním `opkg install wpad hostapd-utils`, není WPS k dispozici. To lze snadno ověřit příkazem:

```
hostapd_cli -h
```

Pokud by WPS k dispozici bylo, obsahoval by výpis po zadání tohoto příkazu mimo jiné:

```
wps_pin <uuid> <pin> [timeout] [addr]  add WPS Enrollee PIN
wps_check_pin <PIN>  verify PIN checksum
wps_pbc              indicate button pushed to initiate PBC
wps_ap_pin <cmd> [params..]  enable/disable AP PIN
wps_config <SSID> <auth> <encr> <key>  configure AP
```

Řešením je stáhnutí zdrojových kódů těchto balíčků, odkomentovat řádky týkající se WPS a provést křížovou kompilaci [14].

10.1 Křížová kompilace balíčků pro OpenWrt

Zařízení pro která je OpenWrt určen mají značně omezené výpočetní možnosti. Proto by kompilování pomocí nich bylo značně složité a hlavně zdlouhavé. Zároveň disponují malou velikostí paměti. Proto v nich nástroje potřebné pro kompilaci nejsou obsaženy. Kompilování tedy musí proběhnou na jiném stroji.

Při kompilování se běžně vytváří balíček, který je použitelný na procesorech se stejnou architekturou na jaké kompilace proběhla. Jelikož v použitém směrovači se nenachází procesor se stejnou architekturou jako v běžném počítači, balíček zkompilovaný na počítači, by ve směrovači nefungoval. Existuje ale možnost křížové kompilace, která umožní provést kompilaci tak, aby běžela na hostitelském systému (počítač) a vytvářela balíček pro cílový systém (směrovač). [16].

10.1.1 Příprava na křížovou kompilaci

Křížová kompilace bude prováděna v operačním systému Ubuntu 12.04. Z důvodu aktuálnějších verzí bude využita vývojová verze (trunk).

Vše je třeba dělat pod uživatelským účtem (ne root). Nejprve bude nainstalován nástroj subversion (zkráceně svn). [17]. A to následujícím příkazem:

```
sudo apt-get install subversion build-essential
```

Po jeho zadání bude vyžadováno zadání hesla správce systému, což předesílá `sudo`. Dalším krokem je vytvoření složky v domovském adresáři, jejíž název nebude obsahovat mezery (ty se nesmí vyskytnout ani v celé cestě k adresáři), např. openwrt. Do této složky je třeba vstoupit a následně do ní budou pomocí nástroje svn staženy a uloženy zdrojové soubory. Pak vstoupit do složky trunk. [17]. K tomu lze použít příkazy:

```
mkdir ~/openwrt
cd openwrt
svn co svn://svn.openwrt.org/openwrt/trunk
cd trunk
```

Pro spuštění křížové kompilace je nezbytné, aby hostitelský počítač obsahoval všechny potřebné balíčky. Jestli je obsahuje lze zjistit zadáním některého z následující příkazů [17]

```
make defconfig
make prereq
make menuconfig
```

Když je odezvou chyba, některý z balíčků chybí. Který, to lze identifikovat z výpisu a také lze použít tabulku potřebných balíčků, která je uvedena v [17]. V Ubuntu se instalace provede pomocí `sudo apt-get install nazev_balicku`. V základní instalaci Ubuntu 12.04 je potřeba zadat následující příkaz, který nainstaluje uvedené balíčky:

```
sudo apt-get install zlib1g-dev flex git-core gawk libncurses5-dev
```

Povolení WPS je potřeba provést v souboru ∼/openwrt/trunk/package/hostapd/files/hostapd-full.config a sice odstraněním znaku `#` ve 2. a 4. řádku v následující části:

```
# Wi-Fi Protected Setup (WPS)
#CONFIG_WPS=y
# Enable UPnP support for external WPS Registrars
#CONFIG_WPS_UPNP=y
```

Je vhodné v ∼/openwrt/trunk/package/hostapd/Makefile pozměnit verzi, aby byly balíčky snadno odlišitelné, např. na:

```
PKG_VERSION:=20120428-s-WPS
```

Pro usnadnění je možné využít upravené verze souboru hostapd.sh (oproti původnímu souboru obsahuje předpřipravené možnosti pro WPS), jenž lze stáhnout z [14] a nahradit jím stejnojmenný soubor v ∼/openwrt/trunk/package/hostapd/files.

