Bezpečnost a Hacking WiFi (802.11) - 5. část Zamietnutie služby (DoS)

Vložil/a matej [1], 12 Duben, 2011 - 20:50

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

Útoky zamerané na zamietnutie služby sú na použitom médiu (vzduch) ľahko realizovateľné a dosahujú okamžitý účinok. Môžu mať niekoľko motivácii:
» škodoradosť / ekonomické ciele,
» dočasné odpojenie stanice zo siete za účelom získania informácii počas pripájania sa,
» odpojenie stanice zo siete za účelom man-in-the-middle útoku (viď. 8.1 Falošné AP),
» DoS iba na zabezpečenú sieť v snahe donútiť neskúseného používateľa vypnúť bezpečnostné prvky.

Väčšina z DoS útokov nie je trvalá, účinky pominú akonáhle útok prestane (okrem prípadov keď sa zariadenie zahltí alebo zasekne, viď. 6.5 Zahlcovanie tabuliek a 6.6 Spotvorené rámce) a sieť sa v krátkom čase (najviac niekoľko sekúnd) zregeneruje. Ich využitie na získavanie informácií alebo man-in-the-middle útoky je však signifikantné.

6.1 Rušenie pásma

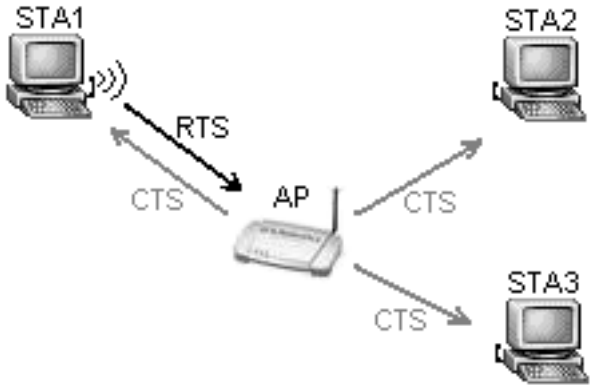
Pre efektívne rušenie pásma je najlepšie použiť zostrojenú rušičku na prislúchajúcich frekvenciách. Tiež je možné upraviť na tento účel ovládače WLAN karty tak, aby mohla odosielať rámce bez čakania (nulový backoff time) a floodovať kanál náhodnými dátami. Väčšina sieťových kariet ale neumožňuje konštantné vysielanie rámcov a firmware nedovolí vysielať v čase, kedy je detegovaná prichádzajúca komunikácia, a tak nedokážu kanál zahltiť úplne, ale iba zhoršiť priepustnosť a odozvu. Rušenie pásma je náročné na použitý hardvér a energiu, a v prípade dlhodobého rušenia je ľahko postihnuteľné (viď. 10. Legislatíva) a z bezpečnostného ohľadu je najmenej obávaným útokom.

6.2 CCA

V máji 2004 sa médiami prehnala správa o vážnom probléme v štandarde IEEE 802.11, konkrétne vo funkcii Clear Channel Assessment (CCA, odhad voľného kanála), ktorý umožňuje DoS na fyzickej vrstve. Jedná sa o testovací režim PLME_DSSSTESTMODE, ktorý je v štandarde uvedený ako odporúčaný, a umožňuje konštantné vysielanie DSSS (Direct Sequence Spread Spectrum, rozložené spektrum s priamou sekvenciou) nosného signálu. Na niektorých sieťových kartách bol tento režim prístupný, čím bolo možné s nízkou potrebou energie rušiť kanál. Funkcia CCA na ostatných zariadeniach vyhodnotí kanál ako obsadený, a teda nie je možné vysielať.
Väčšina sieťových kariet prístup k PLME vrstve (Physical Layer Management Entity, entity na manažment fyzickej vrstvy) neumožňuje, takže útok nie je veľmi rozšírený. Taktiež nie je známa utilita, ktorá by testovací režim dokázala na nejakej karte zapnúť.
Zariadenia IEEE 802.11a nie sú voči tomuto útoku náchylné, pretože pracujú v pásme 5 GHz. Zariadenia IEEE 802.11g použité v nemiešanom režime (t.j. iba g, bez podpory b) vďaka OFDM (Orthogonal Frequency Division Multiplex, multiplex s ortogonálnym delením frekvencií) tiež nie sú voči tomuto útoku náchylné.

