Організаційні засоби захисту являють собою організаційно-технічні й організаційно-правові заходи, які здійснюються в процесі створення й експлуатації обчислювальної техніки, апаратури телекомунікацій для забезпечення захисту інформації. Організаційні заходи охоплюють всі структурні елементи апаратури на всіх етапах їх життєвого циклу.

Морально-етичні засоби захисту реалізуються у вигляді всіляких норм, які склалися традиційно або складаються в міру поширення обчислювальної техніки й засобів зв'язку в суспільстві. Ці норми здебільшого не є обов'язковими як законодавчі заходи.

Законодавчі засоби захисту визначаються законодавчими актами, якими регламентуються правила користування, обробки й передачі інформації обмеженого доступу й встановлюються заходи відповідальності за порушення цих правил.

Захист інформації в системі обробки інформації повинен ґрунтуватися на наступних основних принципах: 1) системності; 2) комплексності; 3) безперервності захисту; 4) розумної достатності; 5) гнучкості керування й застосування; 6) відкритості алгоритмів і механізмів захисту; 7) простоти застосування захисних заходів і засобів.

Системний підхід до захисту комп'ютерних систем припускає необхідність обліку всіх взаємозалежних, взаємодіючих і мінливих у часі елементів, умов і факторів, суттєво значимих для розуміння й вирішення проблеми забезпечення безпеки. При створенні системи захисту необхідно враховувати всі слабкі, найбільш уразливі місця системи обробки інформації, а також характер, можливі об'єкти й напрямки атак на систему з боку порушників, шляхи проникнення в розподілені системи й несанкціонованого доступу до інформації. Система захисту повинна будуватися з урахуванням не тільки всіх відомих каналів проникнення й несанкціонованого доступу до інформації, але й з урахуванням можливості появи принципово нових шляхів реалізації загроз безпеки.

Надійшла до редколегії 30.08.2011

Зыбин С.В.

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАНОГО ДОСТУПА В СИСТЕМАХ ОБРАБОТКИ ИНФОРМАЦИИ

В статье рассматриваются вопросы защищенности систем обработки информации

Zybin S.V.

PRIV FROM NESANKCIONIROVANOGO ACCESS IN THE SYSTEMS OF TREATMENT OF INFORMATION

The questions of protected of the systems of treatment of information are examined in the article

УДК 681.51:519.876

Яциковська У.О.[1] , Карпінський М.П. [2]

[1]*Тернопільський національний технічний університет імені Івана Пулюя*
[2]*Університет в Бєльську-Бялій і Державна вища професійна школа в Новому Сончі, Польща*

МОДЕЛЮВАННЯ МЕРЕЖНОГО ТРАФІКУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІД ЧАС РЕАЛІЗАЦІЇ АТАК ТИПУ DOS/DDOS

Удосконалено математичну модель мережного трафіка, що дозволяє на практиці виявляти атаки типу DoS/DDoS. Обґрунтовано спосіб запобігання атакам на основі використання процедури реконфігурації мережі, це утруднює практичну реалізацію атаки типу DoS/DDoS. Запропоновано алгоритм створення нових віртуальних каналів передачі даних для забезпечення мінімального обсягу трафіка незалежно від реконфігурації комп'ютерної мережі.

Ключові слова: комп'ютерна мережа, трафік, маршрутизація, атаки типу DoS/DDoS.

Вступ

Широке використання комп'ютерних мереж створює умови для реалізації атак, що використовують стандартні алгоритми маршрутизації. Відомо, що протокол маршрутизації в передачі даних це набір правил та домовленостей стосовно обміну мережевою інформацією між маршрутизаторами для визначення маршруту передачі даних, який задовольняє заданим параметрам якості обслуговування та забезпечує збалансоване навантаження усієї комп'ютерної мережі в цілому, тому задача дослідження мережного трафіку набуває особливої актуальності. Питанням організації та побудови комп'ютерних мереж, в тому числі і питанням маршрутизації, присвячені роботи вчених М.Ю.Ільченко, С.Г. Буніна, О.С. Петрова та роботи зарубіжних вчених Д. Девіса, Д. Барбера, У. Прайса, В. Вілінгера, Д. Вільсона, Д. Рахсона та ін. [1].

Для реалізації атак типу DoS/DDoS у сучасних комп'ютерних мережах характерна багаторівнева маршрутизація, при якій комп'ютерна мережа певним чином розбивається на підмережі, що працюють за стандартними протоколами. Більшість реалізацій атак типу DoS/DDoS розраховані на мережі з однорідною структурою або на мережі з фіксованою структурою доменів. Часта зміна компонентів комп'ютерної мережі призводить до зміни її топології, складу і кількості доменів маршрутизації, що впливає на ефективність процедури маршрутизації, та сприяє роботі алгоритмів типу DoS/DDoS. Тому виникає необхідність у розробці нових методів захисту комп'ютерної мережі від зазначених, що забезпечить передачу інформації із заданими параметрами якості обслуговування при мінімальному обсязі трафіка шляхом розробки методу захисту трафіку від надлишкової інформації на основі визначення критерію пропускної здатності мережі та обчислювальних ресурсів [2].

