PŘÍRODOVĚDECKÁ FAKULTA UNIVERZITY PALACKÉHO
KATEDRA INFORMATIKY

BAKALÁŘSKÁ PRÁCE

Demonstrace útoků na WIFI sítích

2013 Petr Vopálenský

Anotace

Cílem práce je vytvoření výukové grafické aplikace demonstrující reálně možné a běžně používané útoky na Wi-Fi sítě, společně s vysvětlením teoretické podstaty těchto útoků a možných řešení ochrany.

Děkuji vedoucímu práce Mgr. Janu Outratovi, Ph.D. za cenné rady a všem, kteří mě jakýmkoliv způsobem podporovali.

Obsah

Seznam obrázků

Seznam tabulek

1. Úvod

V této bakalářské práci se zabýváme tvorbou aplikace, která jednoduchým a názorným způsobem demonstruje většinu běžných útoků na Wi-Fi sítě. Dále aplikace vysvětluje teoretickou podstatu těchto útoků a ukazuje možnosti ochrany proti nim. Aplikace je navržena tak, aby běžnému uživateli umožňovala provést aktivní otestování bezpečnosti sítě s vysvětlením jednotlivých úkonů, případně uživateli doporučila vhodné zabezpečovací postupy.

Bezdrátové sítě se staly naprosto běžnou součástí našich životů. Jedny z nejčastěji využívaných, vedle telefonních, jsou počítačové sítě založené na standardu IEEE 802.11 neboli Wi-Fi[1] sítě. Jejich obliba roste hlavně díky jednoduchosti použití, rychlosti, možnosti mobility a samozřejmě i ceně. Proto je dnes najdeme prakticky v každé domácnosti, kancelářích, restauracích a jiných veřejných místech. Avšak s rozšířením Wi-Fi sítí vyvstává otázka jejich zabezpečení. V praxi je vidět, že běžní uživatelé mají naprosto tristní znalosti o možnostech zabezpečení sítě a většinou ponechávají bezpečnostní prvky ve výchozí, často nedostatečné konfiguraci. Tato bakalářská práce se věnuje tvorbě aplikace, která jednoduchým a jasným způsobem demonstruje jedny z nejběžnějších útoků na Wi-Fi sítě, vysvětluje jejich teoretickou podstatu a možnosti ochrany.

V první části práce popíšeme standard IEEE 802.11 a jeho dodatky obecně. Seznámíme se s dnes nejpoužívanějšími standardy v pásmu 2,4 GHz a 5 GHz. Postupně probereme metody zabezpečení Wi-Fi sítí, od jednodušších, jako je skrytí SSID, filtrace MAC adres, až po zabezpečení WEP, WPA a WPA2. Nastíníme si jejich slabiny a způsoby řešení ochrany. V závěru této části si zopakujeme obecně platná bezpečnostní doporučení pro vhodnou volbu hesla, také zmíníme dodatečné způsoby ochrany síťových dat jako například VPN, tunelování a firewally.

Těžiště bakalářské práce spočívá ve vytvoření a popisu výukové aplikace, která nám formou různých tutoriálů ukazuje a objasňuje rozmanité útoky na Wi-Fi sítě. V aplikaci také nabízíme nejčastější řešení vedoucí ke spolehlivé ochraně dané sítě. Útoky provádíme v operačním systému GNU/Linux, převážně využíváme nástroje balíku Aircrack-ng. Dále se věnujeme návrhu architektury aplikace a popisu použitých technologií, včetně programátorské a uživatelské příručky.

Tato práce se téměř nezabývá IEEE standardy, místo toho pojednává o grafické aplikaci, která nám srozumitelnou formou představí základní metody zabezpečení, jejich slabiny a případné řešení ochrany. Aplikace také podporuje aktivní otestovaní bezpečnosti sítě praktickou ukázkou útoku.

Zdůrazněme, že tato práce je zaměřena na vytvoření uživatelsky snadno uchopitelné aplikace, nikoliv na podrobný teoretický rozbor všech známých technologií a algoritmů.

[1] http://www.ieee802.org/11/

2. Standardy IEEE 802.11

Pracovní skupina IEEE (Institute of Electrical and Electronics Engineers) vyvinula (a stále vyvíjí) standard pro bezdrátovou komunikaci v počítačových sítích s názvem IEEE 802.11. Po čase se ukázaly nedostatky tohoto standardu a tak byl rozšířen o takzvané sady dodatků, viz Tabulka 1. Nejznámější dodatky řeší zvýšení maximální rychlosti přenosu dat (802.11b, 802.11g) a vylepšení zabezpečení (IEEE 802.11i).

Standardy IEEE 802.11 pracují v licenčně volném pásmu 2,4 GHz nebo v pásmu 5 GHz. Nevýhodou volného pásma 2,4 GHz je, že dochází k interferenci s dalšími zařízeními používajícími stejné pásmo (mikrovlnné trouby, Bluetooth, ...).

IEEE 802.11 pracuje na fyzické[2] vrstvě, kde řeší způsob přenosu dat, a na linkové vrstvě, kde zajišťuje autentizaci, asociaci a šifrování.

2.1. IEEE 802.11

Původní standard, vyvinut v roce 1997. Pracoval v pásmu 2,4 GHz a umožňoval přenosové rychlosti 1 Mbit/s a 2 Mbit/s.

2.2. IEEE 802.11a

Z důvodu velkého rušení v pásmu 2,4 GHz byl v roce 1999 vyvinut standard IEEE 802.11a, který pracuje v pásmu 5 GHz. Obrovskou výhodou byla maximální rychlost až 54 Mbit/s. Nevýhodou je však nekompatibilita se standardy IEEE 802.11 a 802.11b, jelikož se zde pracuje s jinou frekvencí.

2.3. IEEE 802.11b

Standard vznikl v roce 1999 jako vylepšená verze původního standardu 802.11. Opět pracuje na frekvenci 2,4 GHz, ale zvládá přenosové rychlosti až do 11 Mbit/s.

2.4. IEEE 802.11g

V roce 2003 byl vydán standard IEEE 802.11g, který dokáže v pásmu 2.4 GHz pracovat s rychlostí až 54 Mbit/s. Je zpětně kompatibilní s IEEE 802.11b.

