Методи за намалување на ефектот на ICMP Smurf нападот врз безжичните мрежи

Александар Тошевски, Митко Богданоски

Европски Универзитет – Скопје Р.Македонија,

toshevski.aleksandar@live.eurm.edu.mk, mitko.bogdanoski@eurm.edu.mk

***Апстракт* – 802.11, или популарно наречени Wi-Fi мрежи, моментално се на врвот на својот развој и популарност. Прилично се евтини, затоа што ги намалуваат трошоците кои се потребни за една жичана инсталација, а нудат голема флексибилност и голем домет, па затоа се користат од интернет провајдери, компаниии, институции, па се до домаќинства. Лесни се за имплементација, бидејќи е доволно само пристапна точка или базна станица и кориснички станици со безжични картички кои се поврзуваат на неа. После автентификацијата, мобилните корисници можат да се движат низ покриената зона без загуба на сигнал или конекција. Лошата страна на овие мрежи е што тие имаат нејасни граници, така олеснувајќи му на напаѓач да собере испратени пакети. Овој труд во првиот дел ги опишува некои од главните ранливи точки на безжичните мрежи, а во вториот дел детално го обработува ICMP Smurf нападот за одбивање на услуги (Denial of Services - DoS), како и одредени методи за спречување и намалување на ефектите од овиј напад.**

***Клучни термини* – ICMP Smurf напад, ранливост, безжични мрежи, безбедност.**

I. ВОВЕД

Главни карактеристики на 802.11 стандардот се можноста за пренос на радио сигналите преку нелиценциран фреквентен спектар, ефикасното кодирање на канали и релативно евтините уреди. Во моментов во употреба има преку 6.3 милијарди безжични уреди. Продажбата на уреди кои се базираат на 802.11 стандардот поради ниската цена на чинење и лесната имплементација константно расте. Работата во незаштитениот фреквентен опсег и широка искористеност го прават овој стандард лесно достапна и примамлива мета за потенцијални напаѓачи. Сепак, одредени истражувања откриј основни недостатоци во механизмите за криптирање [1,2] и автентификациските протоколи [3], како и недостатоци во основните мрежни протоколи, што конечно доведе до развој и создавање на серија од протоколи, додатоци и замена на постоечките.

Постојат безброј примери за злоупотреба на слабостите на овој стандард преку DoS напади. Први DoS напади во големи размери, кои го привлекоа јавното внимание, се случија во Февруари 2000 година [4]. Големи сајтови, меѓу кои и оние на CNN, Yahoo и Amazon, неколку дена страдаа од дистрибуирани напади. После неколку месечна истрага беше уапсен 15-годишен Канаѓанец со алиас Mafiaboy [5], и истиот беше обвинет за извршување на нападите. Во Јануари 2001, тој ги призна делата и се изјасни како виновен за 56 криминални дела поврзани со инцидентот. CNN и другите жртви тврдеа дека нападот направил штета од околу 1.7 милијарди долари. Од тогаш во медиумите објавени се информации за многу други напади. Сепак, веројатно дека и многу големи и добро познати компании не пријавуваат DoS напади со цел да ја зачуваат добрата корпоративна слика за својата компанија. Еден од најинтересните и најнови напади е DDoS нападот на веб сајтот на Wikileaks [6], кој беше неоперативен неколку часови, пренасочувајќи ги посетителите кон сервер изнајмен од Amazon.com.

Во овој труд ќе се задржиме на недостатоците на криптирањето и ICMP протоколот.

II. ИСКОРИСТУВАЊЕ НА СЛАБОСТИТЕ НА БЕЗЖИЧНИТЕ МРЕЖИ

Во оваа секција ќе бидат разработени недостатоците на безжичните мрежи преку слабостите на нивното криптирање и автентификација и мрежните протоколи.

А. Слабости на криптирањето

WEP (Wired Equivalent Privacy) е издаден во 1997, и дизајниран да обезбеди компатибилност со безбедноста на жичаните мрежи. Без разлика на тоа колку е добар или лош, долг или краток, WEP

клучот може да биде разбиен. WPA (Wi-Fi Protected Access) е алгоритам за криптирање, кој е замена за WEP. WPA се разликува од WEP бидејќи има поголеми 48 битни иницијализирачки вектори и користи Temporal Key Integrity Protocol (TKIP). TKIP динамички и фреквентно ги менува клучевите и обезбедува заштита од напади врз нив. WPA клучот може да се направи доволно силен за да се оневозможи разбивање со речник.

