Bezpečnost a Hacking WiFi (802.11) - 4. část WPA a WPA2

Vložil/a matej [1], 3 Listopad, 2010 - 14:28

- Cracking [2]
- Hacking [3]
- Networks & Protocols [4]
- Security [5]
- WiFi & Wireless [6]

5. WPA a WPA2

Pre vyriešenie problémov súvisiacich s WEP bolo navrhnuté IEEE 802.11i [4], ratifikované v júni 2004. Definuje Robust Security Network (RSN) s odporúčaným TKIP (Temporary Key Integrity Protocol, protokol s integritou dočasných kľúčov) a CCMP (CCM, Counter-Mode/Cipher Block Chaining-Message Authentication Code, počítadlový mód s autentifikáciou správy reťazením blokov šifier, publikovaný ako NIST SP800-38C [5]). 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.

5.1 Špecifikácia WPA/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.

Všade, kde je to možné, by sa malo používať WPA2 – CCMP (AES).

5.1.1 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. Samotnú autentifikáciu nemusí robiť AP, ale môže na tento účel použiť centralizovaný RADIUS server (Remote Authentication Dial In User Service, protokol na autentifikáciu

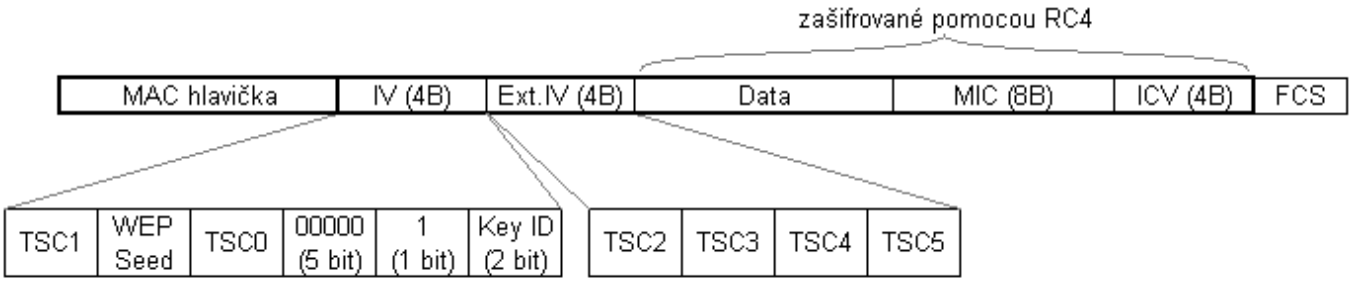
používateľov) – s ním komunikuje tiež pomocou IEEE 802.1x.
Typy EAP, ktoré Wi-Fi aliancia testuje a certifikuje pod WPA a WPA2 pre Enterprise (korporátne) použitie (program „Extended EAP“, ktorý bude o niekoľko mesiacov zrejme povinný pre certifikáciu WPA2), sú:

• **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 trasportnej 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 je možné používať aj iné typy EAP, medzi ktoré patria:
• **EAP-MD5**
• **LEAP** – Cisco Lightweight EAP.

V Enterprise prostredí je odporúčané používať iba certifikované výrobky. EAP MD5 a LEAP neboli do certifikácie zahrnuté kvôli nedostatočnej úrovni ochrany –napríklad meno používateľa je prenášané ako plaintext, slabá kryptografická úroveň (viď. 5.3 Slovníkový útok na LEAP), preto ich nie je vhodné používať.

5.1.2 TKIP

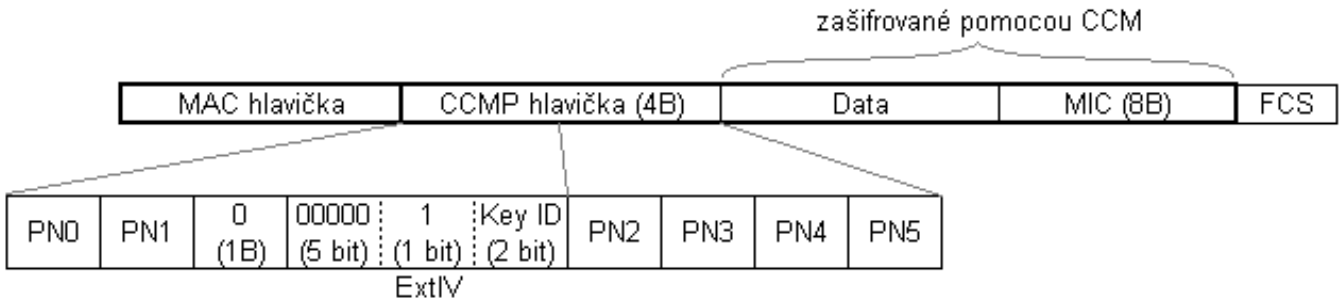


obr. 5 1: Enkapsulácia TKIP

TKIP bolo navrhnuté tak, aby išlo implementovať na starom hardvéri. Formát rámca zašifrovaného pomocou TKIP je na obr. 5 1 a je kombatibilný s pôvodným formátom (viď. obr. 4 1: Enkapsulácia WEP) – 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.

5.1.3 CCMP



obr. 5 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. 5 2. Nie je konkrétnym pravidlom odlíšiteľný od TKIP (viď. obr. 5 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.