2.5. IEEE 802.11n

IEEE 802.11n je standard, který si klade za cíl dosáhnout teoretických rychlostí až 600 Mbit/s. Využívá technologií předchozích standardů a navíc přidává

[2]http://phoenix.inf.upol.cz/ outrata/courses/ps/texts/lecture2.pdf

používání technologie MIMO [2]. Reálná rychlost se však pohybuje pod 200 Mbit/s.

2.6. IEEE 802.11ac

Do budoucna (pravděpodobně v roce 2014) se plánuje nový standard IEEE 802.11ac, který by měl zvládat přenosové rychlosti přesahující 1 Gbit/s.

Standard	**Rok vydání**	**Frekvence (GHz)**	**Max. rychlost (Mbit/s)**
IEEE 802.11	1997	2,4	2
IEEE 802.11a	1999	5	54
IEEE 802.11b	1999	2,4	11
IEEE 802.11g	2003	2,4	54
IEEE 802.11n	2009	2,4/5	600
IEEE 802.11ac	2014	2,4/5	1800

Tabulka 1. Nejdůležitější standardy IEEE 802.11

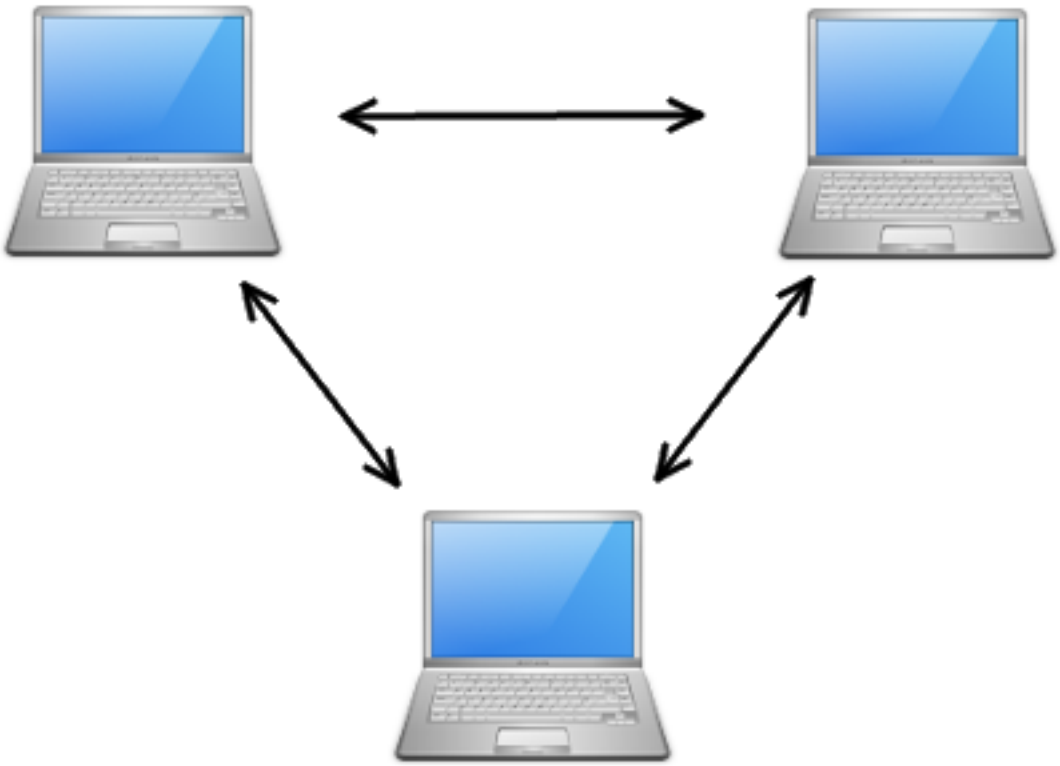
3. Topologie Wi-Fi sítí

Jak už bylo napsáno, Wi-Fi je označení pro několik standardů IEEE 802.11 popisujících bezdrátovou komunikaci v počítačových sítích.

V praxi se používají dvě základní topologie Wi-Fi a to Ad-hoc a režim infrastruktury.

3.1. Ad-hoc zapojení

V této topologii jsou si stanice prakticky rovnocenné, síť nemá centralizované řízení. Topologie je vhodná pro malý počet stanic. Každé dvě komunikující stanice musí být ve vzájemném rádiovém dosahu. Při spojení více stanic navzájem může docházet k rušení signálu.

