лемме 1, $N=\left(q^3-1\right)\left(q^2-1\right)$. Раскрывая выражение (10) путем подстановки $s=\left|(2k+1/4)^{1/2}-1/2\right|$ при большом значении q получим (11).

IV Выводы

1. Кривая Ферма $X^{q^2+q+1}+Y^{q^2+q+1}+Z^{q^2+q+1}$ имеет большой род $g=\left(q^2+q\right)\left(q^2+q-1\right)/2$ и оценка (8) для ε определена для широкого диапазона практических значений k. Для $k\geq g$ справедливо выражение $\varepsilon=(k+g)/N$ для вероятности коллизии. Оценки вероятности коллизии для кривой Гурвица являются подобными. Асимптотика вероятности коллизии универсального хеширования по кривой Ферма при малых значениях k определяется отношением корня квадратного длины данных к размерности поля, в $\sqrt{k}$ лучше, по сравнению с хешированием по проективной прямой $X+Y+Z=0$ и равняется асимптотике хеширования по кривой Эрмита в квадратичном поле той же размерности F_{p^2}, $p^2=q^3$.

2. Практический алгоритм вычисления хеш кода по рациональными функциями $x=X/Z$, $y=Y/Z$ кривой Ферма определяется схемой вычисления Горнера по двум переменным $h_{x,y}(m)=\sum_{j=0}^{s} y^j\cdot\sum_{i=0}^{s-j} m_{i,j}\cdot x^i$. Сложность универсального хеширования равна $N_{опер}=k+s$, $s=\left|(2k+1/4)^{1/2}-1/2\right|$, что соответствует сложности по кривой Эрмита в квадратичном поле [3].

3. Асимптотическая оценка сложности универсального хеширования по кривой $X^{q^2+q+1}+Y^{q^2+q+1}+Z^{q^2+q+1}$ определяется $N_{опер}(FC)=k+\sqrt{2}k^{1/2}$, так как $s=\left|(2k+1/4)^{1/2}-1/2\right|$. Хеширование по кривой Ферма по сравнению с хешированием по проективной прямой сложнее на $N_{опер}(FC)-N_{опер}(PC)=\sqrt{2}k^{1/2}$ операций. Относительное увеличение сложности вычислений является несущественным $N_{опер}(FC)/N_{опер}(PC)=1+\sqrt{2}k^{-1/2}$.

Література: ***1.*** *Bierbrauer J. On families of hash functions via geometric codes and concatenation. / Bierbrauer J., Johansson T., Kabatianskii G., Smeets B. //Advances in Cryptology-CRYPTO '93 Proceedings, Springer-Verlag.- 1994.-P. 331-342.* ***2.*** *Халимов Г. З. Аутентификация с применением алгеброгеометрических кодов. / Халимов Г. З., Кузнецов А. А. //Радиотехника. Всеукр. межвед. науч.-техн. сб.- 2001.- Вып. 120.- С. 103-109.* ***3.*** *Халимов Г. З. Аутентификация с применением Эрмитовых кодов. /Халимов Г. З., Иохов А. Ю. // Вестник ХПИ. – Х., -2005. НТУ „ХПИ". –Вып. 9. –С. 26-32.* ***4.*** *Халимов Г. З. Универсальное хеширование по максимальным кривым Гурвица. / Халимов Г. З. // Журнал "Прикладная радиоэлектроника". Харьков: ХНУРЭ. 2010. - Том. 9 № 3, - С.365-370* ***5.*** *Pellikan R. The Klein quartic, the Fano plan and curves representing design / Pellikan R.// In Codes, Curves and Signals: Common Threads in Communications, (A. Vardy Ed.), Kluwer Acad. Publ., Dordrecht. -1998. - P.9-20,* ***6.*** *Beelen P. The Newton polygon of plane curves with many rational points./ Beelen P., Pellikan R. //, Designs, Codes and Cryptography.- 2000. -V.21.- P. 41–67.*

УДК 004.7

ВИРІШЕННЯ ПРОБЛЕМИ ДОСТУПНОСТІ ОДНОТИПНИХ ОБ'ЄКТІВ МЕРЕЖІ ЗА ДОМЕННИМ ІМ'ЯМ В ПРОТОКОЛІ ТРАНСЛЯЦІЇ МЕРЕЖЕВИХ АДРЕС

Юрій Яремчук, Дмитро Кец, Євгеній Ніколаєв, Дар'я Іванішина
Вінницький національний технічний університет