6.3 RTS/CTS

Pre prítomnosť skrytých uzlov vo WLAN je v štandarde na zamedzenie kolízii pri posielaní dlhších rámcov definovaná technika riadiacich rámcov Request To Send (RTS, požiadavka na vyslanie) a Clear To Send (CTS, dovolené vyslať).



obr. 6-12: Príklad RTS/CTS komunikácie

Na obr. 6-12 je príklad použitia tejto techniky. STA1 a STA3 môžu byť navzájom mimo rádiového dosahu, teda STA1 nevie, či STA3 vysiela a naopak. Ak chce STA1 poslať dlhší rámec na AP a vyhnúť sa prípadnej kolízii, pošle najprv RTS s požiadavkou o „rezervovanie“ kanála na istú dobu, danú poľom Duration v rámci (trvanie). AP následne odpovie rámcom CTS, ktorý vyhradí kanál na danú dobu (Duration) pre STA1. Tento rámec je poslaný všetkým staniciam, aby bolo zrejmé, že v danej dobe môže začať vysielať iba STA1 (identifikovaná pomocou MAC adresy v CTS rámci).
Každá stanica si po prijatí RTS alebo CTS rámca podľa Duration nastaví Network Allocation Vector (NAV) – časovač, ktorý indikuje obsadenosť kanála (navyše od funkcie CCA).

6.3.1 Flood RTS rámcov

Cieľom útoku je bez energeticky náročného zahlcovania kanála zabrániť komunikácii. Princíp je nasledovný:

```
1. pošleme RTS rámec na AP s ve?kou hodnotou Duration
2. AP broadcastuje CTS rámec s ve?kou hodnotou Duration
3. stanice nevysielajú (o?akávaný efekt)
```

Štandard povoľuje staniciam vynulovanie NAV v prípade, že bol prijatý RTS rámec a v očakávanej dobe nebol detegovaný prichádzajúci signál (kanál ostal voľný) – to spôsobí „odignorovanie“ RTS/CTS a zabráni tak očividnému DoS.
To znamená, že NAV budú mať nastavené iba stanice, ktoré prvotný RTS nezachytili. Ostatné stanice, vrátane AP, môžu vysielať. Útok teda má požadovaný efekt v sieti, kde je veľa skrytých uzlov (napríklad mestské prístupové siete so smerovými anténami).

6.3.2 Flood CTS rámcov

obr. 6-13: Formát CTS rámca

CTS rámec je veľmi jednoduchý, určený na vyhradenie kanála na danú dobu. Posiela ho stanica alebo AP ako odpoveď na RTS rámec. Na obr. 6-13 je príklad CTS rámca – Frame Control (riadiace pole): Type 1 (Control) (typ=riadiaci rámec), Subtype 12 (Clear To Send) (podtyp=CTS), voliteľné (Flag) bity nastavené na 0 (tu je možných viac prijateľných kombinácii). Pole Duration (trvanie) je udávané v milisekundách, platné hodnoty sú 0 až 32767, udávané v mikrosekundách ako malý endián (menej signifikantný bajt je prvý). V našom prípade ho nastavíme na veľkú hodnotu 32000, čo je v hexadecimálnom tvare 7D00.
Pre Receiver Address (adresa prijímateľa) sú tiež možné alternatívy (existujúca adresa vrámci sieti, neexistujúca adresa). Frame check sequence (FCS) je vypočítavaný obvykle až pri odosielaní (hardvérovo), a preto nás nezaujíma.

6.3.3 Realizácia CTS útoku

Možné sú viaceré varianty útoku, s rôzne nastavenými flag bitmi v poli Frame Control, a s rôznymi cieľovými MAC adresami. Na odosielanie rámca
„C400007D010203040506“
s falošnou MAC adresou použijeme utilitu framespam (spomenutá v 2.3.2):

```
$ echo -en "\0304\0\0\0175\01\02\03\04\05\06" > CTS.packet      # \0 berie oct
hodnoty
# ./framespam -i rausb0 -d 30000 < CTS.packet

Frame Spammer
Copyright (c) 2007, Matej Sustr

Info    : Sending many frames (delay 30000 us)
......
```

-i ... určuje zariadenie na vyslanie rámca (musí byť v monitor mode),
-d ... určuje delays v mikrosekundách medzi rámcami (nezadané = 10000),
-n ... určuje počet rámcov, ktoré sa majú poslať (nezadané = nekonečno).
Na štandardný vstup presmerujeme rámec určený na odoslanie. Pri nezadanom parametri -n môžeme program zastaviť obvyklým spôsobom pomocou ctrl-c.