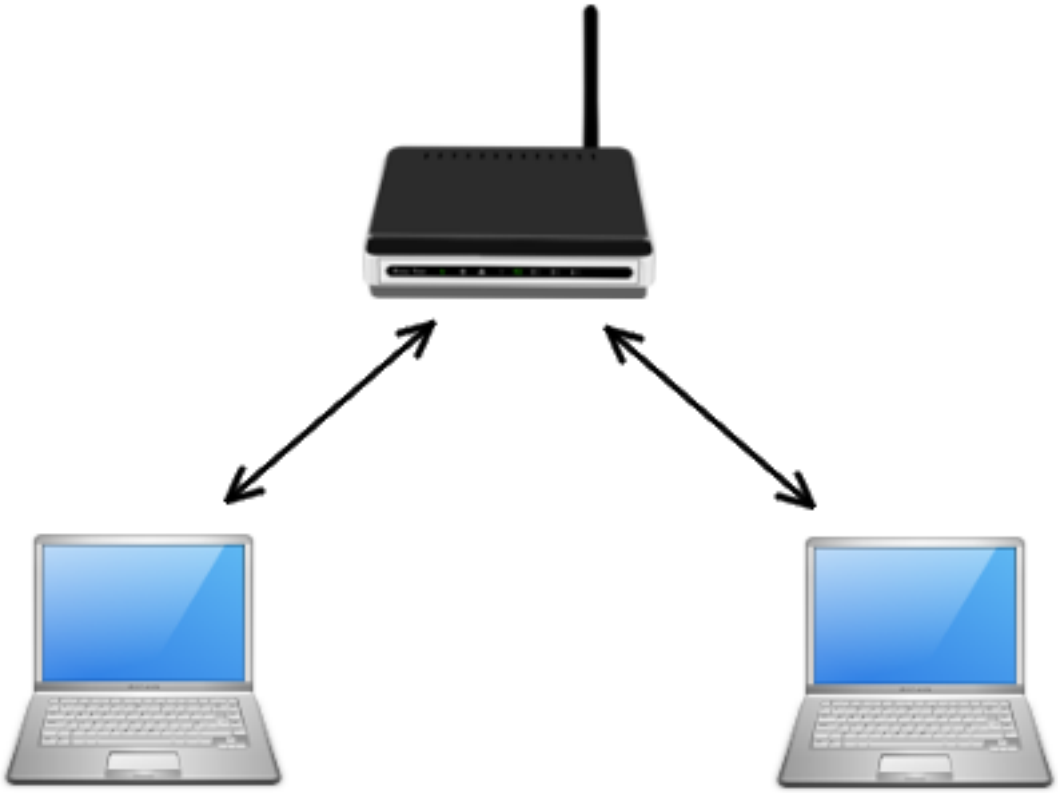


Obrázek 1. Ad-hoc zapojení

3.2. Režim infrastruktury

Zde existuje minimálně jeden přístupový bod, který slouží jako spojovací prvek. Stanice spolu komunikují výhradně s tímto přístupovým bodem. Přístupový bod dokáže komunikovat s více stanicemi současně. Stanice při komunikaci nemusí

být ve vzájemném rádiovém dosahu, jelikož jejich veškerá komunikace probíhá přes přístupový bod. Takže, oproti ad-hoc řešení, každá stanice udržuje pouze jedno spojení, a to na přístupový bod.



Obrázek 2. Režim infrastruktury

4. Zabezpečení WIFI

Rádiový signál je na bezdrátových sítích vysílán do éteru a může být zachycen téměř kýmkoliv, kdo je v dosahu vysílání. Je samozřejmě nežádoucí, aby kdokoliv mohl číst jakákoliv data v síti, a proto bylo zavedeno několik způsobů zabezpečení. Většina z nich se však ukázala jako nedostačující a pro útočníka představují lehce obejitelnou překážku.

4.1. Skrytí SSID

Často používaným zabezpečením je ukrytí identifikátoru sítě SSID (Service Set Identifier, identifikátor sady služeb). Stanice se může připojit do bezdrátové sítě pouze v případě, že zná její SSID (její název). V normálním nastavení vysílá přístupový bod SSID v Beacon rámcích [1]. Jednoduchou konfigurací lze dosáhnout toho, že SSID v Beacon rámcích nevysílá, respektive vysílá jako prázdný řetězec. Bez znalosti SSID se tedy stanice nemůže k síti asociovat.

Získání SSID není žádný problém, protože stanice při asociování do sítě vysílají takzvaný Association request [1] rámec, kde je SSID přenášený bez jakéhokoliv zabezpečení. Stačí nám tedy počkat, až se do sítě přihlásí některá ze stanic a odposloucháváním komunikace zjistíme i SSID. Ve skutečnosti se ani tato zdlouhavá pasivní metoda nepoužívá. Místo toho donutíme stanici k odpojení zasláním DEAUTH rámce. Stanice se posléze pokusí znova asociovat a my odchytíme Association request, a tím okamžitě zjistíme SSID.

Ochrana neexistuje. SSID nikdy nebyl určený jako bezpečnostní prvek a nikdy neměl být skrývaný. Skrývaní SSID je tedy vhodné pouze pro zabránění asociování nenakonfigurovaných stanic, případně takových, které jsou nastavené na automatické připojení do libovolné dostupné sítě.

4.2. Filtrace MAC adres

Jednou z ochran, která se občas využívá, je filtrace podle MAC (Media Access Control) adres zařízení, která se mohou připojit k danému přístupovému bodu (AP). Ochrana vychází z předpokladu, že žádná dvě zařízení nemohou mít shodnou MAC adresu. AP má nastaven seznam zařízení, která se mohou připojit a požadavky ostatních se ignorují. I když je MAC adresa zapsána přímo na síťové kartě zařízení, většinou ji lze jednoduše softwarově změnit. Změna je jen dočasná a po rebootu počítače se vrací na původní hodnotu.

Zdrojová a cílová MAC adresa se v bezdrátové síti vysílá nešifrovaně, a to i v případě, že je použito zabezpečení WEP, WPA nebo WPA2. Prostým odposloucháváním provozu na síti zjistíme připojené stanice.

Ochrana neexistuje. Pouhým pasivním monitorováním síťového provozu lze velmi lehce zjistit MAC adresy asociovaných stanic. Ochrana filtrováním MAC

adres však může dobře posloužit proti neúmyslnému připojení náhodných stanic v dosahu přístupového bodu.

4.3. WEP

Je volitelný doplněk zabezpečení bezdrátových sítí podle původního standardu IEEE 802.11 z roku 1999. WEP znamená Wired Equivalent Privacy, soukromí ekvivalentní drátovým sítím. Původní myšlenka byla vytvoření zabezpečení srovnatelného s klasickou drátovou sítí Ethernet, i přesto, že rádiový signál je vysílán do okolí a prakticky každý může vysílaná data odposlouchávat.

WEP pracuje na linkové vrstvě, kde šifruje přenášená data pomocí proudové šifry RC4 a k integritě dat využívá kontrolní součty CRC-32 [7].