Аналіз практичної реалізації атаки у глобальній мережі дозволяє визначити механізми захисту інформації в комп'ютерних мережах на основі використання алгоритмів типу DoS/DDoS. Для усунення причин атак на інфраструктуру і базові протоколи мережі доцільно змінити конфігурацію комп'ютерної системи. На першому етапі дослідження необхідно проаналізувати мережевий трафік для запобігання несанкціонованого зчитування з фізичного каналу передачі даних, це дозволить уникнути перехоплення витоку інформації. Цю задачу можна успішно розглядати шляхом створення віртуальних мереж, алгоритмів тунелювання, ідентифікації, аутентифікації [3].

Основна частина

На практиці більша половина з'єднань суб'єктів глобальної мережі використовує віртуальні з'єднання, оскільки цей метод є динамічним захистом мережного з'єднання і не передбачає використання статичної ключової інформації. Тому взаємодія без встановлення віртуального каналу є однією з можливих причин успіху віддалених атак типу DoS/DDoS.

Небезпека більшості DDoS-атак полягає в тому, що на перших етапах не порушують протоколу обміну даними. Вони проявляють себе, коли обчислюваного ресурсу мережі стає недостатньо. Для запобігання таких атак достатньо правильного налаштування маршрутизатора та міжмережевого екрану.

Для спрощення реалізації DoS/DDoS алгоритмів користувачу слід дотримуватись номінальних швидкостей передачі даних, це дозволить на практиці уникати алгоритмів оптимізації мережевих трафіків, на котрих реалізуються багато атак [4].

Від атак типу flood можна ефективно відмежуватись шляхом розподілу основного каналу зв'язку на декілька віртуальних. Це дозволить створити інші мережні інтерфейси при ураженні каналу DoS/DDoS алгоритмами. Міжмережеві екрани доцільно неперервно активізувати та налаштувати так, щоб внутрішні мережеві сервіси були недоступними для зовнішнього користувача. Доцільно встановити аналізатор мережевого трафіку, значення його параметрів дозволить вчасно виявити початок атак. Перед безпосереднім початком атаки боти поступово нарощують потік пакетів на систему. Тому необхідне неперервне спостереження за маршрутизатором, під'єднаним до зовнішньої мережі [5].

Ефективність методів маршрутизації знаходиться в прямій залежності від топології мережі та її розміру. Багаторівнева маршрутизація в значній мірі залежить від оптимального розбиття комп'ютерної мережі на домени маршрутизації. Таким чином, однією з основних

задач захисту функціонування комп'ютерної мережі є трафік мережі, в основу котрих покладемо принцип мінімального обсягу мережевих даних. Задачу захисту мережевих даних зведено до задачі мінімізації параметрів передачі інформації [6]. Відомо, що при використанні відомих протоколів маршрутизації всередині домену зміна топології мережі призводить до зростання трафіку за нелінійним законом, тому реконфігурація доменів маршрутизації у процесі зміни топології мережі сприяє зменшенню обсягу трафіку та часу формування шляхів передачі даних, а також утруднює реалізацію атаки типу DoS/DDoS. На підставі удосконаленої математичної моделі визначається вибір кількості та розміру доменів маршрутизації. З метою забезпечення максимальної ефективності функціонування комп'ютерної мережі, процедура маршрутизації має враховувати зміни топології мережі. Однак більшість протоколів маршрутизації не передбачають процедури зміни структури доменів маршрутизації. У зв'язку з цим виникає необхідність розробки нової моделі маршрутизації, яка за рахунок врахування атак відмови в обслуговуванні ресурсів маршрутизації дозволить підвищити ефективність передачі інформації в комп'ютерних мережах. При цьому необхідно враховувати умови доцільності значень параметрів пропускної здатності мережі та обчислювальних ресурсів.

Доцільно визначити параметри, що регулюють обсяг пакетів, що передані по кожному каналу зв'язку окремо, і загальний обсяг пакетів, що передані за час поновлення таблиць маршрутизації. Загальний обсяг трафіка визначається такою моделлю:

$$V = \frac{T_{sys}}{\Delta t_{sys}} \sum_{i,j=1}^{N} P_i Q_j , \qquad (1)$$

де Δt_{sys} – час одного такту системи;

Q_j – обсяг інформації, переданої за один такт по кожному окремому каналу;

P_i – степінь компрометації вузла;

Tsys – час, на протязі якого при зміні топології мережі вузли розповсюджують повідомлення про поновлення маршрутів.