WPA2 е базиран на архитектура за робустна безбедносна мрежа (Robust Security Network), кој обезбедува поддршка за сите механизми кои се на располагање во WPA, како и:

1. Силна криптирачка и автентикациска поддршка кај инфраструктурните и ад-хок мрежите (WPA е ограничена само на инфраструктурни мрежи),
2. Намален overhead во деривацијата на клучот при автетификацијата,
3. Поддршка за кеширање опортунистички клучеви за намалување на overhead-от при роаминг помеѓу точки за пристап,
4. Поддршка за пред-автентификација, каде станицата ја комплетира IEEE802.1x автентикациската размена пред роаминг,
5. Поддршка за CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) енкриптирачки механизам базиран на Advanced Encryption Standard (AES) шифра како алтернатива на TKIP протоколот.

WPA2 е најнапреден протокол за криптирање искористен кај 802.11 мрежите и од март 2006 година е задолжителен за сета нова опрема. Сертифициран е од страна на Wi-Fi Alliance, осигурувајќи дека секој релативно модерен хардвер ќе ги поддржува и WPA и WPA2. Сепак, Md Sohail Ahmad пронајде недостаток во WPA2 [7] кој овозможува man-in-the-middle-style експлоатација, кога еден Wi-Fi корисник собира податоци од други легитимни корисници и инјектира злонамерен сообраќај во мрежата.

Слабостите на WEP

Wired Equivalent Privacy (WEP) е безбедносен протокол кај безжичните мрежи кој ги криптира податоците наменети за испраќање. Во мрежа заштитена со WEP, сите станици делат еден симетричен клуч Rk наречен root клуч. При трансфер може да се изгуби пакет поради грешка во преносот, па затоа WEP ги криптира сите пакети посебно. WEP генерира 40 битен клуч за секој пакет. 24 битен иницијализациски вектор (IV) се додава на root клучот Rk, и од овие два елементи се добива К клучот за секој пакет. Низа од клучеви се генерира од К. За заштита на интегритетот на М пораката во отворен текст се додава 32 битен CRC32 (Cyclic Redundancy Check) checksum наречена ICV (Integrity Check Value). Добиениот отворен текст потоа се криптира со XOR енкрипција со низата од клучеви. Добиениот шифриран текст, заедно со кореспондирачкиот иницијализирачки вектор, се праќаат. Криптираната порака е одредена со следната формула:

$$C = [M \,||\, ICV] + [RC4(R_k \,||\, IV)]$$

Каде || е конкатенација, а + е XOR операцијата.

Приемната станицата, како точка за пристап или некој друг радио NIC, по пристигнувањето на рамката врши декриптирање. Како резултат на тоа, WEP врши криптирање на податоци само помеѓу 802.11 станиците. Откако рамката влегува во жичната страна на мрежата, како на пример меѓу пристапните точки, WEP повеќе не се користи. WEP е ранлив поради релативно кратките IV-и и клучевите кои остануваат статични. RC4 алгоритмот за криптирање не е виновен за овие слабости. Со само 24 бита, WEP секогаш ги користи истите IV за различни податочни пакети. За големи зафатени мрежи, повторувањето на IV-и може да се случи во рок од околу еден час. Ова резултира во пренос на рамки кои имаат поток од случајни карактери кои се премногу слични. Доколку напаѓач собере доволно рамки базирани на истиот IV, тој може да ги утврди споделените вредности меѓу нив, односно, на поток од случајни карактери или споделениот таен клуч. Ова секако води до декриптирање на било која 802.11 рамка.

Слабости на WPA

WPA користи два алгоритма за криптирање на податоците за транспорт, TKIP и AES. Ќе се фокусираме на TKIP, што е модифицирана верзија на WEP. Користи софистицирана функција за мешање на клучеви со иницијализирачки вектори за доделување на секој пакет. Со ова се спречуваат сите досегашни напади врз клучевите, бидејќи секој бајт од клучот зависи од секој бајт од сесискиот клуч и инцилизирачкиот вектор. Додатно, се вклучува 64 битен Message Integrity Check (MIC) наречен MICHAEL, во секој пакет за да се спречи напад на слабиот CRC32 механизам за заштита на интегритетот. За да се заштити од replay напади се користи TSC (Time Stamp Counter) бројач на секвенци кој дозволува пакетите да стигнуваат само редоследно.

За да се нападне мрежата, напаѓачот собира сообраќај сé додека не дојде криптирано ARP (Address Resolution Protocol) барање или ARP одговор. Овие пакети се лесни за препознавање поради карактеристичната должина. Додатно, изворната и дестинациската Ethernet адреса не се заштитени од WEP и TKIP и барањата се праќаат до broadcast адресата. Поголемиот дел од

пратената информација му е позната на напаѓачот, освен последниот бајт од изворната и дестинацискатa IP адреса, 8 бајтниот MIC и 4 бајтната ICV checksum.

Сега напаѓачот може да лансира модифициран chopchop [8] напад кон WEP мрежата за да ги декриптира непознатите бајти од отворен текст.