Další úpravou ve stejném umístění je opravení souboru wps-hotplug.sh, který obsahuje špatný název tlačítka. Tento soubor by bylo možné opravit i později v samotném systému (v umístění etc/hotplug.d/button/50-wps). V prvním řádku je třeba přepsat wps na BTN_1, takže bude vypadat takto:

```
if [ "$ACTION" = "pressed" -a "$BUTTON" = "BTN_1" ]; then
```

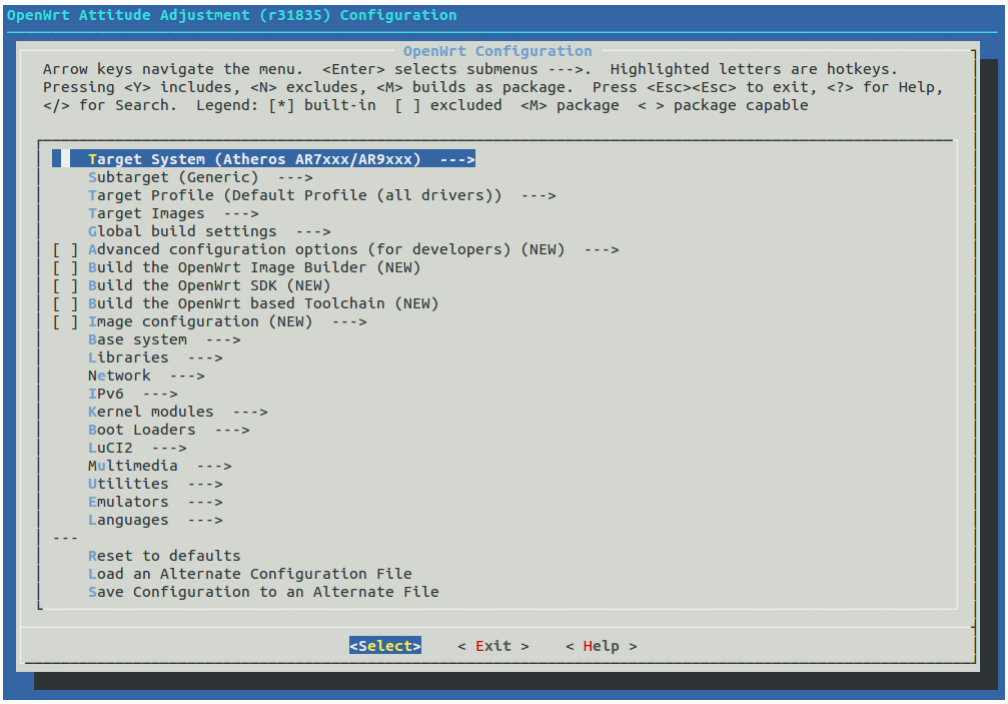
Touto opravou je umožněno fungování tlačítkové metody WPS.

10.1.2 Postup křížové kompilace

Dalším potřebným krokem je spuštění konfiguračního menu příkazem:

```
make menuconfig
```

V něm je potřeba nastavit cílovou architekturu (Target System) na „Atheros AR7xxx/AR9xxx“ a v části „Network“ vybrat potřebné balíčky wpad a hostapd-utils (pomocí M), zároveň je nutno zrušit výběr balíčku wpad-mini. Podobu konfiguračního menu ukazuje obrázek 10.1.



Obr. 10.1: Konfigurační menu.

Pak musí následovat příkazy:

```
make tools/install
make toolchain/install
```

Nakonec se spustí kompilace balíčků zadáním:

```
make package/hostapd/compile
```

Požadované balíčky jsou totiž postaveny na hostapd. Dokumentace a zdrojové kódy k hostapd jsou umístěny v [9].

