BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 2, Number 354 (2015), 50 – 54

MODELS AND METHODS OF EFFICIENCY INCREASE OF DETECTION AND LOCALIZATION OF THE DISTRIBUTED OF NETWORK ATTACKS

G. A. Shangytbayeva[1], Z. Zhumagalieva[2], N. K. Shangytbayev[3]

[1] Kazakh National Technical University named after K. I. Satpayev, Almaty, Kazakhstan;
[2] K. Zhubanov Aktobe Regional State University, Kazakhstan;
[3] Polytechnic College of Aktobe, Kazakhstan.
E-mail: gul_janet@mail.ru; zanar82@mail.ru; nurzhan90@mail.ru

Keywords: information security, computer networks, the network and distributed attacks, attacks of Denial–of– service.

Abstract. The paper presents a method to improve the detection and localization of distributed network attacks. The description of the main network attacks such as "Denial of Service" is given. the algorithm of operation of malefactors with attacks of this type is given. In the article the method for detection of the distributed network attacks is offered. The valuation method of probability of loss of arbitrary request in case of its passing on networks of mass service. The offered method increases productivity of use of the calculated resource of a computer network for big distributed network attacks by a failure in service. Use of the received results allows to raise the network security level.

УДК 004.75: 004.43.5

БӨЛІСТІ ЖЕЛІЛІК ШАБУЫЛДАРДЫ АНЫҚТАУ ЖӘНЕ ШЕКТЕУ ТИІМДІЛІКТЕРІН ЖОҒАРЫЛАТУ ӘДІСТЕРІ

Г. А. Шаңғытбаева[1], Ж. Жұмағалиева[2], Н. К. Шаңғытбаев[3]

[1] Қ.И. Сәтпаев атындағы Қазақ ұлттық техникалық университеті, Алматы, Қазақстан;
[2] Қ. Жұбанов атындағы Ақтөбе өңірлік мемлекеттік университеті, Қазақстан;
[3] Ақтөбе политехникалық колледжі, Қазақстан

Тірек сөздер: ақпараттық қауіпсіздік, компьютерлік желілер, желілік және бөлістік шабуылдар, "қызмет көрсетуден бас тарту" шабуылдары.

Аннотация. Мақалада бөлісті желілік шабуылдарды анықтау және шектеу тиімділіктерін жоғарылату әдістері берілген. Негізгі желілік шабуылдардың, соның ішінде "қызмет көрсетуден бас тарту" бөлістік желілік шабуылының сипаттамалары беріледі. Осы текті шабуылдар жұмысының алгоритмі келтірілген. Мақалада бөлісті желілік шабуылдарды анықтау әдісінің тиімді жолдары қарастырылған. Бұл мақалада ұсынылып отырған әдіс өте үлкен көлемдегі "қызмет көрсетуден бас тарту" бөлістік желілік шабуылдар кезінде компьютерлік желілердегі есептелінетін ресурстарды пайдалану тиімділігін арттырады. Беріліп отырған әдіс компьютерлік желілердегі желілік шабуылдардан қорғаныстық күшейтеді. Сондай-ақ, интернет желілеріндегі қорларды пайдалана алу өнімділігін жоғарылатады. Ғылыми жұмыста қарастырылған шешімдердің нәтижелерін желілердегі қауіпсіздік деңгейін жоғарылату мақсатында қолдануға болады.

Кіріспе. Егер де сіз компьютерлік технологиялар негізінде немесе желілік қауіпсіздік саласында жұмыс істейтін болсаңыз, онда сізге, міндетті түрде, қазіргі таңда «DoS шабуылы» деген атқа ие "қызмет көрсетуден бас тарту" термині таныс болар. Қазіргі кезде ол интернет желісінде өте кең тараған желілік шабуылдар түріне жатады.

"Қызмет көрсетуден бас тарту" немесе «DoS шабуылы» – интернеттегі желілік машиналарды қажеті жоқ, өте көп мөлшердегі интернет трафиктермен толтырып жіберетін, желілерге зиянын тигізуге арналған желілік шабуылдардың бір түрі. Оның әсерінен көптеген желілік машиналар қайта-қайта жүктеліп, зардап шегеді, тіптен, қолданыстан да шығып қалады.