Анотація: **Проведено аналіз проблеми доступності однотипних локальних сервісів до глобальної мережі, зокрема, доступності однотипних об'єктів до мережі за доменним ім'ям. Для вирішення даної проблеми було запропоновано метод, який шляхом додавання нових і розширення існуючих таблиць протоколу NAT та інтеграції з ними модифікованих таблиць протоколу DNS, забезпечує доступність сервісів за глобальним доменним ім'ям. Запропонований метод дозволив значно**

скоротити кількість використовуваних глобальних IPv4- адрес та підвищити стійкість до атак зловмисників з глобальної мережі.

Summary: **The paper analyzes the problem of local availability of similar services to the global network, including access to the same objects on the network domain name. To solve this problem was proposed a method that by adding new expansion of existing tables NAT protocol and integration with their modified tables Protocol DNS, ensure affordable services for the global domain name. A method to dramatically reduce the number of used global IPv4-addresses, and increase resistance to malicious attacks from the global network.**

Ключові слова: **Трансляція мережених адрес, локальний сервіс, доменне ім'я.**

I Вступ

Сьогодні все більш актуальною стає проблема доступності однотипних об'єктів мережі за ім'ям в протоколі трансляції мережевих адрес. Вирішення даної проблеми дозволить значно розширити можливості протоколу трансляції мережевих адрес IPv4, що отримав широке використання, забезпечивши можливість збільшення кількості глобальних сервісів і зменшити зростання використовуваних адрес цього протоколу. А крім того, дозволить вирішити проблему доступності однакових сервісів, розміщених в одній локальній мережі, доступних користувачеві за різними глобальними іменами DNS, але через одну адресу IPv4 в глобальній мережі Інтернет.

Як приклад, можна розглянути надання доступу до віддалених робочих станцій, доступ до яких відбувається через Інтернет. Доступ забезпечується за рахунок використання протоколу RDP (англ. Remote Desktop Protocol – протокол віддаленого робочого столу) [1]. Для доступу до локальної робочої станції потрібно використовувати порт 3389 і відповідно глобальну IP-адресу. Для забезпечення підключення до багатьох локальних робочих станцій при доступній одній глобальній IP-адресі потрібно використовувати протокол NAT і таблицю перенаправлення.

Значні прогресивні зміни в розвитку обчислювальної техніки, які відбулися за останнє десятиріччя, обумовили потребу в потужних та об'ємних розрахунках. Як наслідок, це дозволило розширити існуючі можливості та розробити нові різноманітні сервіси, які, в свою чергу, дозволяють забезпечувати інформатизацію суспільства. Всі ці технології набули значного розвитку завдяки існуванню основної технології інформатизації – Інтернету. Глобальна мережа Інтернет, в основному, побудована на протоколі IPv4, який під час розробки не передбачав такого стрімкого розвитку та глобалізації, оскільки був спроектований для обслуговування локальних мереж. Але завдяки своїм перевагам на момент зародження мережі Інтернет був обраний як стандарт. Як наслідок, виникла гостра проблема обмеженості використання протоколу IPv4, що полягає у закінченні доступних (вільних) IP- адрес [2].

Протокол IPv4 дозволяє використовувати лише 2^{32} (4 294 967 296) глобальних IP- адрес, яких на вересень 2010 року залишилося менше 6% від їх загальної теоретично доступної кількості [3]. В 1992 році було розпочато розробку нового протоколу IPv6, який забезпечує 2^{128} глобальних IP- адрес. Не зважаючи на всі переваги IPv6, до цього часу його так і не вдалося запровадити, оскільки він потребує нового мережевого обладнання, що є досить трудомістким та дорогим процесом оновлення на глобальному рівні.

У 1994 році було запропоновано альтернативне вирішення проблеми. Це протокол маршрутизації мережевих адрес NAT (з англ. Network Address Translation) [4]. Цей протокол дозволяє значно скоротити кількість використовуваних глобальних IP- адрес. Однак, даний протокол також має суттєвий недолік, що пов'язаний з обмеженістю використання з'єднань типу «один до багатьох» через один порт, ідентифікуючи об'єкти мережі за допомогою глобального імені DNS (з англ. Domain Name System).