5.2 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 PBKDF2 je definovaná v PKCS #5 [6].

5.2.1 Realizácia útoku na PSK

Demonštračná utilita coWPAtty umožňuje lámanie len pomocou slovníka, brute-force 8 až 64 znakových hesiel je takmer nemožný. Je potrebné zachytiť EAPOL rámce pri zostavovaní spojenia, čo môžeme dosiahnuť zachytávaním v monitorovacom režime pomocou wireshark a jednorazovým odpojením stanice, viď. 6.4 Deautentifikácia. Uložený pcap súbor potom môžeme použiť na lámanie:

```
$ ./cowpatty -s testt -f slovnik –r eapol.cap
cowpatty 4.0 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against passphrase.
Starting dictionary attack.  Please be patient.

The PSK is "12345678".

679 passphrases tested in 15.84 seconds:  42.88 passphrases/second
```

-s ... určuje SSID (musí byť správne, rozlišujú sa veľké/malé písmená),
-f ... určuje súbor so slovníkom,
-r ... určuje pcap súbor, z ktorého sa má načítať EAPOL komunikácia.

V teste bol použitý slovník 1000 číselných hesiel, ktorý obsahoval správne PSK – inak by nebolo nájdené.
Program coWPAtty umožňuje aj predvypočítanie hashov, čo je možné paralelizovať na viacerých počítačoch. Použitie SSID vo výpočte PMK však slúži na zasolenie („salt“) hashu, to znamená nutnosť vzťahovať všetky výpočty ku konkrétnemu SSID.

V októbri 2006 v projekte od Church of Wifi (http://www.churchofwifi.org/ [7]) nazvanom „Church of Wifi coWPAtty lookup tables“ predvypočítali zo slovníka 170 tisíc slov pre každé zo zoznamu top 1000 používaných SSID hashe pre coWPAtty. Tabuľka zaberá 7 GB a je k dispozícii na stiahnutie. To im nestačilo, a tak vo februári v projekte „Church of Wifi Uber coWPAtty lookup tables“ predvypočítali zo slovníka jedného milióna používaných 8- a viac-znakových hesiel tabuľky tiež k dispozícii na stiahnutie. Výpočet bol urobený pomocou 15-tich FPGA polí (Field-programmable gate array, programovateľné hradlové pole) za 3 dni.

5.2.2 Obrana pred slovníkovým útokom

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.

5.3 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 2003 v [17]. 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. k?ú?: H1 H2 H3 H4 H5 H6 H7`
- `2. k?ú?: H9 H10 H11 H12 H13 H14`
- `3. k?ú?: H15 H16 0 0 0 0 0 – pä? nulových bajtov`

Tretí kľúč má tak iba 216 možností – po dešifrovaní response vieme určiť 2 posledné bajty MD4 hashu, čo umožní jednoduché vyhľadanie v predvypočítanej 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) predvypočítané tabuľky. Proof-of-concept utilita asleap (http://asleap.sourceforge.net [8]) bola zverejnená v apríli 2004. Útoku je možné zabrániť použitím inej autentifikačnej metódy, napríklad EAP-TLS s existujúcou PKI.

5.4 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, bližšie opísané v kapitole 8.

5.5 Wi-Fi Protected Setup

Nový štandard WPS – Wi-Fi Protected Setup (zabezpečené nastavenie Wi-Fi) z januára 2007 od Wi-Fi aliancie je určený pre jednoduché bezpečné nastavenie domácej siete. Funguje na princípe autokonfigurácie, zariadenia môžu byť pripojiteľné do siete niekoľkými spôsobmi:

- **PIN metóda** – číslo prečítané z nálepky alebo displaya na novej stanici používateľ zadá do AP,
- **PBC metóda (push button)** – stlačením tlačidla na novej stanici aj AP,
- **NFC metóda (Near-Field Communication)** – blízkou komunikáciou – donesením novej stanice blízko ku AP,
- **USB metóda** – prenesením údajov medzi stanicou a AP pomocou USB kľúča.

Pre získanie WPS certifikátu musia všetky zariadenia podporovať PIN metódu, AP musia podporovať PBC metódu, ostatné metódy sú voliteľné. Samotná autokonfigurácia prebieha pomocou výmeny viacerých EAP správ.
Zatiaľ je tento štandard málo rozšírený, určený len na domáce použitie a na spustenie procesu má byť potrebná fyzická interakcia človeka. Je možné, že časom sa nájdu bezpečnostné chyby v špecifikácii WPS.

URL článku:
https://security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-4-%C4%8D%C3%A1st-wpa-wpa2

Odkazy:
[1] https://security-portal.cz/users/matej
[2] https://security-portal.cz/category/tagy/cracking
[3] https://security-portal.cz/category/tagy/hacking
[4] https://security-portal.cz/category/tagy/networks-protocols
[5] https://security-portal.cz/category/tagy/security
[6] https://security-portal.cz/category/tagy/wifi-wireless
[7] http://www.churchofwifi.org/
[8] http://asleap.sourceforge.net
[9] http://matej.sustr.sk/publ/dipl/
[10] http://creativecommons.org/licenses/by-nc/3.0/