Vytvořené balíčky se nacházejí v ~/openwrt/trunk/bin/ar71xx/packages.

10.2 Instalace vytvořených balíčků

Vytvořené balíčky je potřeba nakopírovat do směrovače, k tomu poslouží následující příkazy:

```
scp ~/openwrt/trunk/bin/ar71xx/packages/wpad_20120428-s-WPS-1_ar71xx.
ipk root@192.168.1.1:/
scp ~/openwrt/trunk/bin/ar71xx/packages/hostapd-utils_20120428-s-WPS-
1_ar71xx.ipk root@192.168.1.1:/
```

Balíčky se nyní nacházejí v kořenovém adresáři, proto je potřeba do něj vstoupit a balíčky nainstalovat:

```
cd /
opkg install wpad_20120428-s-WPS-1_ar71xx.ipk
opkg install hostapd-utils_20120428-s-WPS-1_ar71xx.ipk
```

10.3 Konfigurace WPS na OpenWrt

V /etc/config/wireless je potřeba nastavit základní parametry Wi-Fi sítě (název sítě, zabezpečení, ...). To je možné provést manuální zápisem do /etc/config/wireless, nebo pomocí uci, jak je to provedeno a okomentováno dále:

```
uci set wireless.@wifi-device[0].channel=auto
#automaticky vyber kanalu
uci set wireless.@wifi-device[0].country=CZ #nastaveni zeme
uci set wireless.@wifi-device[0].disabled=0 #povoleni zapnuti Wi-Fi

uci set wireless.@wifi-iface[0].ssid=testnet #nazev site
uci set wireless.@wifi-iface[0].key=**heslo**
#klic pro prihlaseni bez WPS
uci set wireless.@wifi-iface[0].wpa_psk_file=/etc/config/hostapd.wps
#soubor pro ukladani automaticky generovanych klicu a MAC adres
uci set wireless.@wifi-iface[0].encryption=wps
#sifrovani zajistuje WPS
uci set wireless.@wifi-iface[0].os_version=00000000 #verze os
uci set wireless.@wifi-iface[0].config_methods='label display
push_button keypad' #metody prihlaseni

uci commit wireless #zapise predchozi zmeny
wifi #zapne Wi-Fi
```

Pokud systém hlásí, že nemůže číst z /dev/random a má nedostatečnou entropii, je to možné provizorně vyřešit zadáním:

```
mv /dev/random /dev/random.original
#prejmenuje random na random.original
ln -s /dev/urandom /dev/random
#vytvori symbolicky odkaz z unrandom na random
```

V této fázi je již funkční tlačítková metoda WPS. Alternativní možností ke zmáčknutí tlačítka je zadání příkazu:

```
hostapd_cli -p /var/run/hostapd-phy0 wps_pbc
```

Pro metodu PIN – interní registrátor, kdy je do AP zapsán PIN žadatele lze využít příkaz:

```
hostapd_cli -p /var/run/hostapd-phy0 wps_pin <uuid> <pin> [timeout]
[addr]
```

Povinnými parametry jsou `uuid` a `pin`, kde místo uuid žadatele lze použít `any` a položka `pin` musí obsahovat PIN žadatele. Nepovinným parametrem `timeout` lze omezit dobu (uvedenou v sekundách) po jakou má možnost žadatel požádat o připojení, popř. lze uvést jeho MAC adresu v `addr`.

Pro metodu PIN – externí registrátor je možností více. Lze ji zcela vypnout zadáním:

```
hostapd_cli -p /var/run/hostapd-phy0 wps_ap_pin disable
```

PIN může být náhodně generován a omezen dobou svojí platnosti (uvedenou v sekundách):

```
hostapd_cli -p /var/run/hostapd-phy0 wps_ap_pin random [timeout]
```

Zjištění aktuálního PINu je možné pomocí:

```
hostapd_cli -p /var/run/hostapd-phy0 wps_ap_pin get
```

K nastavení vlastního PINu poslouží:

```
hostapd_cli -p /var/run/hostapd-phy0 wps_ap_pin set <PIN> [timeout]
```

Používání statického PINu není doporučováno, ale může být zadán parametrem ap_pin v hostapd.conf [9].