11 Mbit/s Ad-hoc sieť				54 Mbit/s Infraštruktúrna sieť				
čas odozvy (ms)					čas odozvy (ms)			
min	priem.	max	stratených		min	priem.	max	stratených
1.00	1.16	2.80	0%	bez útoku	0.67	2.33	14.18	0%
1.00	2.62	34.00	0%	CTS 60ms	0.67	12.28	123.53	0%
0.88	2.76	34.02	0%		0.87	43.79	2156.12	6%
0.88	2.97	34.33	0%		2.32	273.87	2172.40	32%
1.00	7.47	65.51	0%	CTS 30ms	0.63	27.30	1034.45	2%
1.31	16.11	66.01	13%		2.42	568.12	3219.15	46%
1.33	30.61	1901.34	79%		36.88	4312.31	6885.34	71%
-	-	-	100%	CTS 10ms	12.461	3259.294	4685.385	96%
-	-	-	100%		-	-	-	100%

tab. 6-5: Odozvy ping -f počas CTS útoku

Pomocou flood ping (ping -f) bola počas 10 sekúnd testovaná úspešnosť útoku na 11 Mbit/s ad-hoc a 54 Mbit/s infraštruktúrnej sieti. Reprezentačná vzorka z výsledkov je zaznamenaná v tab. 6 -5. Pri posielaní rámca CTS s hodnotou Duration 32000 („kanál rezervovaný na 32ms“) každých 60ms je zreteľné zvýšenie maximálneho času odozvy v oboch prípadoch.

Pri posielaní rámca každých 30ms došlo k značnej stratovosti najmä na 54Mbit/s sieti, ale nie

k úplnému vyradeniu z prevádzky. To mohlo byť spôsobené:
» oneskorením samotného programu (použitý časovač je málo spoľahlivá funkcia usleep()),
» oneskorením komunikácie s USB zariadením (sieťová karta),
» oneskorením vyslania rámca na sieťovej karte (kvôli CCA),
» stratou vyslaného CTS rámca (rušenie).

Pri pauze 10ms medzi jednotlivými CTS je však už sieť úplne vyradená z prevádzky, okrem prípadu keď je tento útočný CTS rámec stratený (stávalo sa na 54Mbit/s sieti). Pri 96% stratovosti už vyššie protokoly nedokážu komunikovať.

6.3.4 Obrana voči RTS/CTS útokom

Účinnou obranou voči RTS/CTS útokom môže byť:
» nedodržanie štandardu a ignorovanie CTS rámcov a hodnoty Duration všeobecne – na úkor zvýšenia kolízii pri prítomnosti skrytých uzlov,
» analýza rámcov a stanovenie, či je Duration rozumná hodnota (pre každý rámec, nielen CTS) – pre NAV používať iba rozumné hodnoty.

Uvedené spôsoby by musel implementovať výrobca zariadenia. IEEE by mohlo v budúcom 802.11w definovať nejaký spôsob ochrany voči týmto útokom. Šifrovanie, resp. podpisovanie riadiacich rámcov je však problematické, keďže v zdieľanom pásme by mali vedieť súčasne pracovať viaceré nezávislé siete.
Wireless IDS môže pomôcť útok odhaliť a upozorniť naň administrátora.

6.4 Deautentifikácia

Keďže management rámce nie sú nijakým spôsobom chránené, je ľahké ich sfalšovať. Týmto môžeme dosiahnuť odpojenie stanice zo siete po dobu útoku. Deautentifikáciu môžeme docieliť rôznymi spôsobmi:
» poslanie falošného „Deauthentication“ rámca stanici (od AP);
» poslanie spotvoreného „Authentication“ rámca AP (od stanice), napríklad so zlým sekvenčným číslom alebo použitým algoritmom – AP následne stanicu deautentifikuje.