Враховуюче вищесказане, слід відзначити, що існуючі на сьогодні методи на основі технологій IPv4 та IPv6 адрес та протокол NAT, які вирішують проблему доступності локальних сервісів у глобальних мережах, мають ряд недоліків. Зокрема в методі на основі використання додаткових глобальних IP- адрес:

- доволі обмежена кількість доступних IPv4- адрес;
- складність інтеграції IPv6 у мережеве обладнання та складність інтеграції в існуючі сервіси;
- велика ймовірність атаки на сервер з глобальної мережі зловмисниками.

В методі на основі протоколу NAT неможливо забезпечити одночасну доступність для більше ніж одного сервісу, які розміщуються на різних серверах локальної мережі.

Таким чином, актуальною є проблема нових рішень щодо вирішення проблеми доступності локальних сервісів у глобальній мережі.

ІІ Метод забезпечення доступності однотипних локальних сервісів до глобальної мережі

Суть даного методу полягає у розширені базових таблиць протоколу NAT та створенні залежних зв'язків з таблицями DNS за рахунок доповнення таблиць NAT додатковими відомостями про існуючі сервіси в локальній мережі з їх локалізацією (IP- адреса та порт), а також доповненням до таблиці DNS-зв'язків з розширеною таблицею NAT і вказанням зв'язку назви доступного сервісу з його глобальною назвою DNS.

Це дозволить використовувати протокол трансляції мережевих адрес у режимі доступу однотипних об'єктів локальної мережі в глобальній мережі за доменним ім'ям, що відповідає схемі зв'язків «багато до багатьох».

У стандартному протоколі NAT принцип надання доступу з глобальної мережі в локальну побудований на співставленні вхідних портів з портами конкретних серверів локальної мережі. Також існує перенаправлення діапазону портів, що дозволяє забезпечити роботу сервісів, які потребують для підключення більше ніж один порт. При перенаправленні портів на певний IP- адрес локальної мережі створюється правило, за рахунок якого відбувається резервування портів. Це означає, що діапазон зарезервованих портів більше не може бути використаним. При цьому кількість серверів, на які можуть бути перенаправленні пакети, відносно не велика, бо максимальна кількість портів, що може бути задіяна, дорівнює 65535.

Оскільки таблиці маршрутизації стандартного протоколу NAT (приклад наведено в табл. 1) не забезпечують потрібну ефективність доступності через один порт до однотипних сервісів, які розміщені на різних серверах, пропонується їх доповнити, додатково записуючи в таблицю значення однотипних сервісів і вказувати відповідно адресу їх серверів, на які будуть перенаправлятись пакети з глобальної в локальну мережу. Приклад доповнення таблиці NAT наведено в табл. 2.

Таблиця 1 – Стандартна таблиця маршрутизації NAT

ID	Port	TypeOfService	IP	Port
1	5190	ICQ	192.168.1.1	5190
2	80	Web – citzi.vntu.net	192.168.1.2	80
3	81	Web – netacad.vntu.net	192.168.1.3	80
4	82	Web – itacad.vntu.net	192.168.1.4	80
…		…	…	…

Таблиця 2 – Модифікована таблиця маршрутизації NAT

ID	InPort	TypeOfService	OutIP	OutPort
1	5190	ICQ	192.168.1.1	5190
2	80	Web – citzi.vntu.net	192.168.1.2	80
3	80	Web – netacad.vntu.net	192.168.1.3	80
4	80	Web – itacad.vntu.net	192.168.1.4	80
…	…	…	…	…

Це дозволить забезпечити доступність до різних сервісів, однак при цьому зменшиться ефективність використання ресурсів пропускної здатності локальної мережі, оскільки одночасно буде дублюватись інформація на всі сервери, записані у таблиці маршрутизації. Як наслідок, суттєво зменшиться пропускна здатність локальних мереж, а також будуть відправлятися надлишкові (невірні) пакети до невідповідних сервісів.

Для вирішення даної проблеми будемо ідентифікувати пакети, що надходять з глобальної мережі до маршрутизуючого пристрою мережі (NAT). Він повинен ідентифікувати за змістом пакету належність його до конкретної служби, яку запитує користувач глобальної мережі.

Суть ідентифікації полягає у використанні фільтрів вхідних пакетів, які дозволять визначити належність вхідного трафіку IP- адреси серверу у локальній мережі для перенаправлення пакетів до відповідного серверу (сервісу). Для реалізації фільтрації вхідних пакетів потрібно створити таблицю, в якій буде вказано назву сервісу і відповідно шаблони (маски) вхідних пакетів, які є характерними для конкретної служби. Це дозволить не створювати надлишкову завантаженість локальної мережі та інших серверів. Приклад динамічної тимчасової таблиці наведено у табл. 3.