11 MOŽNOSTI OPRAVY BEZPEČNOSTNÍ CHYBY TECHNOLOGIE WPS

Odhalená bezpečnostní chyba byla nalezena v metodě přihlašování metodou PIN – externí registrátor. U ostatních metod žádná slabina publikována nebyla.

Při návrhu je třeba vycházet z možností jednotlivých metod přihlašování pomocí WPS:

- **PBC metoda** – má-li uživatel možnost fyzického přístupu k AP, je pro něj nejsnadnější tuto metodu použít. Nemusí znát a pamatovat si žádné údaje. Nemusí se nikam přihlašovat, ani nic vyplňovat. Stačí jen zmáčknout dvě tlačítka (v počítači většinou softwarové). Největší problém této metody je nutnost umístění směrovače v snadném dosahu uživatele.
- **Metoda PIN – interní registrátor** – může být použita uživatelem, pokud má přístup do konfigurace AP, kam zadá PIN vygenerovaný v počítači. Uživatel již musí mít znalost přihlašovacích údajů do AP a musí do něj přepsat správně PIN.
- **Metoda PIN – externí registrátor** – předpokládá znalost statického PINu. Uživatel nemusí mít AP ve svém fyzickém dosahu a může být bez možnosti vstoupit do jeho konfiguračního rozhraní.

Mají-li být tyto metody využívány takovým způsobem pro něž jsou vhodné, odpadá při úvahách o opravě metody přihlašování pomocí AP PINu možnost fyzického kontaktu s AP a možnost přihlásit se do konfiguračního rozhraní. Na základě těchto předpokladů se možnosti značně omezují. Odpadá i možnost automatického vypnutí této metody při detekci útoku, bez následného automatického zapnutí.

Dalším omezujícím faktorem je cílová skupina využívající zařízení s WPS, tedy lidé s minimálními nebo žádnými znalosti v oblasti bezpečnosti a konfigurace takovýchto zařízení. Řešení tedy musí klást minimální nároky na uživatele.

11.1 Návrhy na opravu

11.1.1 Omezený počet neúspěšných pokusů za časový úsek

Řešením může být systém, který bude hlídat počty neúspěšných pokusů o přihlášení pomocí AP PINu. Velmi brzy (např. po 2 neúspěšných pokusech) by tuto metodu přihlašování dočasně vyřadil z provozu (např. na 30 minut). O čemž by uživatel, při dalším pokusu o přihlášení, mohl být informován v odezvě na neúspěšný pokus. Při takto navržených hodnotách by vyzkoušení všech možností trvalo cca 115 dní. V malých firemních a domácích sítích nelze předpokládat velké počty přihlašujících

se uživatelů touto metodou. Opsat 8 číslic a před potvrzením si je zkontrolovat by neměl být takový problém. Na nutnost pečlivosti by v tomto případě měl být uživatel, v místě kde PIN zadává, taktéž informován.

11.1.2 Proměnlivý PIN

Další a zajímavější možností je nenechat PIN statický, protože to je jeden z hlavních předpokladů pro snadnou možnost útoku. Když by se PIN nepředvídatelně měnil, velmi by se tím zvýšila bezpečnost této metody. Vyvstává zde ale otázka, jak by se takový měnící PIN dozvěděl uživatel, který nemá ani fyzický přístup k AP, ani přístup do jeho konfiguračního rozhraní.

Možností by bylo využití matematické rovnice, která by zcela stejně běžela na směrovači i počítači. Vstupní podmínkou by bylo zadání statického PINu (uvedeného na AP) a nějaký proměnlivý element. Rovnice by nemusela být nijak složitá, protože statický PIN by zůstal neodhalen a šlo by především a nepredikovatelnou proměnlivost aktuálně správného PINu.

Proměnlivým elementem by mohl být čas a datum. Ke změně PINu by mohlo docházet např. každých 5 minut, vždy v dané časové okamžiky. K synchronizaci času na směrovači a počítači by mohly být využívány NTP (Network Time Protocol) servery (popř. s možností zadání času manuálně pro uživatele na počítači).