6.4.1 Zmazanie ARP cache

Ak útok trvá dlhšie (3-5 sekúnd), OS Windows pripojenie indikuje ako „odpojené“, čo si používateľ môže všimnúť. Dosiahneme tým však zmazanie ARP cache, teda po zastavení útoku a obnovení spojenia sa pošle ARP request akonáhle stanica bude chciet komunikovať pomocou IP protokolu (čo býva aj na stanici bez prítomnosti používateľa).
Toto môžeme využiť pri útokoch na WEP – najmä reinjekcia ARP (viď. 4.2.1), potrebná pre Kleinov útok (viď. 4.9).

6.4.2 Realizácia deautentifikačného útoku

Na jednoduchý deautentifikačný útok môžeme v monitorovacom režime použiť program aireplay-ng z balíka Aircrack-ng:

```
# ./aireplay-ng -0 0 -a 00:11:3b:07:00:14 -c 00:11:3b:0b:22:0c rausb0
02:07:23  Sending DeAuth to station   -- STMAC: [00:11:3B:0B:22:0C]
02:07:24  Sending DeAuth to station   -- STMAC: [00:11:3B:0B:22:0C]
...
```

-0 0 určuje typ útoku (deauth) a počet rámcov na vyslanie (0 = nekonečno),
-a ... určuje MAC adresu AP (zhodné s BSSID),
-c ... určuje cieľovú MAC adresu, ktorá má byť deautentifikovaná,

rausb0 je zariadenie použité na vyslanie rámca (musí byť v režime monitor).

Deautentifikačný rámec sa pošle každú sekundu, čo stačilo na úplné vyradenie klienta pri použití WEP, WPA-TKIP aj WPA2-AES zabezpečenia. Ovládač sa pokúšal o opätovnú autentifikáciu a asociáciu, na čo vždy v zápätí dostal deautentifikačný rámec a musel začať odznovu. Po dobu útoku (30 sekúnd) bola sieť „odpojená“, ARP cache sa zmazala a nebola možná žiadna komunikácia. Po zastavení útoku sa stanica do 1 až 5 sekúnd asociovala, (v prípade WPA a WPA2) prebehla výmena kľúčov cez EAP a pripojenie bolo opäť funkčné.

6.4.3 Obrana pred nežiadúcou deautentifikáciou

Riešenie kompatibilné s existujúcim hardvérom navrhli John Bellardo a Stefan Savage v . Keďže žiadna stanica sa nedeautentifikuje pred následným vyslaním dát, treba implementovať časovač (napr. 5-10 sekúnd), ktorý by deautentifikáciu oneskoril – ak bude v tomto intervale prijatý dátový rámec, deautentifikácia sa ignoruje; ak nie, vykoná sa. Implementácia je možná na softvérovej úrovni (ovládač) buď výrobcom, alebo open-source vývojármi.
Budúci IEEE 802.11w zrejme prinesie „autentifikovanú deautentifikáciu“ (podpísané management rámce), ktorá takisto tento problém vyrieši.

6.5 Zahlcovanie tabuliek

Každé zariadenie má obmedzenú pamäť. Jednoduché AP, určené pre domácnosti a malé firmy, dokážu autentifikovať a asociovať len malé množstvo staníc (väčšinou 16 až 256). To na legitímne používanie postačuje, pri útoku sa však tabuľky určené na udržiavanie informácií o stave autentifikácie, asociácie a vzájomného šifrovacieho kľúča (v prípade WPA/WPA2) jednotlivých staníc môžu zaplniť. AP potom nie je schopné obslúžiť žiadneho ďalšieho klienta – v prípade, že počas útoku navyše deautentifikujeme legitímne stanice, bude sieť vyradená z prevádzky.
Útok môžeme urobiť v monitorovacom režime pomocou programu aireplay-ng z balíka Aircrack-ng, a to v cykle:

```
# hex="0 1 2 3 4 5 6 7 8 9 A B C D E F"; AP=“00:11:3b:07:00:14“
for i1 in $hex; do for i2 in $hex; do for i3 in $hex; do
  ./aireplay-ng -1 0 -e testt -a $AP -h de:ad:be:ef:0$i1:$i2$i3 rausb0
done; done; done
07:34:01  Waiting for beacon frame (BSSID: 00:11:3B:07:00:14)
07:34:01  Sending Authentication Request
07:34:01  Authentication successful
07:34:01  Sending Association Request
07:34:01  Association successful :-)
...
07:35:15  Sending Authentication Request
07:35:15  Authentication successful
07:35:15  Sending Association Request
07:35:15  Association denied (code 17)
```

-1 0 určuje typ útoku (fake assoc) a počet reasociácii,
-e ... určuje SSID siete,
-a ... určuje MAC adresu AP (zhodné s BSSID),
-h ... určuje falošnú MAC adresu, ktorú autentifikujeme a asociujeme,
rausb0 je zariadenie použité na vyslanie rámca (musí byť v režime monitor).