Дослідження показали, що протягом реалізації атаки виду DoS/DDoS збільшується кількість скомпрометованих вузлів та зростає загальний обсяг трафіка V.

Результати чисельного експерименту представленні на рис. 1.

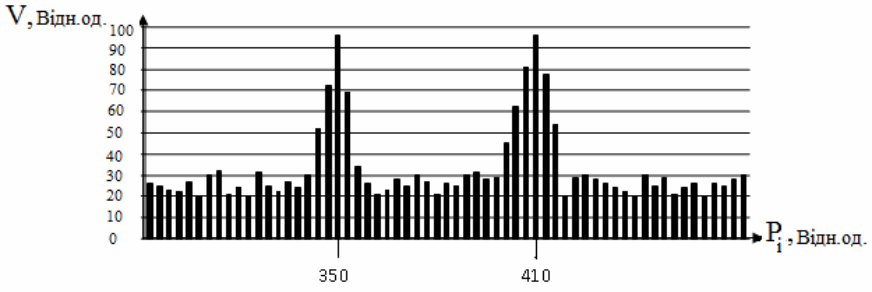

Рис. 1 Залежність обсягу трафіка від атак виду DoS/DDoS

Аналіз рисунка показує, що під час атаки стрімко збільшується обсяг трафіку у каналах мережі, більшу половину трафіку використовує алгоритм типу DoS/DDoS. Це в значній мірі уповільнює роботу мережі. Для запобігання подібних ситуацій доцільно скористатися аналізаторами трафіку, що контролюють обсяг пакетів в мережі. Також слід виконувати процедуру маршрутизації за допомогою розподіленої системи агентів маршрутизації за умови, що маршрутизація всередині домену здійснюється агентом, який входить у склад цього домену, а маршрутизація між доменами виконується на рівні взаємодії агентів марш-

рутизації. Це пояснюється тим, що обмін службовою інформацією в мережі здійснюється тими ж каналами, що і передача корисної інформації.

Для підвищення ефективності процедури маршрутизації в роботі запропоновано розділити дані по віртуальних каналах. З цією метою множина робочих станцій та віртуальних каналів між ними організовані у вигляді локальної комп'ютерної мережі. Спосіб формування та динамічної реконфігурації доменів маршрутизації дозволяє підвищити ефективність процедури маршрутизації комп'ютерної мережі [7]. Формування та динамічна реконфігурація доменів здійснюється за допомогою спеціалізованої системи маршрутизації, основними функціями якої є визначення кількості та місця розташування робочих станцій, оновлення маршрутної інформації та вибір шляху, що відповідає вимогам стійкості і мінімальної часової затримки.

Для запобігання зазначеним атакам доцільно ввести в систему додаткові детектори моніторингу трафіку мережі. Ці детектори дають вказівки виконуючим модулям у різних сегментах мережі [8]. В результаті, перед атакованим потоком утворюється екран, що відмежовує атаку від внутрішньої мережі. Маршрути обираються динамічно або статично таким чином, щоб використовувати лише фізично безпечні підмережі, вузли комутації та канали. Передавання даних, що мають мітки безпеки, через певні підмережі, вузли комутації та канали доцільно заборонити політикою безпеки.

Висновки

У статті удосконалено математичну модель загального обсягу трафіка, що дозволяє на практиці виявляти атаки типу DoS/DDoS. Використання отриманих результатів дозволяє підвищити рівень безпеки мережі за рахунок організації багаторівневих протоколів маршрутизації. Для запобігання зазначеним атакам доцільно ввести в систему додаткові детектори моніторингу трафіку мережі. Обґрунтовано спосіб запобігання атакам на основі використання процедури реконфігурації мережі, що дозволило утруднити практичну реалізацію атаки типу DoS/DDoS, шляхом створення нових віртуальних каналів передачі даних. Цей спосіб забезпечує мінімальний обсяг трафіка незалежно від реконфігурації комп'ютерної мережі.