DoS шабуылдарының негізгі мақсаты – желідегі негізгі машинаның қызметтерін (мысалы, web сайттар, DNS сервері т.б.) белгілі бір пайдаланушылар үшін уақытша тоқтата тұру.

Ал, DoS шабуылдары өте қажетті қызметтер, мысалы, банктік қызмет көрсету, электронды коммерция, жеке деректерді өңдеу, несиелік карталар, басқа да қызметтер атқара алатын web–серверлерде жүзеге асады.

DoS шабуылдарының ең көп тараған түрі соңғы кездері кеңінен таныла бастаған DDoS (Distributed Denial of Service – распределенный отказ в обслуживании, қызмет көрсетуден бас тарту) шабуылы болып табылады. Ол әрі қуатты, әрі күрделі шабуыл болып табылады.

DoS шабуылының бір ғана шығыс орны болады, ал DDoS бернеше бөлістік желілер арқылы жайылатын көптеген IP – мекен-жайдан таралады [1].

DoS және DDoS шабуылдары. DDoS – бұл ағылшын тілінен Distributed Denial of Service сөз тіркесінен қысқартылып алынған, қазақ тіліне аударғанда "Бөлістік қызмет көрсетуден бас тарту" деген мағынаны білдіреді. Яғни, ол дегеніміз – көптеген бөлістік (әртүрлі интернет– қосылыс нүктелерінен шығатын) сұраныстардың әсерінен желілік ресурстар қызметтерінен бас тарту деган сөз. DoS– шабуылдарынан (Denial of Service – «Отказ от обслуживания», "Қызмет көрсетуден бас тарту") DDoS – шабуылының айырмашылығы бұл жағдайда қайта жүктелу қандай да нақты бір интернет– түйіндеріндегі сұраныстар нәтижесінде орын алады.

Егер DDos– шабуылдары өте қиын да күрделі болатын болса, онда кез келген ресурстың – кішігірім ақпараттық сайттардан бастап өте ірі интернет–дүкендеріне дейін немесе пошталық серверлерге дейін жұмыстан шығып қалу қаупі басым болады. Шабуыл кезінде сайт–серверде қолданушылардан миллиондаған сұраныстарға дейін келіп түседі, соның салдарынан желі серверінде келеңсіз жағдайлар орын алып, қайта жүктеліп, істен шығуға дейін алып келеді. Сан мыңдаған келіп түскен сұраныстарды өңдеп үлгере алмайды, соның әсерінен желі серверінің жылдамдығы төмендеп, кейіннен жұмысын мүлдем тоқтатады. Сол себептен де желі серверінің жұмысы күрделеніп, қиындап кетеді [2].

DDoS шабуылы қазіргі кезде өте кең таралған және өте қауіпті желілік шабуылдардың бірі болып саналатын, желілік шабуылдың "Қызмет көрсетуден бас тарту" түріне жататын бөлістік шабуыл болып табылады. Оның нәтижесінде жоғарыда айтып өтілгендей, заңды қалданушылардың, желілер мен жүйелердің, басқа да ресурстардың қызметтері бұзылады немесе толық бұғатталады.

DdoS шабуылдарының басым көпшілігі негізгі базалық Internet (TCP/IP) хаттаманы қолданады, атап айтсақ, SYN сұранысты жүйені өңдеу әдісін пайдаланады.

Қызмет көрсетуден бас тартуға әкелетін негізгі екі түрлі шабуылды бөліп қарауға болады.