Uživatel by tedy do programu, který by používal pro přihlašování, napsal statický PIN. Tento program by na základě zadání statického PINu vypočítal aktuální proměnlivý PIN a jeho hodnotu odeslal do AP za účelem přihlášení. AP zná svůj statický PIN a jelikož by na něm byla totožná rovnice jako v počítači, měl by i stejný proměnlivý PIN.

Rovnice by musela mít takovou podobu, aby se výsledné PINy předvídatelně neopakovaly (např. za určitá časová období) a aby využívala celého rozsahu sedmi číslic (osmá je kontrolní součet).

Vhodnými kandidáty na využití v rovnici by bylo sčítání, násobení, umocňování a modulo.

Při implementaci této metody lze využít a popř. upravit některé části ze zdrojových souborů hostapd [9]. Zmíněná funkce je podobná té, kterou hostapd využívá pro generování náhodného PINu [9]:

```
unsigned int wps_generate_pin(void)
{
unsigned int val;

/* Generate seven random digits for the PIN */
```

```
if (random_get_bytes((unsigned char *) &val, sizeof(val)) < 0) {
struct os_time now;
os_get_time(&now);
val = os_random() ^ now.sec ^ now.usec;
}
val %= 10000000;

/* Append checksum digit */
return val * 10 + wps_pin_checksum(val);
}
```

Náhodnost by byla zaměněna za statickou hodnotu AP PINu a popř. rovnice dále pozměněna. Především by musely být určeny doby generování nového PINu a doby jeho platnosti.

Pro výpočet kontrolního součtu by posloužila následující část kódu [9]:

```
unsigned int wps_pin_checksum(unsigned int pin)
{
unsigned int accum = 0;
while (pin) {
accum += 3 * (pin % 10);
pin /= 10;
accum += pin % 10;
pin /= 10;
}

return (10 - accum % 10) % 10;
}
```

Pro kontrolu celého PINu včetně kontrolního součtu kód [9]:

```
unsigned int wps_pin_valid(unsigned int pin)
{
return wps_pin_checksum(pin / 10) == (pin % 10);
}
```

11.1.3 Návrh jiného systému

Možností by také bylo navrhnou zcela jiný systém použitý při přihlašování, než jaký ukazuje obrázek 9.11, jenž byl neposkytoval informace o tom, jestli byla polovina PINu správná. Tím by zachoval velký počet možností kterých PIN může nabývat.

ZÁVĚR

V rámci práce byly nejprve definovány důležité pojmy z oblasti bezpečnosti Wi-Fi sítí. Byla rozepsána možná bezpečnostní rizika pro Wi-Fi sítě a popsány důležité obecné kroky při návrhu bezpečné sítě.

Dále byly vybrány a nastudovány některé mechanismy zabezpečení Wi-Fi sítí a jejich známé bezpečnostní slabiny. Vybrány byly proto, že jejich použití umožňuje většina Wi-Fi zařízení a je vhodné ověřit míru zabezpečení, kterou poskytují. Následně byly na tyto zabezpečovací mechanismy provedeny útoky, které mají ukázat jejich slabiny a omezení, z čehož vyplývá vhodnost jejich použití i úskalí, kterých se lze vyvarovat.

V práci byl popsán princip útoků i fungování vybraných bezpečnostního mechanismů. Z toho následně vyplývá, co je příčinou selhání bezpečnostních mechanismů.

Byly provedeny útoky na přerušení spojení mezi přístupovým bodem a připojenými klienty, na zjištění skrytého SSID s připojenými klienty i bez připojených klientů, na bezpečnostní technologie WEP a WPS.

Při útocích byla využívána distribuce operačního systému GNU/Linux BackTrack. Podstatné údaje z průběhu útoků byly zaznamenány pomocí programu Wireshark a vloženy do práce jako obrázky s vyznačením nejdůležitějších parametrů.