Martin Beck и Erik Tews во својот труд "Practical attacks against WEP and WPA" [9] презентираат напад врз TKIP криптиран сообраќај. Во рок од 12-15 минутен пристап до мрежа успеале да декриптираат ARP request и response и испратиле 7 пакети со прилагодена содржина во мрежата.

Според Guillaume Lehembre [10] најпрактична ранливост на WPA е напад кон неговиот PSK, односно на PMK (Primary Master Key) кој е добиен со користење на алгоритмот PBKDF2 (Password–Based Key Derivation Function) за претворање на лозинката, SSID (Service Set ID), должината на SSID, големината на хешовите (4096) и должината на излезот (256). WPA 4-насочниот handshake е дизајниран да се реализира преку несигурни канали и со отворен текст, и единствен чекор што треба да се направи е да се фати полн автентикациски 4-насочен handshake помеѓу легитимен клиент и AP. Ова не е лесно да се направи без инјекција на пакет, но ако има среќа да се фати целосен handshake, во тој случај може да се реализира разбивање. Може да се присили на автентификациски handshake со лансирање на деавтентификациски напад, но само ако постои легитимен клиент кој е веќе поврзан.

B. Слабости на мрежните протоколи

Тука, накратко ќе бидат објаснети најчестите видови на DoS напади кои се јавуваат на различните мрежни нивоа.

DoS на физичко ниво

DoS нападите на физичко ниво се општо познати како попречување (jaming). Попречувањето има за цел да се спречи станица, како и AP успешно да емитува или прима рамки во физичкото ниво, така што рамките не можат да се пренесат на повисоките нивоа.

DoS нападите врз физичкиот слој можат да се класифицираат според нивните цели:

- Напад со бесконечни ресурси - Resource Unlimited Attack (RUA),
- Напад врз преамбула,
- SFD (Switched Firewall Director) напад,
- Реактивен напад,
- HR (Удри и Бегај) напад,
- Напад врз симболи,
- Монополизирачки напад.

Напади на MAC ниво

MAC протоколот на 802.11 дозволува напаѓачот селективно или комплетно да го наруши пристапот до мрежата со користење на неколку пакети и ниска потрошувачка на енергија.

Селективни MAC напади се напади каде напаѓачот цели кон индивидуална станица, не кон целата мрежа:

1. Деавтентикациски/Деасоцијативен напад,
2. Duration inflation напад,
3. Напад кон 802.11i,
4. Напад против sleep модот.

Комплетнитете MAC напади се напади врз AP за трошење на нејзините конечни пресметувачки и мемориски ресурси и таа не може да нуди услуги на други станици. Тие напади се следните:

1. Преплавување со барања за проверки,
2. Преплавување со автентикациски и асоцијативни барања.

Напади на мрежно ниво

Ако напаѓач успее да се поврзе на безжичната мрежа, тогаш без проблеми може да изврши DoS напад. Нападот се извршува со праќање на голема количина на податоци кон жртвата. Примери на вакви напади:

1. ICMP Flood,
2. ICMP Smurf,
3. Ping of Death,
4. Fragile,
5. Teardrop,
6. Рутирачки (RIP) напади.

Напади на транспортно ниво

Нападите кон транспортното ниво користат барања за конекција кон оперативниот систем на жртвата. Примери за вакви напади се:

1. TCP SYN напад,
2. SSL Man-in-the-Middle напад,
3. Land напад,
4. TCP Connection Hijacking,
5. UDP Flood напад,
6. Port Scan напад.

Напади на апликациско ниво

Се изведуваат со праќање на големо количество легитимни барања кон апликација. На пример, HTTP flood нападот може да прати стотици илјади page request до веб сервер и да ја потроши серверската можност за процесирање.

Според методите кои ги користат, DoS нападите се делат на неколку видови:

1. **Трошење на пропусен опсег (Bandwidth Consumption)** - напаѓачи го завземаат пропусниот опсег на далечинска или локална мрежа. Мрежната врска на жртвата е сатурирана од големиот сообраќај генериран од напаѓачот.

2. **Изгладнување за ресурси** - овој вид на напад ги таргетира системските ресурси на машината на жртвата. При овој напад машината не е во можност да работи нормално и да обезбедува услуги низ мрежата. Напаѓачот ќе ја злоупотреби алоцираната квота на системски ресурси за да ја урне машината и метата ќе биде приморана да ја ресетира поради оптовареност на системот и пре-искористеност на процесорот, или, ако напаѓачот успее да се здобие со недозволен пристап, едноставно да ги оневозможи процесите со извршување на kill команда.