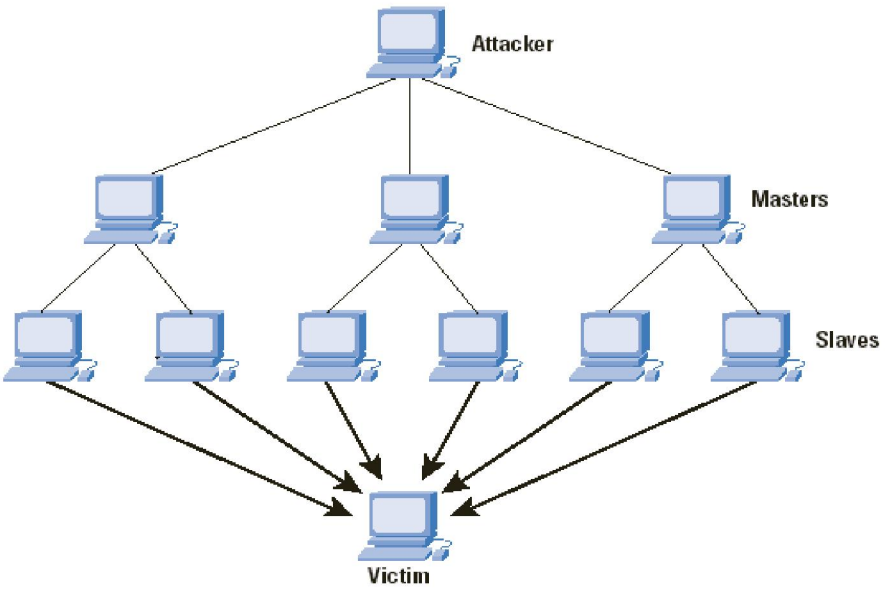
Бірінші түрге жататын шабуыл нәтижесінде барлық жүйенің немесе желінің жұмысы тоқтатылады. Бұл жағдайда хакер жүйеге күтпеген жерден деректерді жібереді, оның әсерінен жүйе қайта жүктеледі немесе істен шығады.

DDoS шабуылдардың екінші түрі өңдеу мүмкін болмайтын өте көп мөлшердегі ақпараттардың әсерінен жүйе немесе жергілікті желі шамадан тыс толып қалады.

DDoS шабуыл кезінде сайтқа деректер әлемнің әр бөліктерінде орналасқан көптеген компьютерлерден үздіксіз келіп түседі. Көптеген жағдайларда бұл компьютерлер алаяқтарды бір жүйеге біріктіретін және бір орталықтан басқаруға мүмкіндік беретін вираустар жұқтырған болып табылады. Мұндай жүйеге кіретін компьютерлер DDoS шабуылдарына өз үлестерін қосып, спамдарды таратады [3].

DDoS шабуылдарының жұмыс жасау қызметтері төмендегі диаграммада берілген (1-сурет).

DoS шабуылында мақсатын жүзеге асыруда, яғни, шабуыл кезінде зиянкес тек бір ғана компьютерді немесе желіні қолданса, ал әдетте, әртүрлі желілерге тиесілі көптеген желілер мен серверлерден шығады. Осылайшы DDoS шабуылы кезінде зиянкес әр алуан желілердің, тіпті, өзге елдердің компьютерлері мен серверлерін пайдаланады. Оны анақтау қиын болғандықтан, алғашында қауіпсіздік қызметтерінің арасында күдік туғыза қоймайды.

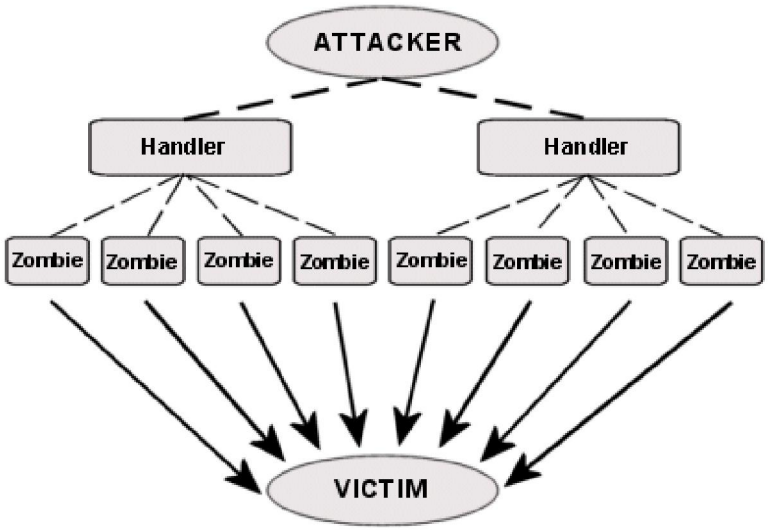


1-сурет – DDoS бөлістік желілік шабуылы

“Қызмет көрсетуден бас тарту” бөлістік шабуылы тұтас желіні немесе жүйені қайта жүктеуге алып келеді. Бұл шабуылдың негізгі мақсаты шабуыл үшін түрлі көздерді (демоны) және басқару кезінде «иелерді» пайдалану болып табылады [4].