Použité AP síce po asociovaní 128 staníc niekoľko krát asociáciu odmietlo kódom 17 („asociácia zamietnutá, pretože AP nemôže vyhovieť ďalším asociovaným staniciam“), so vzniknutou situáciou sa však hravo vysporiadalo – po istom čase od asociovania posiela niekoľko Null function rámcov asociovanej stanici. Ak nie je prijatý ACK (Acknowledgement, potvrdzovací riadiaci rámec) na žiaden z nich, stanicu jednoducho bez oznámenia z tabuliek odstráni.
Na dobre navrhnutých AP nie je tento typ útoku závažný, po odchode útočníka sa dokážu ľahko

zregenerovať vyradením neaktívnych staníc.

6.6 Spotvorené rámce

Chybne implementovaný firmware a ovládače je možné poslaním konkrétne zostaveného rámca zaseknúť. Môžu potom vykazovať rôzne nepredpokladané stavy – v prípade samostatných zariadení „zatuhnutie“ alebo podivné správanie sa; v prípade OS GNU/Linux zaseknutie sa ovládača jadra alebo kernel panic; v OS Windows zaseknutie systému alebo blue-screen.

Vo všeobecnosti sú takýmito rámcami také, ktoré majú niektoré z polí dlhšie, ako je maximálna veľkosť podľa špecifikácie. Môžu to byť napríklad Beacon alebo Probe rámce s príliš dlhým SSID. Zostrojiť takýto rámec môžeme ručne (v spolupráci s Wireshark pre referenciu jednotlivých polí) a poslať pomocou utility framespam.
Buffer overflow v ovládačoch je niekedy možné zneužiť aj na prienik do systému. Viac o tejto problematike je v časti 7.1.

6.7 Útok na MIC v TKIP

Návrhári si boli vedomí kryptograficky slabého algoritmu Michael použitého na výpočet MIC v TKIP, preto je zakomponovaná ochrana voči útoku na MIC. Ak v prijatom rámci je správne FCS aj ICV, ale MIC nie, je pravdepodobné, že sa jedná o útok. Štandard určuje, že počet zlyhaných MIC môže byť najviac jedno za minútu – ak sú v intervale 60 sekúnd prijaté 2 rámce, v ktorých MIC takto zlyhalo, musí sa príjem rámcov na minútu zastaviť a následne vymeniť šifrovacie kľúče pomocou EAPOL. Každé zlyhanie MIC má byť zaznamenané a hlásené administrátorovi.
Tento prístup zabráni útokom na obsah prenášanej správy, ale môže viesť ku DoS. Udalosť má však byť zaznamenaná a hlásená, preto je použitie na nenápadný DoS útok nevhodné. Účinnou obranou voči takémuto možnému útoku je použitie WPA2 (AES šifrovania).

6.8 Mazanie rámcov (teoretické)

Prenos rámcov v IEEE 802.11 je s kladným potvrdzovaním – každý úspešne prijatý rámec adresát ihneď potvrdí odpoveďou (v prípade management rámcov) alebo krátkym ACK rámcom. Teoreticky je možné prenášanému rámcu poškodiť integritu (napr. zašumením), teda kontrolný súčet (FCS) u príjemcu nesadne a rámec sa zahodí. Následne môžeme poslať sfalšovaný ACK rámec, čo spôsobí, že odosielateľ považuje rámec za doručený a nebude ho opakovať.

Tento útok vyžaduje hardvér schopný vysielať v konkrétnom požadovanom čase a jeho praktická implementácia nie je známa. Navyše spojovo orientované protokoly vyššej vrstvy (TCP) dokážu správu doručiť aj cez chybový kanál.

URL článku:
https://security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-5-%C4%8D%C3%A1st-zamietnutie-slu%C5%BEby-dos

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://matej.sustr.sk/publ/dipl/
[8] http://creativecommons.org/licenses/by-nc/3.0/