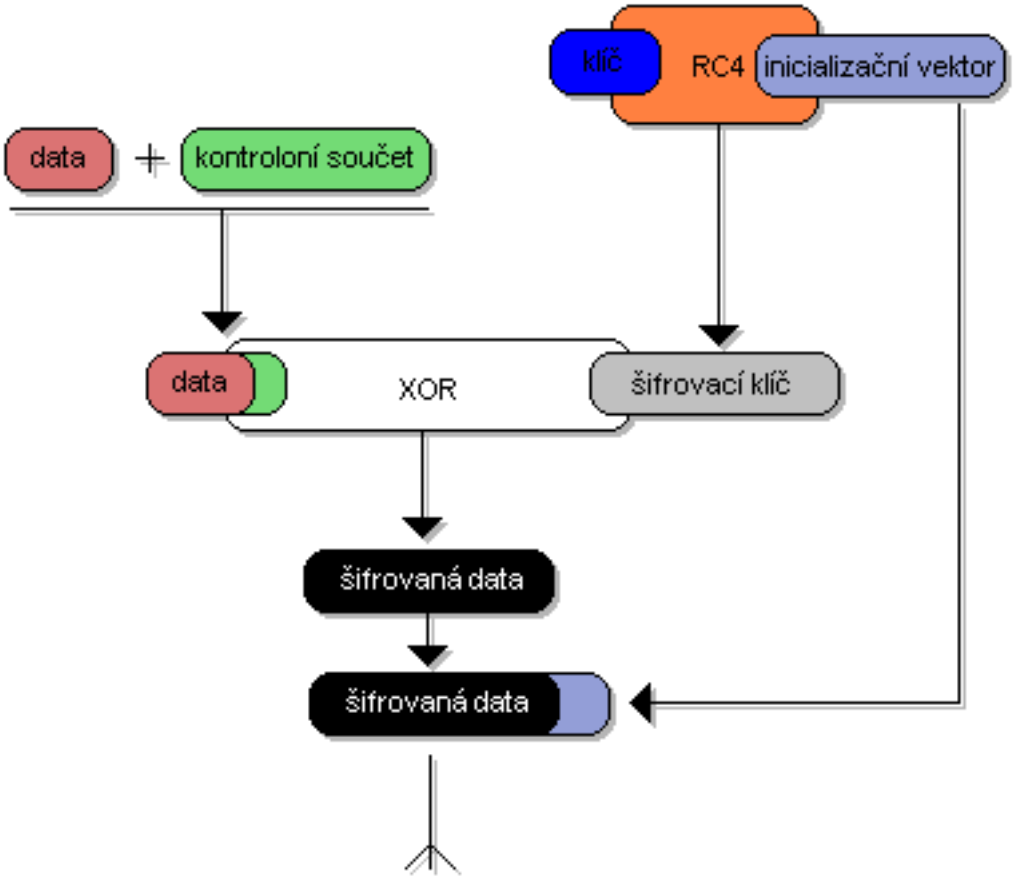
Šifrování se provádí buď 64bitovým nebo 128bitovým klíčem. Ten se skládá z tajného klíče a inicializačního vektoru (IV), který má v obou variantách 24 bitů. Protože se inicializační vektor přenáší nešifrovaně, zbývá na šifrovanou část 40 bitů v případě 64bitového, či 104 bitů v případě 128bitového klíče. Od toho také se také odvíjí označení WEP-40 a WEP-104, v komerční sféře občas značeno WEP-64 a WEP-128. Algoritmy šifrování a dešifrování jsou pro WEP-40 a WEP-104 shodné.

4.3.1. Šifrování WEP

- Z nešifrovaného textu se spočítá kontrolní součet CRC (32 bitů) nazývaný ICV (Integrity Check Value).
- CRC (Cyclic Redundant Checksum) se připojí na konec zprávy.
- Nyní se spojí inicializační vektor (IV) s tajným klíčem, který byl zadán při připojení.
- Na IV spojený s tajným klíčem je puštěn generátor pseudonáhodných čísel RC4 (PRNG).
- Vznikne šifrovaný klíč.
- Funkce XOR se aplikuje na šifrovaný klíč a nešifrovaný text spojený s CRC.
- Vzniká šifrovaný text, ke kterému se na začátek připojí IV.

4.3.2. Dešifrování WEP

- Nešifrované IV ze začátku zprávy se připojí k tajnému klíči.
- Výsledek se předá RC4 generátoru, aby vytvořil sekvenci šifrovacího klíče.



Obrázek 3. Šifrování WEP, zdroj: airodump.cz

- Nyní se provede XOR mezi šifrovacím klíčem a šifrovanou zprávou.
- Vznikne dešifrovaná zpráva. Z té se spočítá CRC a porovná se s odesílanou hodnotou.
- Pokud všechny součty souhlasí, paket se přijme. Jinak se zahodí.

4.3.3. Autentizace

Autentizace je proces ověření identity stanice. Jedná se ověření jednocestné, ověřuje se pouze stanice, ale nikoliv AP. Stanice musí o autentizaci do sítě sama požádat.

Existují dvě metody autentizace:

- **Open system autentizace** – Stanice vlastně neprovádí žádnou autentizaci a nezáleží na jejím WEP klíči. Stanici stačí znát pouze SSID sítě a může se pokusit o asociaci. WEP klíč se používá až při následném šifrování dat.

- **Shared-key autentizace** – Shared Key autentizace, neboli autentizace sdíleným klíčem, používá WEP klíč pro autentizaci i pro šifrování dat. Klíč je společný pro všechny stanice v síti. Stanice nejprve požádá přístupový bod (AP) o autentizaci, AP odpoví výzvou (což je náhodné číslo). Stanice výzvu zašifruje pomocí WEP a pošle zpět AP. Pokud AP dešifruje výzvu, tak autentizuje stanici, viz Obrázek 4.

Obrázek 4. Shared-key autentizace

4.3.4. Slabiny WEP

V návrhu došlo k chybám a WEP obsahuje několik bezpečnostních slabin:

- Inicializačních vektorů je pouze 2^{24} kombinací. Při běžném provozu se počet kombinací snadno vyčerpá a inicializační vektory se začnou opakovat.
- Některé IV jsou slabé a lze z nich lehce odvodit klíč.
- Nikde není definováno, jak se má inicializační vektor generovat. Útočník může stále dokola opakovat jeden a ten samý IV.

- Pouze jednocestná autentizace – uživatel neví, zda se opravdu připojuje ke správnému přístupovému bodu.
- Statický klíč, nedochází k dynamické obměně klíče.
- Na všech stanicích se používá stejný šifrovací klíč.
- ICV je náchylný na útoky, kdy se změní bity v datech, ale nezmění se ICV.

4.3.5. Ochrana

WEP byl prolomen několika způsoby a nedoporučuje se vůbec používat. Pokud je to možné, měl by být WEP nahrazen WPA2-PSK pro domácí použití a WPA2-802.11X/EAP pro firemní použití.

4.4. 802.1X

802.1X je protokol, který poskytuje bezpečnou autentizaci do sítě. Pokud je připojeno nové zařízení, port na přepínači je zablokován dokud se zařízení úspěšně neuatentizuje. Ve Wi-Fi sítích pracuje na principu logických portů přístupového bodu. Přístupový bod zprostředkovává spojení mezi stanicí a autentizačním serverem (většinou Kerberos, nebo RADIUS). Samotná autentizace se realizuje pomocí protokolu EAP (Extensible Authentication Protocol) – protokol zprostředkování výměny autentizačních zpáv mezi klientskou stanicí, přístupovým bodem a autentizačním serverem.