3. **Недостатоци при програмирање** - оперативните системи, апликациите или вградениот софтвер паѓаат при справување со посебни услови. Напаѓач може да го злоупотреби овој недостаток и да прати непрописни пакетски податоци, со цел да створи состојба на пренатрупување на меѓумеморијата (buffer overflow) и да го крахира системот. На пример, озлогласениот Pentium .f00f DoS напад дозволуваше кориснички процес да крахира било кој оперативен систем со извршување на невалидната инструкција 0xf00fc7c8. [11]

4. **Рутирачки и DNS напади –** овие напади можат да бидат катастрофални и тешки за откривање. Ги искористуваат слабостите RIP v1 и BGP v4 рутирачки протоколи за манипулација на рутирачките табели, негирајќи услуги за легитимните мрежи. Сообраќајот на жртвите е рутиран до мрежата на напаѓачот или до "црна дупка" (мрежна адреса која не постои – Black Hole). DNS протоколот е наследно ранлив на овој вид на напад поради слабоста на своите 16-битни трансакциски ID-ја, кои се користат при комуникација со други системи. Кога DNS изведува lookup, ќе врати погрешна IP адреса за domain name, пренасочувајќи кон "црната дупка" или до напаѓачот, каде што од жртвата можат да бидат побарани доверливи податоци кои можат да бидат злоупотребени (пр. податоци за кредитни картички). Ова е познато како DNS cache poisoning. Во 1993 Кристоф Шкуба издал труд "Addressing Weakness in the DNS Protocol" [12], во кој ги објасни ранливостите и техниката DNS Cache Poisoning.

5. **Генерички DoS напади** – во оваа категорија спаѓаат сите DoS напади кои не спаѓаат во горенаведените категории и можат да се опишат како генерички. Тие можат да делуваат на многу различни системи и ефектите кои се појавуваат кај жртвите се слични со "изгладнување" за ресурси и нападите за трошење на пропусен опсег. Поголем број од овие напади користат некаков вид на манипулација на протоколи. Најчесто се бираат интернет протоколите од транспортното и мрежното ниво (пр. TCP, UDP, IP, ICMP). IP spoofing е заедничка техника речиси за сите овие напади. Оваа техника се изведува со манипулација на изворната IP адреса во IP насловот на пратениот пакет. Со цел напаѓачот да ја продолжи ефективноста, а да го намали запирањето и лоцирањето користи лажна IP адреса. Со ова тој добива некаква анонимност.

III. ICMP Протокол

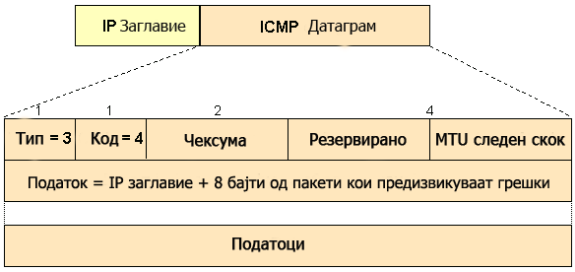
Internet Control Message Protocol (ICMP) документиран во RFC 792 [13], е протокол за дијагностицирање и пријава на грешки. Истиот се смета за потребен дел од секоја IP имплементација. Протоколот е длабоко интегриран во IP, но сепак доставата на пакети е недоверлива. Главни функции на ICMP протоколот се:

1 **Објавување на мрежни грешки** – како што се недостапност на машина или цела секција од мрежата.

2 **Објавување на мрежно загушување** – кога рутер ќе почне да баферира премногу пакети, со оглед на тоа што не може да ги прати доволно брзо како што стигнуваат, ќе генерира *ICMP Source Quench* пораки за намалување на брзината на испраќање. Ова ќе предизвика намалување на брзината за пренос на пакети.

3 **Помош при барање неисправности** – ICMP поддржува ECHO функција, која праќа двостран ехо пакет помеѓу две машини. Ping е вообичаена алатка за менаџмент на мрежата и е базиран врз оваа ECHO функција. Ping праќа серија на пакети и го мери средното време на патување и процентуално пресметува загуба на пакети.

4 **Објавува Тајмаут** – ако TTL (време на живот) полето на IP пакетот падне на нула, рутерот го отфрла пакетот и најчесто генерира ICMP пакет со објава за ова. Постојат севкупно 11 видови ICMP пораки, секоја од нив со специфичен код. RFC 972 комплетно ги дефинира сите типови на наслови. Форматот на ICMP насловот зависи од видот на пратените пораки.