Таблиця 3 – Таблиця тимчасової динамічної маршрутизації

ID	TypeOfService	TemplatePackage
1	ICQ	DATA 0x800….
2	Mail	DATA 0x4078….

Далі потрібно створити механізм зв'язків між таблицею шаблонів різних сервісів і модифікованою таблицею NAT, в якій вхідні пакети на етапі підключення розпізнаються, та визначити їх належність до різних сервісів. Після чого, використовуючи модифіковану таблицю маршрутизації NAT, можна перенаправляти пакети на відповідні сервери локальної мережі. Цим забезпечується доступність до подібних сервісів, які водночас знаходяться на різних серверах (зв'язок «багато до багатьох»).

Враховуючи особливість доповнення таблиць маршрутизації NAT виникає проблема, пов'язана з повторним підключенням, коли через деякий час після першого підключення, надходять від користувача пакети даних, які неможливо ідентифікувати за шаблонними масками. При усуненні цієї проблеми слід враховувати, що в пакетах передавання даних не міститься інформація про належність її до сервісів, а ідентифікувати дані за маскою не можливо. Тому потрібно використовувати додаткову динамічну таблицю, в якій вказувати IP- адресу та порт, з яких відбулося підключення, а також IP- адресу та порт, на які було перенаправлено пакет. Також слід враховувати той факт, що відслідкувати процес закінчення сеансу зв'язку неможливо, тому слід додати поле до стандартної таблиці NAT, де буде вказуватися максимальний час існування кожного запису. Приклад модифікованої таблиці NAT наведено в табл. 4.

Таблиця 4 – Модифікована таблиця NAT

ID	InIP	InPort	TypeOfService	OutIP	OutPort	EndTime
1	112.13.75.93	45328	ICQ	192.168.1.1	5190	2010-01-01 12:45:48
2	240.9.3.14	15985	Web – citzi.vntu.net	192.168.1.2	80	2010-01-01 12:24:17
…	…	…	…	…	…	…
66	159.46.97.1	53589	Web – netacad.vntu.net	192.168.1.3	80	2010-01-01 12:34:25
67	67.79.14.2	38945	Mail	192.168.1.4	449	2010-01-01 13:00:08

Для покращення якості ідентифікації належності пакетів до служб під час первинного підключення пропонується використовувати додаткову прив'язку до DNS назв сервісів. Але, враховуючи особливість змісту пакетів, в яких частіше всього не вказується DNS-назва підключення (окрім Web-пакетів), слід використовувати співставлення запитуваного сервісу клієнтом під час запиту IP-адреси в момент співставлення її з DNS ім'ям.

Якщо розглядати загальну структуру роботи DNS, то на запит користувача DNS-сервер повертає IP-адресу. На сьогоднішній день існує близько 11 глобальних серверів (вони доступні для всіх користувачів мережі Інтернет), які надають IP-адресу відповідно до запиту за іменами другого рівня (vntu.net, nokia.com). Імена третього рівня частіше всього обслуговує користувач, який придбав ім'я другого рівня (citzi.vntu.net, netacad.vntu.net). Оскільки суб'єкт, який надає доступ до певних сервісів і має придбане доменне ім'я другого рівня, може розмістити у себе DNS сервер, це дозволить розмістити DNS службу безпосередньо на пристрої маршрутизації а також контролювати всі імена третього рівня.

Для реалізації даного методу потрібно створити додаткову динамічну таблицю маршрутизації на основі DNS запитів, яка буде зберігати інформацію про IP-адреси клієнтів та назви DNS, які вони запитували. Ці дані дозволять проаналізувати, який сервіс був запитаний клієнтом і створити відповідний запис в модифікованих динамічних таблицях NAT. Для забезпечення швидкодії такої таблиці потрібно додати мітки часу, які будуть визначати час життя записів. Це дозволить видаляти з таблиці неактуальні записи, за рахунок чого зменшиться час пошуку даних по таблиці. Приклад таблиці записів динамічних співставлень DNS запитів наведено у табл. 5.