DDoS (бөлістік қызмет көрсетуден бас тарту) шабуылын ұйымдастыруда қолданылатын ең көп танымал утилиттерге Tribal Flood Network (TFN), TFN2K, Trinoo және Stacheldraht утилиттері жатады.

Төменде беріліп отырған 2-суретте DDoS шабуылын ұйымдастыру мысалы көрсетілген.



2-сурет – “Қызмет көрсетуден бас тарту” бөлістік желілік шабуылы

Зиянкес шабуыл көздерін басқару үшін «Иелерді» (masters) пайдаланады. TCP қосылу үшін «Иелерді» қолдану оларды баптау және шабуылға дайындау кезінде қажет. «Иелер» тек қана UDP хаттамасы арқылы шабуыл көздеріне командаларды жібереді. «Иелерсіз» зиянкес шабуылдың әрбір көзімен өзі жеке-жеке байланыс жасап отырар еді. Мұндай жағдайда, шабуыл көзін тауып алу оңай болар еді және оны жүзеге асыру үшін өте көп уақыт қажет болар еді.

Шабуылдың әрбір көзі «Иесімен» арнайы хабарламалар арқылы байланысып отырады. Қолданылатын утилиттерге байланысты байланыс қуаттау (авторизации) немесе шифрлеу механизмдері

арқылы жүзеге асып отырады. Шабуыл көзі мен «Иесін» орнату үшін зиянкес белгілі күдіктікті (мысалы, буферді келесі қызметтермен – RPC, FTP т.б. толтыру) пайдаланады. Шабуылдың өзі Smurf немесе SYN–тасқыны болып табылады және негізгі желінің немесе жүйенің қызметінен бас тартуға әкеледі [5].

Қызмет көрсетуден бас тарту бөлістік желілік шабуылын анықтау әдісі. Қазіргі заманғы компьютерлік желілерді құру кезінде сенімділігі мен қолжетімділікке арналған желілік есептеу ресурстарын есепке алу қажет. b – бағдарлағыш (маршрутизатор, Router) хабарламаларын таңбалауға арналған IP– тақырыбындағы биттер саны болсын. Мысалы, b = 25 [2-4].

Желідегі шабуылдарда әрбір X бағдарлағыштан V қолданушыға M_X хабарламаны жеткізу алгоритмі кездейсоқ сілтеме әдісіне негізделген. Бұл әдістің негізі M_X үшін келесі түрлендірулерді қолдану болып табылады:

– M_X-тің мәні мынадай болуы тиіс, $|M_X|$ l-ге еселі болуы керек.

– M_X тізбегінде өте үлкен (және статистикалық кездейсоқ) C = C(M_X) бақылау қосындысын есептеу керек. Негізгі мақсат C(M_X) бақылау қосындысы кездейсоқ немесе статикалық кездейсоқ (мысалы, кездейсоқ хэш функция) және бастамашы шабуылдарға төзімді бола білуі тиіс.

– M_X тізбегін W бір бірімен қиылыспайтын M_0, M_1, M_2,..., M_{l-1} сөздер бөліктеріне бөлу.

– b_i = [i, C, M_i] болатындай b битті қайта жазуда қолданылатын блоктар жиынтығын құру.

Осылайша блок индекстен, бақылау қосындысынан және і хабарлама үзіндісінен тұрады.

b_i блогы M_X хабарламаны V қолданушыға жеткізу үшін қолданылады, бірақ, олар еркін реттілікпен берілмейді. Мысалы, M_X хабарламасы үшін C = C (M_X) M_X-тің ассоциативті мекен–жайы ретінде және M_X-тің барлық бөліктерінің сілтемесіне арналған бақылау қосындысы ретінде қолданылады. C-ның мәні статистикалық кездейсоқ және бастамашы шабуылдарға төзімді болады, сол себепті де хабарламаны қалпына келтіру алгоритмі үшін қолданылады.