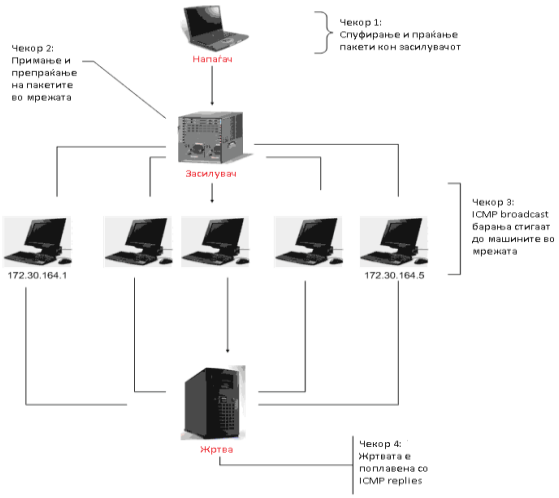


Сл. 1- ICMP Заглавие

На слика 1 е прикажано заглавието на ICMP пораката. Полето со IP адреса од изворот во ECHO порака ќе биде дестинација за ECHO reply пораката. За да се формира ECHO reply порака, изворната и дестинационата адреса ги заменуваат местата, кодот за тип се менува во нула, и сумата за проверка (или hash сума) повторно се пресметува. Многу DoS напади го експлоатираат користењето на ICMP ECHO пораки (и се разбира Ping командата). Примери за вакви напади се Smurf, Ping Flood и Ping of Death, како посебен вид на Ping Flood напад.

SMURF Напад

Овој напад е DoS напад, каде напаѓачот генерира значително голем сообраќај со кој го оневозможува работењето на одреден хост или дел од мрежата. Ова го постигнува со ангажирање на одреден број на машини за засилување (амплификација) на сообраќајот и ја искористува слабоста на ICMP протоколот. Еден од најпознатите Smurf напади се случи 1998 врз мрежата на Универзитетот во Минесота [14] и нападот траел околу еден час.
Нападот почнува со праќање на неколку “spoofed” ICMP ECHO пакети до “broadcast” адресата (најчесто .255) од амплификациската мрежа. Се лажира полето со изворната адреса за да изгледа како жртвата да го пратила барањето. Бидејќи ICMP ECHO барањето е пратено на broadcast адреса, сите машини од засилувачката мрежа одговараат на жртвата. Пример, еден ICMP ECHO пакет пратен на засилувачка мрежа од сто машини му дозволува на напаѓачот да го засили DoS нападот за сто пати. За време на нападот се зафатени и посредникот (напојувачот) и жртвата.

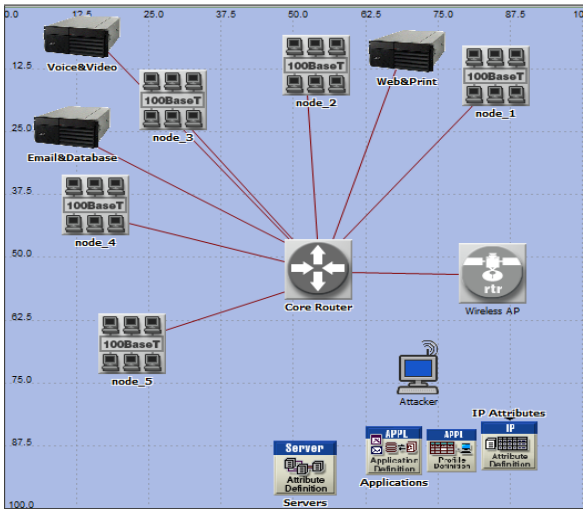


Сл.2 Smurf Напад

Секоја машина на засилувачката мрежа што има можност за овозможено ECHO ќе одговори кон жртвата, правејќи голема количина на сообраќај. Логичка шема на овој напад е прикажана на слика 2.

Симулација и Анализа на Smurf нападот

Бидејќи за изведување на Smurf напад ни требаат голем број на машини кои ќе служат за амплификација, изведувањето на нападот во мала лабораторија е непратично и потешко изводливо, а евентуалното негово изведување користејќи го Интернетот е нелегално. Затоа, презентирањето на ефектите на овој напад ќе биде со помош на OPNET Modeler, кој е одличен за симулирање и собирање на податоци за анализирање.



Сл. 3 Скица на симулацијата

Во нашиот проект имаме една локална мрежа со чија помош ќе симулираме напад. Напаќачот мрежата ја напаќа преку безжичната.

Ќе разгледаме три сценарија. Во првото нема никаков напад и мрежата работи без пречки, во второто е изведен напад со голем број на засулувачки машини, а во третиот најголем број на засилувачки машини.

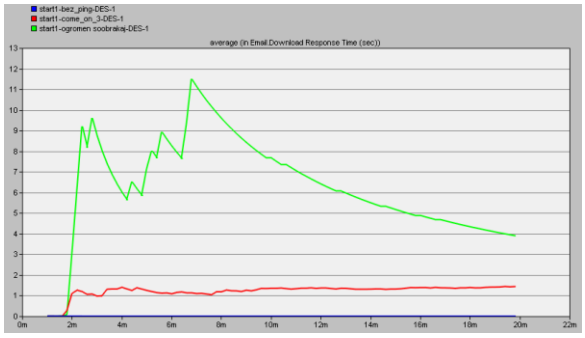
Табела 1. Карактеристики на нападите

	Напад 1	Напад 2	Напад 3
Број на засилувачи	0	24500	35840
Интервал (секунди)	2	2	2
Големина на пакети (бајти)	64	64	64
Број на испратени пакети	Unlimited	Unlimited	Unlimited
Timeout (секунди)	20	20	20

Времето на симулација е 20 минути. Почетокот на профилот е подесен на 100 секунди и време издвоено за апликациите од 5 секунди. Ова време се смета за време за загревање, кое овозможува процесите во системот да дојдат во нормала.