K provádění útoků byly použity programy, které mají dostupné zdrojové kódy, jsou u nich vidět jednotlivé fáze útoku a lze u nich provádět další analýzu jejich fungování.

Největší důraz byl kladen na aktuální bezpečnostní problém, který představuje technologie WPS. U ní byl důkladně rozebrán princip fungování, aby bylo možné pochopit důvod bezpečnostní chyby a princip útoku. U obrázku 9.11 popisujícího nejdůležitější část z principu funkce WPS byla opravena chybná interpretace, která se vyskytuje v oficiální dokumentaci [30], i v dalších dílech z ní čerpajících.

Dále byla na Wi-Fi směrovač TP-LINK TL-WR1043ND nahrána GNU/Linuxová distribuce OpenWrt a následně zprovozněna technologie WPS. To bylo učiněno z důvodu možného provedení implementace bezpečností opravy v tomto otevřeném systému.

K samotné implementaci už z důvodu časové náročnosti předchozích částí bohužel nedošlo. V závěrečné kapitole byly popsány možnosti pro opravu této bezpečnosti alespoň z teoretického hlediska. Pokud by časové hledisko vycházelo příznivěji byla by implementována popsaná metoda proměnlivého PINu. Při této implementaci by bylo nejlépe vyjít ze zdrojových kódů softwaru hostapd [9], jehož využívá distribuce OpenWrt nejen pro technologii WPS.

LITERATURA

[1] About the Project. *OpenWrt Wiki* [online]. 15.3.2012 [cit. 2012-05-16]. Dostupné z: <http://wiki.openwrt.org/about/start>.

[2] About Windows Connect Now. MICROSOFT. *MSDN: Možnosti vývoje softwaru pro klientské počítače, web, cloud a telefony* [online]. 7.2.2012 [cit. 2012-05-20]. Dostupné z: <http://msdn.microsoft.com/en-us/library/windows/desktop/ee844574(v=vs.85)>.

[3] *Aircrack-ng : Main documentation* [online]. c2009-2011 [cit. 2011-10-22]. Dostupné z WWW: <http://www.aircrack-ng.org/documentation.html>.

[4] BACKTRACK LINUX. *BackTrack* [online]. [c 2011] [cit. 2012-04-16]. Dostupné z: <http://www.backtrack-linux.org>.

[5] BARKEN, Lee. *Jak zabezpečit bezdrátovou síť WI-FI.* Vydání první. Brno : Computer Press, 2004. 174 s. ISBN 80-251-0346-3.

[6] BRISBIN, Shelly. *Wi-Fi : postavte si svou vlastní wi-fi síť.* Praha : Neocortex, 2003. 248 s. ISBN 80-86330-13-3.

[7] BURDA, Karel. *Bezpečnost informačních systémů* [online]. Brno : FEKT VUT v Brně, 1.11.2005 [cit. 2011-11-11]. 104 s. Dostupné z WWW: <https://www.vutbr.cz/www_base/priloha.php?dpid=23579>.

[8] HANÁČEK, Petr. Bezpečnostní funkce v počítačových sítích. *Zpravodaj ÚVT MU* [online]. 1999, X, 2, [cit. 2011-11-23]. s. 5–9. Dostupný z WWW: <http://ics.muni.cz/bulletin/articles/171.html>. ISSN 1212-0901.

[9] *Hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator* [online]. 10.5.2012 [cit. 2012-05-22]. Dostupné z: <http://hostap.epitest.fi/hostapd>.

[10] IEEE Std 802.11™-2007 *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* New York : IEEE Computer Society, 12 June 2007. 1184 s. ISBN 0-7381-5656-6. Dostupné z WWW: <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>.

[11] Index of /backfire/10.03.1/ar71xx/. OpenWrt. [online]. 21.12.2011 [cit. 2012-05-17]. Dostupné z: <http://downloads.openwrt.org/backfire/10.03.1/ar71xx/>.

[12] Instalace OpenWRT na TP-LINK TL-WR1043ND. *OpenWrt TP-LINK TL-WR1043ND* [online]. 2011, 19. 8. 2011 [cit. 2012-05-17]. Dostupné z: <http://sites.google.com/site/openwrttplinktlwr1043nd/home/instalace>.