Хабарламаны қалпына келтіру алгоритмі өте қарапайым, сондықтан C мәнімен бірдей болатын b_i блоктар жиыны үшін қолданушы бірге хабарлама блоктарының тізбегі дұрыс болатындай етіп, C бақылау қосындысын қолдана отырып, еркін реттілікпен b_i блоктар құрады.

V қолданушы дұрыс реттілікпен құрылған b_i нақты тізбегіне ие болған кезде ғана M_X хабарламасын қалпына келтіре алады.

Егер бағдарлағышты таңбалауға арналған IP–тақырыпты кейбір биттерді қайтадан қолданатын болса, онда сәйкесінше IP–тақырыбындағы b бірнеше битті төмендегідей тәсілмен бөлуге болады:

– і индекс үзіндісіне арналған [log l] биттер;

– ассоциативті мекен– жай және бақылау қосындысы болып есептелетін C бақылау қосындысына арналған бит;

– M_i сөздерға арналған h = b – c – [log l] бит.

C(M_X) немесе M_X функциясы кездейсоқ болсын, онда C(M_X) бақылау қосындысының мәні статистикалық кездейсоқ және шабуыл бастамашысы үшін күтілмеген жағдай. Бірақ, хэш–функция бастапқы өлшеммен сәйкес әрі екі әртүрлі хабарламалы M_X және M_y бағдарлағыштарына арналған C(M_X) = C(M_Y) үшін кездейсоқ болады. Атап айтқанда, C(M_X) барлық M_X хабарламасын біле бермейтін, тек X мәнін ғана білетін бастамашы үшін болжанбайтын болуы тиіс. M_X-тің мәні l-ге еселі болуы керек, сол кезде ғана M_X үшін C = C(M_X) бақылау қосынды c– битті есептеуге болады және M_X мәнін әрбірі h бит биіктікті l– ден M_0, M_1, M_2,..., M_{l-1} сөздер W тізбегіне бөлуге болады. L блоктан b_i = [i, C, M_i] болатындай b_0, b_1, …, b_{l-1} жиынтығын анықтаймыз, мұнда C бақылау қосындысы әрбір b_i блогына кіреді. C– ның мәні b_i блогын бірге байланыстырады және блоктар үшін ассоциативті мекен– жайы болып табылады [6–8].

Осылайша, кездейсоқ сілтемелер тәсілі өлшемі үлкен тізбекті хабарламаның бақылау қосындысын пайдаланады. Бұл әдісте M_X хабарлама үзіндісі C бақылау қосындысы тізбегі ассоциативті мекен-жайы және берілген хабарлама деректерінің бүтіндігі ретінде қолданыла алатындай етіп құрылады.

Қорытынды. Мақалада қарастырылып отырған мұндай әдіс желілік шабуылдарда бағдарлағыш (маршрутизатор, router) саны 500 болған жағдайда қолданушылар хабарламаларын қалпына келтіруге арналған ең тиімді де жедел тәсілі болып табылады. Сондықтан, мұндай кездейсоқ сілтеме әдісін қолдану қысқа уақыт кезеңінде хабарламаларды қалпына келтіруге және желілік шабуылдардың үлкен көлемінде шабуылдарын көздерін анықтауға мүмкіндік береді. Олай болса,

ғылыми мақалада ұсынылып отырған тәсіл компьютерлік желілердегі өте үлкен "қызмет көрсетуден бас тарту" бөлістік шабуылдарда компьютерлік ресурстарды пайдалану тиімділігін арттыратыны сөзсіз.

ӘДЕБИЕТ

[1] Халиль Х.А. Алгоритмы маршрутизации в мобильных сетях // Горная электромеханика и автоматика: наук.-техн. – 2002. – С. 94-100.

[2] Dean D. An algebraic approach to IP traceback. // In Network and Distributed System Security Symposium (NDSS). – 2001. – P. 3–12.