Література

1. Колесник О. Б. Інформаційні технології та інструментальні засоби адаптивного управління мобільними безпровідними обчислювальними мережами : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.06 "Інформаційні технології" / Колесник Олексій Броніславович; Харківський нац. ун-т радіоелектроніки України. – Х., 2008. – 25 с.
2. Айрапетян Р.А. Методи захисту програмного забезпечення від несанкціонованого доступу та шкідливих програм : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.21 "Системи захисту інформації" / Айрапетян Роберт Артемович; Одеський нац. політехн. ун-т України. – О., 2009. – 18 с.
3. Жуков И. А. Распределенное управление трафиком в мобильных сетях / И. А. Жуков, И. Н. Давиденко // Електроніка та системи управління. – 2008. – № 2 (16). – С. 161–167.
4. Давиденко И. Н. Способ повышения эффективности процесса маршрутизации в мобильных сетях большой размерности / И. Н. Давиденко // Вісник Національного технічного університету України "КПІ" : Інформатика, управління та обчислювальна техніка. – 2008. – № 47. – С. 287–296.
5. Клименко И.А. Способ динамической маршрутизации с поддержкой требуемого уровня качества обслуживания в мобильных сетях без фиксированной инфраструктуры // Проблеми інформатизації та управління: Зб. наук. пр. – К.: НАУ, 2005. – Вип. 15. – С. 102–112.
6. Клименко И.А., Аль Рабабах Мохаммед Абдель-Кадер, Мухаммед Ель Амин Бабикер. Организация виртуальных каналов в мобильной сети Интернет // Вісник Національного техн. ун-ту України "КПИ": Інформатика, управління та обчислювальна техніка. – К.: ТОВ "ВЕК+", 2004. – Вип. 42. – С. 84–93.
7. Гузий Н.Н. Система защиты сетевого периметра на основе обнаружения аномалий / Н.Н. Гузий, Г.В. Данилина, Я.В. Милокум // Вісник інженерної академії України. – 2008. – Вип.3-4. – С. 61-67;

8. Клименко И.А. Способ адаптивной маршрутизации с учетом параметров качества обслуживания в мобильных сетях Ad Hoc // Тр. Наук.–практичної конф. молодих вчених та аспірантів "Інтегровані інформаційні технології та системи" (ІІТС–2005). – Київ: НАУ, 2005. – С. 78–80.

Надійшла до редколегії 21.05.2011

Яциковская У.О. , Карпинский Н.П.

МОДЕЛИРОВАНИЕ СЕТЕВОГО ТРАФИКА КОМПЬЮТЕРНОЙ СЕТИ ПРИ РЕАЛИЗАЦИИ АТАК ТИПА DOS/DDOS

Усовершенствована математическая модель общего объема трафика, что позволяет на практике выявлять атаки типа DoS/DDoS. Обосновано способ предотвращения атак на основе использования процедуры реконфигурации сети, что позволило затруднить практическую реализацию атаки типа DoS/DDoS. Предложен алгоритм создания новых виртуальных каналов передачи данных для обеспечения минимального объема трафика независимо от реконфигурации компьютерной сети.

Yatsykovska U.O. , Karpinski M.P.

MODELING NETWORK TRAFFIC OF COMPUTER NETWORK DURING THE IMPLEMENTATION ATTACKS SUCH AS DOS/DDOS

Was improved mathematical model of network traffic, allowing in practice to detect attacks such as DoS/DDoS. Grounded way to prevent attacks through the use of network reconfiguration procedures, it is difficult for practical implementation attacks such as DoS/DDoS. The algorithm to create new virtual data channels to ensure a minimum amount of traffic regardless of reconfiguring computer network.

УДК 621.391.24

Скопа О.О.

Одеський державний економічний університет

ОБЧИСЛЕННЯ АПЕРІОДИЧНОЇ АВТОКОРЕЛЯЦІЙНОЇ ФУНКЦІЇ ТА ВИЗНАЧЕННЯ КРИТЕРІЇВ ЇЇ ЯКОСТІ ПО В.П. ІПАТОВУ

Наводяться відомості щодо обчислення аперіодичних автокореляційних функцій АФМ-сигналів та визначення критеріїв їх якості.

Ключові слова: аперіодична автокореляційна функція; критерій якості; АФМ-сигнал; чіп; широкосмуговий сигнал

Постановка проблеми в загальному вигляді, зв'язок з важливими науковими і практичними завданнями. Періодична залежність є загальним типом компонент часового ряду. Можна легко побачити, що при однотипних вимірюваннях будь-яких параметрів кожне спостереження дуже схоже на сусіднє. Крім того, додатковим фактором є наявність періодичної складової, що повторюється. Це означає, що кожне спостереження схоже на спостереження, що було в той же самий час, але на попередньому періоді. Т.ч., періодична залежність може бути формально визначена як кореляційна залежність порядку k між кожним i-м та $(i-k)$-м елементом ряду. Її можна виміряти за допомогою автокореляції (тобто кореляції між самими членами ряду). Величину k зазвичай називають лагом (зрушенням, запізнюванням). Якщо помилка вимірювання не дуже велика, то періодичність можна визначити візуально, розглядаючи поведінку членів ряду через кожних k часових одиниць [1]. У літературі ступінь кореляції між членами ряду прийнято визначати за допомогою автокореляційної функції (АКФ), яка є статистичним взаємозв'язком між випадковими величинами з одного ряду, але узятих зі зрушенням, наприклад, для випадкового процесу – зі зрушенням за часом. Для такого випадку найбільш точне визначення АКФ наве-