[13] Nastavení a správa sítě pomocí Průvodce technologií Wi-Fi Protected Setup*. *IT manufacturer and solutions provider to the Public Sector / Stone Group* [online]. [2010] [cit. 2012-05-19]. Dostupné z: <http://www.stonecomputers.com/ftp/Rock/Drivers/Drivers/P170hm/Option/02_WLAN/Intel/XP/Docs/CSY/wps.htm>.

[14] Obsługa klawisza wps/qss w openwrt. *RpcWiki* [online]. 4.7.2010 [cit. 2012-05-21]. Dostupné z: <http://rpc.one.pl/index.php/lista-artykulow/34-openwrt/83-obsluga-klawisza-wps-qss-w-openwrt>.

[15] *Open Clipart Library* [online]. [cit. 2011-12-10]. Dostupné z WWW: <http://openclipart.org>.

[16] OpenWrt Buildroot – About. *OpenWrt Wiki* [online]. 30.12.2011 [cit. 2012-05-21]. Dostupné z: <http://wiki.openwrt.org/about/toolchain>.

[17] OpenWrt Buildroot – Installation. *OpenWrt Wiki* [online]. 22.4.2012 [cit. 2012-05-21]. Dostupné z: <http://wiki.openwrt.org/doc/howto/buildroot.exigence>.

[18] *OpenWrt: Wireless Freedom* [online]. [cit. 2012-05-16]. Dostupné z: <https://openwrt.org>.

[19] OpenWrt - Obsługa WPS (Wi-Fi Protected Setup): łatwa i szybka autoryzacja klientów Wi-Fi. *Eko.one.pl: OpenWrt, Linux, USB, notebooki i inne ciekawe rzeczy* [online]. 21.4.2012 [cit. 2012-05-21]. Dostupné z: <http://eko.one.pl/?p=openwrt-wps>.

[20] PARSONS, Keith R. *Wireshark Hands-On Exercises* [online]. 17.6.2010 [cit. 2011-11-03]. Dostupné z: <http://sharkfest.wireshark.org/sharkfest.10/B-5_Parsons%20HANDS-ON%20LAB%20-%20WLAN%20Analysis%20with%20Wireshark%20&%20AirPcap.pdf>.

[21] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace : Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G.* Vydání první. Brno : CP Books, 2005. 179 s. ISBN 80-251-0791-4.

[22] PUŽMANOVÁ, Rita. *Lupa.cz* [online]. 1. 11. 2007 [cit. 2011-11-25]. Bezpečnost WiFi záleží jen na vás. Dostupné z WWW: <http://www.lupa.cz/clanky/bezpecnost-wifi-zalezi-jen-na-vas>.

[23] PUŽMANOVÁ, Rita. *Širokopásmový Internet : Přístupové a domácí sítě.* Vydání první. Brno : Computer Press, 2004. 377 s. ISBN 80-251-0139-8.

[24] SOSINSKY, Barrie. *Mistrovství - počítačové sítě.* Vydání první. Brno : Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.

[25] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí.* Vydání první. Brno : CP Books, 2005. 338 s. ISBN 80-251-0417-6.

[26] TL-WR1043ND. TP-LINK TECHNOLOGIES CO., Ltd. *Vítejte u společnosti TP-LINK* [online]. [c2012] [cit. 2012-04-21]. Dostupné z: <http://cz.tp-link.com/products/details/?model=TL-WR1043ND>.

[27] TP-Link TL-WR1043ND. *OpenWrt Wiki* [online]. 12.5.2012 [cit. 2012-05-14]. Dostupné z: <http://wiki.openwrt.org/toh/tp-link/tl-wr1043nd>.

[28] TP-Link TL-WR1043ND v1.8 a.jpg. *InfoDepot Wiki* [online]. 2011, 07.05.2011 [cit. 2012-05-15]. Dostupné z: <http://infodepot.wikia.com/wiki/File:TP-Link_TL-WR1043ND_v1.8_a.jpg>.