Таблиця 5 – Таблиця записів динамічних співставлень DNS запитів

ID	InIP	TypeOfService	EndTime
1	112.13.75.93	login.icq.com	2010-01-01 12:45:48
2	240.9.3.14	citzi.vntu.net	2010-01-01 12:24:17
…	…	…	…
66	159.46.97.1	netacad.vntu.net	2010-01-01 12:34:25
67	67.79.14.2	email.vntu.net	2010-01-01 13:00:08

Для вдосконалення механізму ідентифікації трафіку мережі також доцільним є створення зв’язків між модифікованими таблицями NAT і динамічними таблицями співставлень DNS записів. Між цими таблицями потрібно створити зв'язок на основі співставлення записів *TypeOfService*. Це дозволить на ранньому етапі підключення визначити місцезнаходження сервісу (у локальній мережі) та попередньо створити записи для підключення, а саме запис до модифікованої таблиці NAT (див. табл. 4).

Запропоновані зміни також дозволять значно зменшити запити до таблиці тимчасової динамічної маршрутизації (див. табл. 3). До цього обробка даної таблиці займала досить багато часу, оскільки потребувала порівняння з усіма вхідними пакетами.

III Висновок

Таким чином, було проведено аналіз проблеми доступності однотипних локальних сервісів до глобальної мережі, зокрема доступності однотипних об’єктів мережі за доменним ім’ям. Для вирішення даної проблеми було запропоновано метод, який шляхом додавання нових і розширення існуючих таблиць протоколу NAT та інтеграції з ними модифікованих таблиць протоколу DNS забезпечує доступність сервісів за глобальним доменним ім’ям. Детально описані всі додаткові поля та таблиці, їх призначення та взаємозв’язок.

Також розробленим методом забезпечується захист серверів від атак зловмисників на різні служби, які розміщені на цих серверах, шляхом підключення до серверів через протокол NAT. Таке рішення дозволяє значно скоротити кількість використовуваних глобальних IPv4-адрес та підвищити стійкість до атак зловмисників з глобальної мережі.

Література: ***1.*** *Рэнд Моримото, Майкл Ноэл. Microsoft Windows Server 2008 R2. Полное руководство // Службы удаленных рабочих столов. – Вильямс. – 2011. – 485-501 с.* ***2.*** *Хилл Брайан. Полный справочник по CISCO. – Вильямс. – 2004. – 1088 с.* ***3.*** *http://www.securitylab.ru/news/398151.php* ***4.*** *Bill Dutcher. The NAT Handbook: Implementing and Managing Network Address Translation 322 p.*

УДК: 004.056.5

ЗМЕНШЕННЯ ВІДХИЛЕНЬ КООРДИНАТ ТОЧОК ВНАСЛІДОК ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ВЕКТОРНІ ЗОБРАЖЕННЯ

Василь Карпінець, Юрій Яремчук
Вінницький національний технічний університет

Анотація: **Проведено аналіз проблеми виникнення значних відхилень окремих точок векторного зображення після вбудовування ЦВЗ. Для вирішення вказаної проблеми запропоновано метод відбору придатних для вбудовування матриць коефіцієнтів ДКП, зміна яких не призводить до значних відхилень координат точок. Для цього перед вбудовуванням використовуються умови для порівняння значень коефіцієнтів з деяким граничним значенням, що визначає максимально можливу зміну коефіцієнтів внаслідок вбудовування ЦВЗ.**

Summary: **The paper analyzes the problem of large deviations of individual points of the vector image after embedding watermark. To solve the given problem the selection method suitable for embedding matrix coefficients of discrete cosine transform, a change which does not lead to significant variations of position. To do this, before embedding conditions used to compare coefficients of a certain limit, which determines the maximum possible change in the coefficients due to watermark embedding.**

Ключові слова: **Стеганографія, цифровий водяний знак, захист авторського права, дискретне косинус-перетворення, векторні зображення.**

I Вступ

Графічні цифрові зображення сьогодні дуже широко використовуються в комп’ютерних системах, зокрема все більшого поширення отримують цифрові зображення векторного формату, що використовуються для проектування архітектурних об’єктів, інтер’єрів, розробки приладів, реклами, логотипів, створення шрифтів, географічних карт тощо, на створення яких витрачається багато часу та коштів. В зв’язку з цим актуальною стає проблема захисту векторних зображень. При цьому особливий інтерес викликає таке забезпечення захисту, для якого не потрібно наявності оригіналу для підтвердження авторства.