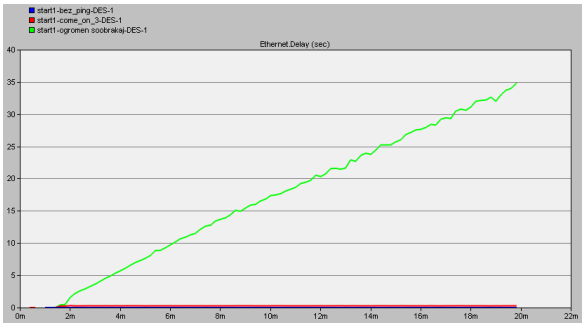
Овде ќе презентираме средни вредности од симулираните глобални статистики на сценариото.

Слика 4 го покажува времето на одзив на серверот за електронска пошта во трите ситуации. Очигледно е дека времето на одзив на многу варира во трите случаи.



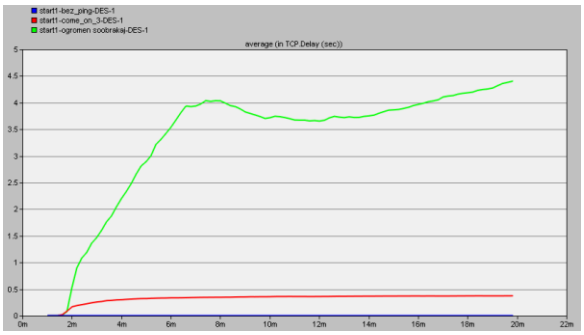
Слика 4. Време на одзив на Email серверот

На Слика 4 е прикажано доцнењето низ мрежата за трите случаи. Од сликата може да се забележи дека имаме значително доцнење во третиот случај, кое всушност е неприфатливо доцнење на мрежата. Ова предизвиикува и значително намалување на QoS (квалитетот на услуга) низ системот.



Слика 5. Ethernet доцнење

Од Слика 6 може да се забележи дека доцнењето во TCP комуникацијата е зголемено и во двата случаи, но доцнењето предизвикано во третиот случај е и до десет пати поголемо од претходната ситуација, кога мрежата е нападната со помал број засилувачки машини. Ова значи дека апликациите и процесите кои го користат овој протокол ќе имаат големи проблеми да функционираат нормално.



Слика 6. TCP доцнење

Според Sanjeev Kumar [15], ако пропусниот опсег на напаѓачот е *Bp* во битови по секунда, тогаш максималниот број на ICMP ECHO пораки пратени кон засилувачкиот домен е:

$$A = \left[\frac{B_p}{M1 + M2} \right] \qquad (1)$$

Каде *M1* е големината на ICMP Echo request пораката, а *M2* е overhead-от потребен за да се испрати пораката преку медиумот.

Испратениот сообраќај од напаѓачот е засилен од засилувачите и вкупниот сообраќај ќе биде:

$$AI = Min\left[\frac{B_i}{M1 + M2}, \frac{NxB_p}{M1 + M2} \right] \qquad (2)$$

каде минималниот сообраќај е една од двете вредности во заградите или сообраќајот на напаѓачот помножен со бројот на засилувачки хостови. *Bi* е пропусниот опсег на засилувачкиот домен кон жртвата.

Следува дека засилувачкиот фактор на нападот - Attack Amplification Factor (AAF) е производ од пропусниот опсег на напаѓачот, бројот од

засилувачки домени Q и N бројот на хостови во засилувачки домен.

$$AAF = Q * N * B_p \quad (3)$$

IV. ПРЕВЕНЦИЈА И ПРОТИВ МЕРКИ ЗА ЗАШТИТА НА БЕЗЖИЧНИТЕ МРЕЖИ

Постојат неколку основни чекори кои треба да се направат за да се заштити домашната мрежа од несакани натрапници кои сакаат да користат Интернет или да украдат приватни информации:

1. **Промена на стандардната лозинки** - Повеќето мрежни уреди, вклучувајќи ги и безжичните пристапни точки, се претходно конфигурирани со стандардни администраторски лозинки да се поедностави почетната конфигурациија. Овие стандарди лозинки лесно се наоѓаат на Интернет, па затоа заштитата која тие ја даваат не е на задоволително ниво,
2. **Ограничување на пристапот** – Дозвола за пристап само на овластени корисници до мрежата. Секое парче на хардвер поврзан на мрежа има MAC адреса. Може да се ограничи или дозволи пристап до мрежата со филтрирање на MAC адреси,
3. **Заштита на SSID** - За да се избегне лесен пристап до мрежата,
4. **Инсталирање firewall** - Покрај firewall на оперативните системи добра пракса за безбедност е да се инсталира firewall на мрежните уреди,
5. **Криптирање на податоците на мрежата** – WEP, WPA, WPA2 и добра лозинка со голем број на карактери и специјални симболи,
6. **Анти-вирусен софтвер** - Може да се намали штетата која напаѓачите можат да ја нанесат на мрежата со инсталирање на анти-вирусен софтвер и одржување на тековни вирусни дефиниции. Многу од овие програми, исто така, имаат дополнителни опции кои можат да заштитат и откријат spyware и тројански коњи.

Администраторите на корпоративните мрежи треба да вршат проценка на ризиците, тестирање и проценка на системот за безбедносни контроли на безжични мрежи почесто отколку кај другите мрежи и системи. Чекори кои можат да се превземат за подобрување на управувањето на безжични мрежи вклучуваат:

1. Одржување и целосно разбирање за топологијата на безжичната мрежа,
2. Етикетирање и попис на безжичните и преносните уреди кои се користат,
3. Често правење на backup на податоци,
4. Периодични безбедносни тестирања и оцена на безжичната мрежа,
5. Изведување на тековни, случајно избрани безбедносни ревизии за контрола и следење на безжичните и преносните уреди.
6. Применување закрпи (patches) и безбедносни подобрувања,
7. Следење на безжичната индустрија за измени на стандардите кои ги подобруваат безбедносните карактеристики и за појава на нови производи,
8. Следење на безжичната технологија за нови закани и слабости.

Треба редовно да се спроведуваат тестови за да се утврди колку сигналот се шири надвор од објектот, а потоа да се приспособи предавателната моќ на антените, односно да се намали до точка каде ќе биде лесно да се лоцира хакер. Антените на AP треба да бидат насочени кон внатрешноста на објектот.

Постојат и комерцијални уреди, како што е AirDefense на Моторола [16], кои се користат како системи за превенција од упади.

Превенција од ефектите на Smurf нападот

Како примарна против мерка за заштита од Smurf напад е да се исклучи “ip directed-broadcast” на рутерот, која и не е баш добра идеја кај оние корисници кои како traceroute користат алатки за дијагностицирање.

Конфигурирање на access листи и firewall-и целосно да го отфрлаат сиот ICMP сообраќај, има негативни последици како отфрлање на ICMP Router Discovery [17], со која хост може да ги открие активните рутери во мрежата.

Слика 6. Блокирање на целиот ICMP сообраќај

Богданоски и Ристески во својот труд [18] разгледуваа однесување на CS PIX 525 8ae adv (CISCO), CKP Window Firewall 4e adv и CKP Unix Firewall 4e adv при ICMP. Cisco firewall-от даде најдобри резултати при справување со овие напади. Меѓу останатите решенија предложена нивна страна, значително подобрени резултати се постигнати со употреба на специјално дизајниран и подесен Failure Recovery механизам.

Power Tech Information Systems во Норвешка хостираат SMURF Amplifier Registry (SAR) [19], која ги регистрира сите познати SMURF

засилувачи и се update-ира на секои пет минути. SAR дозволува да се тестираат сите Интернет поврзани IP мрежи дали се конфигурирани за да користат како SMURF засилувачи. Информацијата може да се искористи за да се блокира сообраќајот од и кон тие мрежи.

Udhayan и Anitha во својот труд [20] предлагаат рестрикциска шема за ICMP со која ќе се намали продуктивноста на нападот и ќе се обезбеди доволно пропусен опсег за ICMP апликациите и ефективно користење на ICMP сообраќајот.

Deal во својата книга [21], препорачува користење на committed access rate (CAR) за ограничување на брзината кон Интернет провајдерот, но и во обратната насока. Со ова се дозволува ICMP со одредена големина и плус додатен burst, а сиот сообраќај над таа големина се отфрла. Командите изгледаат вака:

- ISP (config) # access-list 100 permit icmp any any echo
- ISP (config) # access-list 100 permit icmp any any echo-reply
- ISP (config) # interface serial0
- ISP (config) # rate-limit output access-group 100 64000 4000 4000 conform-action transmit exceed-action drop

Ако сите мерки за претпазливост не успеат и ако се соочуваме со DoS напад, прво треба да пробаме да ги исклучиме непотребните услуги, а ако тоа не е доволно да се изгаси мрежата/серверот додека не помине нападот.