[29] VIEHBÖCK, Stefan. *Brute forcing Wi-Fi Protected Setup: When poor design meets poor implementation.* [online]. 26.12.2011 [cit. 2012-05-18]. Dostupné z: <http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf>.

[30] Windows Connect Now–NET: A WINDOWS® RALLY™ SPECIFICATION. [online]. 2006, s. 75, 08.12.2006 [cit. 2012-05-20]. Dostupné z WWW: <http://download.microsoft.com/download/a/f/7/af7777e5-7dcd-4800-8a0a-b18336565f5b/WCN-Netspec.doc>.

[31] WI-FI ALLIANCE. *Certified Products* [online]. [c2012] [cit. 2012-05-18]. Dostupné z: <http://certifications.wi-fi.org/search_products.php>.

[32] Wi-Fi Protected Setup™. WI-FI ALLIANCE. *Wi-Fi Alliance* [online]. [c2012] [cit. 2012-05-18]. Dostupné z: <http://www.wi-fi.org/knowledge-center/articles/wi-fi-protected-setup%E2%84%A2>.

[33] Wi-Fi trpí nepochopitelnou bezpečnostní chybou. *O počítačích, IT a internetu – Živě.cz* [online]. 4. 1. 2012 [cit. 2012-05-18]. Dostupné z: <http://www.zive.cz/clanky/wi-fi-trpi-nepochopitelnou-bezpecnostni-chybou-video/sc-3-a-161699>.

[34] ZANDL, Patrick. *Bezdrátové sítě Wifi : Praktický průvodce.* Vydání první. Brno : Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ACK	ACKnowledgment – potvrzení
AES	Advanced Encryption Standard
AP	Access Point – přístupový bod
BSSID	Basic Service Set IDentifier
CBC	Cipher-Block Chaining – zřetězení šifrových bloků
CRC	Cyclic Redundancy Check – cyklický redundantní součet
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service – odepření služby
DVD	Digital Versatile Disc – digitální víceúčelový disk
EAP	Extensible Authentication Protocol
FMS	Fluhrer, Mantin, Shamir
GNOME	GNU Network Object Model Environment
GNU	GNU's Not Unix
GPL	General Public License – všeobecná veřejná licence
IEEE	Institute of Electrical and Electronics Engineers – Institut pro elektrotechnické a elektronické inženýrství
ISO/OSI	International Standards Organization / Open System Interconnection – Mezinárodní organizace pro normalizaci / propojení otevřených systémů
IV	Initialization Vector – inicializační vektor
JTAG	Joint Test Action Group
KDE	K Desktop Environment
LAN	Local Area Network
LuCi	Lua Unified Configuration Interface
MAC	Media Access Control
NACK	Negative ACKnowledgment

NTP	Network Time Protocol
opkg	Open PacKaGe management
PBC	Push Button Configuration
PIN	Personal Identification Number – osobní identifikační číslo
PTW	Pychkine, Tews, Weinmann
QSS	Quick Security Setup
RC4	Ron's Code no. 4
SDK	Software Development Kit – softwarová vývojová sada
SSH	Secure SHell
SSID	Service Set IDentifier
UCI	Unified Configuration Interface
USB	Universal Serial Bus – univerzální sériová sběrnice
U-Boot	Universal Bootloader – univerzální zavaděč
WAN	Wide Area Network
WEP	Wired Equivalent Privacy – soukromí ekvivalentní drátovým sítím
Wi-Fi	Wireless Fidelity – bezdrátová věrnost
WPS	Wi-Fi Protected Setup
XOR	eXclusive OR – exkluzivní logický součet (exkluzivní disjunkce)

SEZNAM PŘÍLOH

A OBSAH PŘILOŽENÉHO DATOVÉHO MÉDIA

Na přiloženém datovém médiu se nachází elektronická verze práce ve formátu pdf.

Dále obsahuje distribuci GNU/Linux OpenWrt, balíčky zkompilované v rámci práce, konfigurační soubory a zdrojové soubory softwaru hostapd.