4.5. WPA

WPA (Wi-Fi Protected Access) vznikl v roce 2002 jako dočasná, co nejrychlejší odpověď na prolomení zabezpečení WEP z roku 2001. Je to část tehdy připravovaného standardu IEEE 802.11i, konkrétně vychází z 3. pracovního návrhu. Je hardwarově kompatibilní s WEP, pouze se musí aktualizovat firmware či software použitého zařízení.

Kvůli zpětné kompatibilitě se data šifrují obdobně jako u WEP proudovou šifrou RC4, ale jsou zde rozšiřující bezpečnostní opatření. Na rozdíl od WEP je použit 128bitový klíč a 48bitový inicializační vektor. Data se již nešifrují statickým klíčem, ale používá se protokol TKIP (Temporal Key Integrity Protocol), který pracuje s dočasnými klíči. Odstraňuje problém s inicializačními vektory a zavádí dynamickou správu šifrovacích klíčů.

WPA také odstraňuje slabý 32bitový kontrolní součet CRC a nahrazuje ho kontrolou integrity MIC (Message Integrity Check), která je součástí standardu IEEE 802.11i. Vstupem pro MIC jsou MAC adresa odesílatele, MAC adresa cíle, MIC klíč a nešifrovaná data.

4.5.1. Režimy autentizace

WPA nabízí dva režimy autentizace:

- **WPA-Personal, WPA-PSK** – vhodné pro domácnosti a menší podnikové sítě – PSK znamená předsdílený klíč (Pre Shared Key). Všichni uživatelé v síti znají tento společný klíč, který musí mít velikost 8 až 63 znaků. Autentizace se provádí na základě zadaného sdíleného klíče. Pokud je shodný s hodnotou uloženou na přístupovém bodě, je stanici povoleno připojení do sítě. Sdílený klíč se používá pouze k připojení do sítě a pro TKIP jako výchozí hodnota k vygenerování šifrovacích klíčů.
- **WPA-Enterprise** – vhodné pro větší a velké podnikové sítě. Autentizace se provádí oproti autentizačnímu serveru přes protokol IEEE 802.1x/EAP.

4.5.2. Útok na WPA-PSK

Jediný známý a v praxi proveditelný útok je útok na WPA-PSK. A to pouze hrubou silou či slovníkovým útokem. Útočník musí odchytit inicializační čtyřcestný handshake. To lze realizovat prostým monitorováním provozu a čekáním, až se některá ze stanic připojí. Také lze aktivně odpojit stanici a monitorovat její následné připojení. Útočníkovi stačí pouze tento čtyřcestný handshake, nic dalšího není třeba. Nemusí nadále monitorovat provoz a druhou fázi útoku, což je slovníkový útok (případně útok hrubou silou), může provést kdekoliv, mimo oblast pokrytí napadené sítě.

Ochrana tkví v použití dostatečně silného hesla (12 znaků a více), které nelze jednoduše zlomit hrubou silou a použitím hesla, které se nevyskytuje v žádném slovníku.

4.5.3. Útok na TKIP

TKIP trpí zranitelností, kdy je možné zasílat námi vygenerovaná data k připojené stanici. Tento útok je však nad rámec tohoto materiálu a proto je zde zmíněn pouze zběžně. Tímto útokem nelze získat PSK ani konektivitu do sítě. Doporučeno je WPA-TKIP nezapínat a raději použít WPA2 s CCMP/AES.

4.6. WPA2, IEEE 802.11i

IEEE 802.11i je dodatek k IEEE 802.11 pojmenovaný WPA2. Finálně řeší bezpečnostní slabiny zabezpečení WEP.

Mechanismus pro šifrování dat, nahrazující TKIP, se nazývá CCMP[3] a je založený na blokové šifře AES[4]. Klíč i datový blok mají shodnou velikost 128

[3]Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
[4]Advanced Encryption Standard

bitů. Klíče jsou generovány dynamicky. Při vývoji CCMP byl kladen maximální důraz na bezpečnost, avšak za cenu ztráty kompatibility s WEP. CCMP je pro WPA2 povinný a je dnes považován za zcela bezpečný a neprolomitelný.

Kontrolu integrity zajišťuje opět MIC, ale oproti WPA v částečně modifikované verzi.

	Šifrování	**Autentizace**	**Využití**
WPA-Personal	TKIP	PSK	Pro domácnost
WPA-Enterprise	TKIP	802.1X	Nepoužívat
WPA2-Personal	CCMP	PSK	Pro domácnost
WPA2-Enterprise	CCMP	802.1X	Pro firmy

Tabulka 2. Režimy WPA a WPA2

Stejně jako v případě WPA i WPA2 nabízí dva režimy autentizace – WPA2-Personal a WPA2-Enterprise. Oba režimy jsou naprosto shodné s WPA.

Ačkoliv se WPA2 považuje ze zcela bezpečný, lze na režim WPA2-PSK (stejně jako v případě WPA-PSK) aplikovat útok odchycením čtyřcestného handshaku. Útok na WPA2-PSK je identický s útokem na WPA-PSK.

4.7. Doplňkové ochrany

4.7.1. Síla signálu

Jedna z málo používaných ochran proti útočníkovi. Omezení dosahu vysílaného signálu je přitom ochranou velice účinnou. Například v panelovém domě nepotřebujeme vysílat signál do sousedních obytných buněk, kde se může skrývat potenciální útočník, ale stačí nám pokrýt pouze prostor našeho bytu.

Pokud jsou naše stanice v jednom směru od přístupového bodu, můžeme nahradit všesměrovou anténou za anténu směrovou.

4.7.2. VOIP síť

Někteří provideři internetového připojení (typicky O2) nabízí přístupové body, které mají v základním nastavení zapnuté vysílání dvou sítí. Jedna je většinou správně nastavená na WPA2-PSK, ale druhá je zabezpečena pouze slabým zabezpečením WEP, většinou vysílá pod SSID „VOIP“. Tato síť představuje bezpečnostní díru do systému a pokud ji nepotřebujete, je doporučeno ji vypnout a nebo změnit WEP na WPA2.