V. ЗАКЛУЧОК

Со развитокот и ширењето на Интернет, знаењето стана глобално достапно и бесплатно, а со него и open source софтверот, пиратеријата и Cyber криминалот. Достапни се секакви туторијали и книги на различни теми и со мало познавање од компјутерската област и со обичен лаптоп, паметен телефон или таблет, било кој човек може да изведе DoS напад. Овие напади се лесни за изведување и може да предизвикаат катастрофални последици врз безжичните мрежи, од деградирање на квалитетот на услуги, до нивно целосно губење и загуба на доверливи податоци. Експертите воведуваат нови техники и технологии за поправка на недостатоците, но напаѓачите се секогаш чекор понапред.

Библиографија

[1] Scott Flusher, Itsik Mantin and Adi Shamir, Weakness in the Key Scheduling Algoritm of RC4, *Lecture Notes in Computer Science*, 2259, 2001.

[2] Nikita Borisov, Ian Goldberg and David Wagner, Intercepting Mobile Communications: The Insecurity of 802.11, In *Seventh International Conference on Mobile Compating And Networking*, Rome Italy, July 2001.

[3] W.A.Arbaugh, N.Shankar, J.Wang and K.Zhang. Your 802.11 Network Has No Clothes, In *First IEEE International Conference on Wireless LANs and Home Networks*, Suntec City, Singapore, December 2001.

[4] CNN.com, The denial of service aftermath (Feb 2000), www.cnn.com/2000/TECH/computing/02/14/dos.aftermath.idg/index.html.

[5] Philip Preville, The Montreal Mirror Online Archive. *On the trail of Mafiaboy*, (Jun 2000), www.montrealmirror.com/ARCHIVES/2000/022400/news1.html.

[6] www.associatedcontent.com/article/6071498/wikileaks_site_taken_down_in_denial.html.

[7] Md Sohail Ahmad, *Hole 196*, Black Hat Arsenal, August 2010, Las Vegas.

[8] KoreK chopchop, www.aircrack-ng.org/doku.php?id=korek_chopchop.

[9] Martin Beck, Erik Tews, *Practical attacks against WEP and WPA*, November 8, 2008.

[10] Guillaume Lehembre, *Wi-Fi security – WEP, WPA and WPA2*.

[11] Robert R. Collins, *The Pentium f00f Bug* (Mart 1995) www.rcollins.org/ddj/May98/F00FBug.html.

[12] Purdue University, Christoph Scuba, *Addressing weaknesses in the DNS protocol* (Aug 1993).

[13] www.networksorcery.com/enp/protocol/icmp/msg10.htm.

[14] http://news.cnet.com/Smurf-attack-hits Minnesota/2100-1001_3-209209.html.

[15] Sanjeev Kumar, Senior Member at IEEE Network Research Lab, *Smurf-based Distributed Denial of Services (DDoS) Attack Amplification in Internet.*

[16] www.motorola.com/web/Business/_Independent%20Pages/_Documents/_StaticFiles/MOT_AD_WP_US-EN.pdf.

[17] Check Point Software Technologies Ltd, SmartDefense Tech, www.smenig.com/resources/white_paper/Security/smart_def_tech_note_2004.pdf.

[18] Mitko Bogdanoski, Aleksandar Risteski, *Wireless Network Behavior under ICMP Ping Flood DoS Attack and Mitigation Techniques*, International Journal of Communication Networks and Information Security (IJCNIS) April 2011.

[19] PowerTech Information Systems, *Smurf Amplifier Registry (SAR)* (July 2003), www.powertech.no/smurf/.

[20] J.Udhayan, R.Anitha, "Demistifying and Rate Limiting ICMP hosted DoS/DDoS Flooding Attacks with Attack Productivity Analysis" *IEEE International Advance Computing Conference (IACC 2009)*, Patiala, India, 6-7 March 2009.

[21] Richard Deal, *Cisco Router Firewall Security*, Published by Cisco Press, Aug 10, 2004

- -

Summary

Methods for Mitigating the Effect of the ICMP Smurf Attack on Wireless Networks

Aleksandar Toshevski, Mitko Bogdanoski

European University – Skopje, R. Macedonia, toshevski.aleksandar@live.eurm.edu.mk
European University – Skopje, R. Macedonia, mitko.bogdanoski@ eurm.edu.mk

***Abstract* – 802.11 or popular called Wi-Fi networks currently are at the pick of their evolution and popularity. They are relatively inexpensive because of easy implemention, no neediness for cabling, and flexibility and great reach. Therefore, they are broadly are used by internet providers, companies, institutions and home users. They are easy to implement because there is only need for an access point or base station and user stations with wireless cards witch allows their wireless connection. After authentication the mobile users can move through the covered area without signal or connection losses. The bad side of these networks is that they have unclear boundaries so an attacker can collect packages that traverse the network. This paper in the first section describes some of the major vulnerable points of wireless networks, and in the second part details for the ICMP Smurf DoS attack, and methods for preventing and reducing the effects of these attacks are presented.**

***Keywords* – ICMP Smurf attack, vulnerabilities, wireless networks, security.**