[3] Apiecionek Ł., Czerniak J.M., Dobrosielski W.T. Quality of services method as a DDoS protection tool // Advances in Intelligent Systems and Computing. 2015. 323. – P. 225-234.

[4] Goodrich M.T. Efficient packet marking for large- scale IP traceback // In 9th ACM Conf. on Computer and Communications Security (CCS). – 2002. – P. 117-126.

[5] Goodrich M.T., Tamassia R., Schwerin A. Implementation of an authenticated dictionary with skip lists and commutative hashing // In Proc. 2001 DARPA Information Survivability Conference and Exposition. – 2001. – Vol. 2. – P. 68-82.

[6] Özçelik I., Brooks R.R. Deceiving entropy based DoS detection // Computers and Security, 48, – 2014. – P. 234-245.

[7] Vijayalakshmi M., Nithya N., Mercy Shalinie S. A novel algorithm on IP traceback to find the real source of spoofed IP packets // Advances in Intelligent Systems and Computing, 325. – 2015. – P. 79-87.

[8] URL:http://arduinokit.ru/computers/administration– of– computers/chto– takoe– otkaz– v– obsluzhivanii– dos– ddos.html

REFERENCES

[1] Khalil A. *Routing algorithms in mobile networks.* Mining Electrical and Automation: nauk.– tehn. **2002,** pp 94-100. (in Russ.).

[2] Dean D. *An algebraic approach to IP traceback.* In Network and Distributed System Security Symposium (NDSS). **2001,** pp. 3-12. (in Eng.).

[3] Apiecionek Ł., Czerniak J.M., Dobrosielski W.T. Quality of services method as a DDoS protection tool. Advances in Intelligent Systems and Computing, 323, **2015,** pp. 225–234. (in Eng.).

[4] Goodrich M. T. *Efficient packet marking for large– scale IP traceback.* In 9th ACM Conf. on Computer and Communications Security (CCS). **2002,** pp. 117–126. (in Eng.).

[5] Goodrich M. T. *Implementation of an authenticated dictionary with skip lists and commutative hashing.* In Proc. 2001 DARPA Information Survivability Conference and Exposition. **2001,** Vol. 2, pp. 68–82. (in Eng.).

[6] Özçelik I., Brooks R.R. *Deceiving entropy based DoS detection.* Computers and Security, 48, **2014**, pp. 234–245. (in Eng.).

[7] Vijayalakshmi M., Nithya N., Mercy Shalinie S. *A novel algorithm on IP traceback to find the real source of spoofed IP packets.* Advances in Intelligent Systems and Computing, 325, 2015. pp. 79–87. (in Eng.).

[8] URL:http://arduinokit.ru/computers/administration– of– computers/chto– takoe– otkaz– v– obsluzhivanii– dos– ddos.html, (in Russ.).

МЕТОДЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ВЫЯВЛЕНИЯ И ЛОКАЛИЗАЦИИ РАСПРЕДЕЛЕННЫХ СЕТЕВЫХ АТАК

Г. А. Шангытбаева[1], Ж. Жумагалиева[2], Н. К. Шангитбаев[3]

[1] Казахский национальный технический университет им. К. И. Сатпаева, Алматы, Казахстан;
[2] Актюбинский региональный государственный университет им. К. Жубанова, Казахстан;
[3] Актюбинский политехнический колледж, Қазақстан

Ключевые слова: информационная безопасность, компьютерные сети, сетевые и распределенные атаки, атаки на отказ в обслуживании.

Аннотация. В статье приведен методы повышения эффективности выявления и локализации распределенных сетевых атак. Дано описание основных сетевых атак типа «отказ в обслуживании». Приведен алгоритм работы злоумышленников с атаками данного типа. В статье предложен метод для обнаружения распределенных сетевых атак. Метод оценки вероятности потери произвольной заявки при ее прохождении по сетям массового обслуживания. Предложенный метод увеличивает продуктивность использования вычисляемого ресурса компьютерной сети при больших распределенных сетевых атаках на отказ в обслуживании. Использование полученных результатов позволяет повысить уровень безопасности сети.

Поступила 26.02.2015 г.