4.7.3. VPN, SSL, TLS

VPN (virtuální privátní síť) je jedno z nejlepších možných řešení zabezpečení. Mezi stanicí a VPN bránou se vytvoří šifrované spojení. I kdyby se útočníkovi podařilo prolomit zabezpečení Wi-Fi, tak se k šifrovaným datům stanice stejně nedostane. Ideální je použití VPN v kombinaci s firewallem takovým způsobem, že kdokoliv se přihlásí do Wi-Fi sítě, může komunikovat jen s VPN bránou, ostatní pakety firewall automaticky zahodí. Tímto způsobem můžeme teoreticky provozovat Wi-Fi síť bez dodatečného zabezpečení (WPA2, WPA, WEP) s jistotou, že potenciální útočník se nedostane k našim datům, ani že nebude schopen využít naši síťovou konektivitu.

Obecně bychom se měli snažit používat protokoly, které garantují bezpečnost komunikace. Typickým příkladem jsou aplikační protokoly nad TLS či SSL – HTTPS, SFTP, IMAPS, ...

5. Popis aplikace

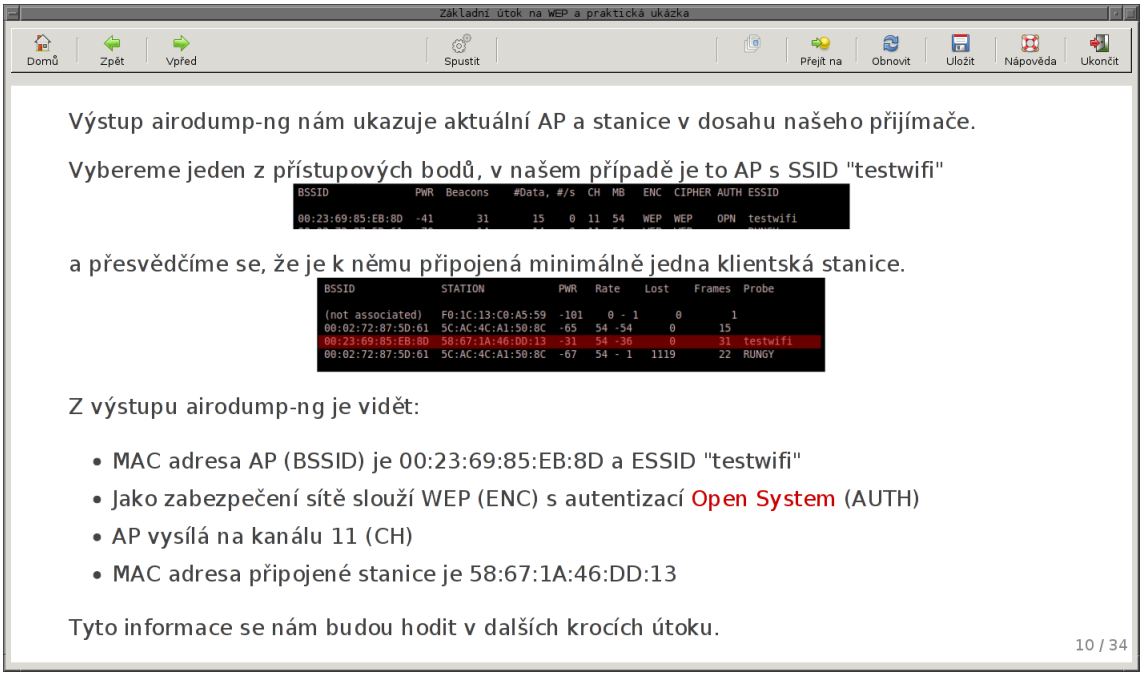
Tato grafická aplikace si klade za cíl vysvětlit a popsat vybrané útoky na Wi-Fi sítě, se zaměřením na nejčastěji skutečně aplikované postupy.

Útoky jsou popsány srozumitelnou formou krok za krokem, aby i méně zkušený uživatel pochopil podstatu většiny útočníkových kroků a dokázal na ně adekvátně zareagovat, případně měl sám možnost si prověřit zabezpečení své bezdrátové sítě.

Aplikace není a ani se nesnaží být všeobsahujícím manuálem s popisem všech reálných a teoretických útoků. Pouze demonstruje ty nejčastěji využívané, se kterými se v praxi běžně setkáváme.

V každé kapitole je nejprve problém vysvětlen teoreticky. Poté následuje praktická ukázka za pomoci běžně dostupných nástrojů, kde si uživatel prostým zopakováním příkazů může útok vyzkoušet v praxi na své vlastní síti. V samém závěru je navrhnuto řešení zabezpečení, pokud takové řešení existuje. Některé z kapitol mají možnost spustit implementaci útoků předem připravenými skripty, které automaticky vyberou nejvhodnější nástroj a provedou daný útok. U všech takto automatizovaných útoků je uživatel prvně dotázán, zda se má útok opravdu provést. Vše je ilustrováno obrázky a snímky obrazovky ze skutečných útoků.

Aplikace je multiplatformní, to znamená, že lze pustit takřka na libovolném systému, který obsahuje komponenty popsané v kapitole 6. Jednotlivé návody jsou však koncipovány primárně se zaměřením na operační systém GNU/Linux a i praktické útoky jsou podporovány a ozkoušeny pouze pod tímto operačním systémem.



Obrázek 5. Ukázka prezentace v aplikaci

6. Použité technologie a architektura aplikace

Aplikace je napsána v interpretovaném programovacím jazyce Perl (Practical Extraction and Reporting Language).

Jako frontend pro grafické uživatelské rozhraní byla použita knihovna GTK+.

Pro samotné prezentování útoků bylo využito značkovacího jazyka HTML, v kombinaci s objektově orientovaným jazykem JavaScript a jazykem pro popis zobrazení CSS.

Vykreslování HTML zajišťuje knihovna WebKit.

6.1. WebKit

Celá prezenční část aplikace je napsána formou webových stránek. Proto vznikla potřeba tento HTML kód nějakým způsobem interpretovat a zobrazovat. Na výběr bylo několik řešení. Nakonec zvítězilo multiplatformní renderovací jádro WebKit[5], jelikož je součástí většiny linuxových distribucí, alespoň těch, které obsahují grafické rozhraní Gnome, které z části na této knihovně závisí.

Všechny stránky prezentace jsou uloženy v kořenovém adresáři aplikace, ve složce `html` a je možné si je prohlížet v libovolném moderním webovém prohlížeči nezávisle na naší aplikaci.

6.1.1. HTML

Aplikace popisuje útoky formou tutoriálů a jazyk HTML je takřka ideální k této formě prezentace. HTML (HyperText Markup Language) je značkovací jazyk, který se dnes zdaleka nevyužívá jen k tvorbě webových stránek.

6.1.2. CSS

CSS (Cascading Style Sheets, kaskádové styly) slouží k popisu zobrazení stránek napsaných v jazyce HTML. Vzhledem k tomu, že značná část aplikace byla napsána v jazyce HTML, bylo jen logické, že k popisu vzhledu bylo použito právě kaskádových stylů.

Pro potřeby naší aplikace byl vytvořen soubor bak.css, který vychází z deck.core.css, a soubor bakstyle.css, který vychází z themes/style/swiss.css. Tyto soubory popisují výsledný vzhled prezentací. Díky jednotnému umístění stylů není problémem změnou jednoho atributu dosáhnout změny vzhledu ve všech našich webových stránkách.

[5] http://www.webkit.org/

6.1.3. JavaScript

JavaScript je objektově orientovaný skriptovací jazyk běžící na straně klienta v prohlížeči. JavaScript obstarává animace, reakce na stisk určitých kláves, skoky mezi stránkami, „expose“ režim, atd.

6.2. GTK2

Pro běh programu v grafickém uživatelském rozhraní je použita multiplatformní knihovna GTK+[6] ve verzi 2.

Toolkit GTK+ se stará pouze o vykreslení hlavního okna, ve kterém je v horní části umístěna lišta s ovládacími tlačítky. Zbytek hlavního okna vyplňuje výsledek vyrenderovaný knihovnou WebKit.

6.3. Perl

Aplikace je napsána v interpretovaném programovacím jazyce Perl[7]. Perl byl vybrán z důvodu jeho přenositelnosti na takřka libovolnou platformu bez nutnosti úpravy kódu a jednoduchosti programování.

Knihovna gtk2 je sice napsána v programovacím jazyce C, ale má vazby na početnou skupinu dalších jazyků. Jedním z nich je i Perl, projekt realizující spolupráci nese název gtk2-perl[8].

Pro manipulaci s knihovnou WebKit bylo vybráno rozšíření perlu perl-gtk2-webkit[9], které nám dovolí vložit vyrenderovaný obsah z knihovny WebKit do okna vykresleného přes toolkit GTK+.

6.4. Pomocné skripty

Aby se nemusely řešit některé rutinní činnosti stále dokola, byly vytvořeny následující pomocné skripty v jazyce Perl s Shellu.

- **generuj.pl** – vygeneruje z předpřipravené šablony konkrétní html prezentaci
- **vse_generuj.sh** – přegeneruje všechny html soubory, všechny prezentace

6.5. Použité systémy a nástroje

[6] http://www.gtk.org/
[7] http://www.perl.org/
[8] http://gtk2-perl.sourceforge.net/
[9] http://search.cpan.org/dist/Gtk2-WebKit/lib/Gtk2/WebKit.pm

6.5.1. BackTrack Linux

Všechny útoky byly demonstrovány v operačním systému GNU/Linux, konkrétně BackTrack Linux[10] ve verzi 5 R3.

6.5.2. Aircrack-ng

Aircrack-ng[11] je kompletní sada nástrojů na prověření bezpečnosti bezdrátových sítí. Obsahuje zejména tyto utility:

- **airmon-ng** – zapínání a vypínání monitorovacího režimu bezdrátové karty
- **airodump-ng** – monitorování a ukládání provozu na síti, vhodné zejména k ukládaní inicializačních vektorů u WEP a čtyřcestného handshaku u WPA/WPA2-PSK
- **aireplay-ng** – dovoluje provádět několik útoků (deautentizace, chopchop, fragmentační útok, ...), test injekce paketů, falešnou autentizaci a reinjekci paketů do sítě
- **aircrack-ng** – nástroj na prolomení WEP či WPA/WPA2-PSK klíče
- **packetforge-ng** – vytváří šifrované pakety (např. ARP) vhodné pro reinjekci do sítě
- **besside-ng** – plně automatizovaný nástroj pro kompletní testování bezpečnosti sítě

Dá se říci, že i jen s pomocí utilit z balíku aircack-ng můžeme provést libovolný útok na Wi-Fi, ať už jde o získání skrytého SSID, útok na WEP, WPA, či vyřazení z provozu (DOS) některé ze stanic.

Praktické ukázky útoků spouštěné aplikací jsou realizovány právě pomocí nástrojů z balíku aircack-ng. Technicky se z aplikace napsané v Perlu zavolá sudo pro uživatele „root“ a aplikaci `gnome-terminal`, ve kterém se pustí konkrétní program pro vykonání požadovaného útoku. Parametry jsou programům předávany z naší aplikace, nebo jsou detekovány automaticky.

6.5.3. Wireshark

Wireshark je mocný analyzátor a sniffer síťového provozu, nejen pro Wi-Fi sítě, ale obecně pro jakoukoliv síť. Tento nástroj je vynikající pomocník při analyzování přenášených dat. V našem případě byl použit na rozbor zachycených paketů. Wireshark dokáže šifrovaná data za běhu dešifrovat.

[10] http://www.backtrack-linux.org/
[11] http://aircrack-ng.org/

6.5.4. Kismet

Pasivní monitorovací nástroj, který dokáže naslouchat síťovému provozu, identifikovat přístupové body a k nim připojené stanice. Zvládá též detekovat a odhalit SSID skrytých sítí, zobrazuje použité šifrování, datový tok a sílu signálu.

Kismet se hodí zejména pro zmapování sítí, přístupových bodů a k nim připojených stanic. Zobrazuje dokonce i IP adresy nalezených zařízení. Nalezené sítě můžeme třídit podle různých kritérií nebo si na konkrétní síti nechat vypsat tok dat. Lze omezit monitorování jen určitého kanálu. A pokud známe heslo k šifrované síti, dokáže Kismet, stejně jako Wireshark, šifrovaná data za běhu dešifrovat.

6.6. Live DVD

Pro zjednodušení a otestování celého řešení bez nutnosti instalovat dodatečné knihovny a nástroje, bylo vytvořeno linuxové live DVD. Toto live DVD umožňuje spustit předpřipravený operační systém GNU/Linux bez nutnosti instalace na pevný disk.

Dvd obsahuje linuxovou distribuci BackTrack Linux[12] ve verzi 5 R3. Distribuce je zaměřena na testování a audit bezpečnosti sítí. Pro úplnost jsou do ní doinstalovány knihovny gtk2-perl a perl-gtk2-webkit pro bezproblémový běh výukové demonstrační aplikace. Aplikaci lze jednoduše spustit kliknutím na ikonku na ploše.

[12] http://www.backtrack-linux.org/

7. Uživatelská příručka

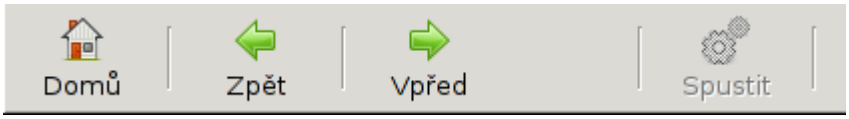
Aplikace lze spustit z předpřipraveného live DVD, po nastartování systému se na ploše objeví ikonka „prezentace“, na kterou stačí dvakrát kliknout.

Pokud instalujeme aplikaci samostatně, můžeme v terminálu použít příkaz:

```
./start.pl
```

Po startu se zobrazí úvodní menu, kde lze vybrat představení útoků formou tutoriálu a nebo přejít k praktickému útoku.

V horní části aplikace se nachází lišta s několika tlačítky.



Obrázek 6. Lišta v aplikaci, levá část

- **Domů** – tlačítko pro návrat do hlavního menu
- **Zpět** – skok o krok nazpět
- **Vpřed** – skok o krok dopředu
- **Spustit** – start praktického útoku. Pokud není útok možný, bude tlačítko neaktivní.
- **Index** – „expose“ efekt. Stránky tutoriálu se zmenší do kolekce pro rychlý výběr.
- **Přejít na** – skok na konkrétní číslo stránky
- **Obnovit** – převykreslení okna
- **Uložit** – vytvoření snímku obrazovky z právě prohlížené stránky. Obrázky se ukládají do složky `screenshots` ve formátu png.
- **Nápověda** – vyvolání nápovědy
- **Konec** – ukončení aplikace

Samotnou prezentaci lze ovládat postranními šipkami, umístěny jsou v polovině obrazovky na pravé i levé straně. Šipky mizí, pokud se už není kam posouvat.

V pravém dolním rohu je u každé prezentace zobrazen počet listů a aktuálně prohlížený list.

Aplikaci lze ovládat nejenom myší, ale i za pomoci klávesnice, viz Tabulka 3.

Obrázek 7. Lišta v aplikaci, pravá část

Klávesa/zkratka	**Funkce**
šipka doleva	posun v prezentaci o krok zpět
šipka doprava	posun v prezentaci o krok dopředu
m	funkce „expose“, náhledové okno pro rychlý výběr
g	zrychlený skok na vybranou stránku
ctrl+1	skok na první stránku prezentace
ctrl+s	vytvoření snímku obrazovky
ctrl+q	ukončení aplikace
ctrl+r	obnovení stránky

Tabulka 3. Klávesy a klávesové zkratky v aplikaci

Závěr

Hlavním přínosem této bakalářské práce je vytvoření snadno ovladatelné aplikace ilustrující praktický a teoretický aspekt nejčastějších Wi-Fi útoků, včetně představení dostupných zabezpečovacích technik. Dále se zde objevuje doporučení pro ochranu síťového provozu.

Obsah bakalářské práce neposkytuje prostor na podrobnou analýzu podnikového řešení WPA/WPA2 ani na útoky na TKIP.

Podle autora je zde navržená a vytvořená aplikace vhodná pro úvodní seznámení s problematikou otestování a zabezpečení Wi-Fi sítí v běžném provozu, neboť Live DVD lze pustit prakticky na libovolném počítači i nepříliš zkušeným uživatelem. Nejenže prezentuje teoretické základy jednotlivých útoků, ale navíc je, po výslovném souhlasu uživatele, i provádí.

Autor věří, že čtenář ocení univerzálnost použitého řešení pro analyzované případy, a naopak promine autorovi případné chyby vyskytující se v textu.

Conclusions

The main contribution of this work is to create easy-to-use application illustrating the practical and theoretical aspects of the most common Wi-Fi attacks. Including the presentation of available security technology.

Reference

[1] Wi-Fi Alliance, *http://www.wi-fi.org/*, Elektronická publikace.

[2] IEEE 802.11, *http://www.ieee802.org/11/*, Elektronická publikace.

[3] Aircrack-ng, *Documentation http://www.aircrack-ng.org/*, Elektronická publikace.

[4] Pužmanová Rita, *TCP/IP v kostce*, Koop nakladatelství, České Budějovice, 2009.

[5] Wireshark, *Documentation*, *http://www.wireshark.org/docs/*, Elektronická publikace.

[6] Outrata Jan, *Počítačové sítě*, *http://site.inf.upol.cz/*, Elektronická publikace.

[7] WiFi overview - Linux Wireless, *wireless.kernel.org*, Elektronická publikace.

[8] Airodump.cz, *http://wiki.airdump.cz/Airodump*, Elektronická publikace.

A. Příloha

- DVD – aplikace pro prezentaci, prezentace ve formě html stránek
- Live DVD – bootovatelné DVD s kompletním instalací GNU/Linux a všech potřebných nástrojů a knihoven, jak pro aplikaci tak pro ukázku útoku

B. Obsah přiloženého DVD

`aplikace/`
: Kompletní adresářová struktura grafické aplikace (v ZIP archivu).

`doc/`
: Dokumentace práce ve formátu PDF, vytvořená dle závazného stylu KI PřF pro diplomové práce, včetně všech příloh, a všechny soubory nutné pro bezproblémové vygenerování PDF souboru dokumentace (v ZIP archivu), tj. zdrojový text dokumentace, vložené obrázky, apod.

`src/`
: Kompletní zdrojové texty programu Aplikace se všemi potřebnými (převzatými) zdrojovými texty.

`readme.txt`
: Instrukce pro instalaci a spuštění programu Aplikace, včetně požadavků pro jeho provoz.

U veškerých odjinud převzatých materiálů obsažených na DVD jejich zahrnutí dovolují podmínky pro jejich šíření nebo přiložený souhlas držitele copyrightu. Pro materiály, u kterých toto není splněno, je uveden jejich zdroj (webová adresa) v textu dokumentace práce nebo v souboru `readme.txt`.