УДК 004.056

О.А. Замула[1], Д.О. Семченко[2]

[1] *Харківський національний університет імені В.Н. Каразіна, Харків*
[2] *Харківський національний університет радіоелектроніки, Харків*

МЕТОД ОБРОБКИ ТА ПЕРЕДАЧІ ЗАХИЩЕНИХ ДАНИХ З ВИКОРИСТАННЯМ СТАНДАРТНИХ ПРОТОКОЛІВ TCP/UDP

Представлено метод обробки та передачі захищених даних. Наведено аналіз існуючих мереж, математичну модель запропонованого методу та обґрунтовані основні вимоги щодо вибору генератора псевдовипадкової послідовності для зміни часових значень. Сформульовані пропозиції щодо використання методу в сучасних телекомунікаційних системах.

Ключові слова: *генератор, безпека, метод, протокол, сід, часові затримки, проксі, мережевий стек, пакет даних.*

Вступ

Постановка задачі. Важливим фактором що впливає на розвиток інформаційно-телекомунікаційної системи є підтримка різноманітних зв'язків між абонентами в мережі з одночасним забезпеченням безпеки цих комунікацій.

Інформаційно-телекомунікаційна система (ІТС) повинна враховувати появу нових технологій та сервісів, а також задовольняти загальним вимогам, що висуваються до елементів цієї системи, такими як: використання відкритих стандартів, інтегрованих рішень, забезпечення масштабування цієї системи тощо [1].

Для того щоб забезпечити надійний захист ресурсів в ІТС повинні бути реалізовані такі задачі [2]:

– криптографічний захист даних для забезпечення конфіденційності, цілісності й автентичності інформації, що передається;

– гарантована ідентифікація користувачів за рахунок використання ключів, смарт-карт тощо;

– комплексний підхід до забезпечення безпеки інформації, що забезпечує раціональне поєднання технологій та засобів інформаційного захисту.

Під час побудови корпоративної мережі постає питання створення надійного захисту від проникнення порушників у мережу. Такий захист реалізується, в тому числі, на базі протоколів TCP/IP і стандартних Internet-додатків (e-mail, Web, FTP) [3, 4].

Для вирішення задач надійного захисту ресурсів в ІТС необхідно, що б методи, засоби та заходи захисту забезпечували, по-перше, захист інформації під час передачі даних через мережу від відомих атак на основі використання криптографічних алгоритмів перетворення інформації, і по-друге, забезпечували скритності самого факту передачі цих даних [5].

Аналіз наукових досліджень. У загальному вигляді структура каналу обміну даними представляється за допомогою схеми, що наведена на рис. 1.

Проведений аналіз існуючих корпоративних мереж, що використовують канали обміну даними згідно з рис. 1 показав, що ефективним рішенням для забезпечення захисту інформації, що передається, є криптографічне перетворення цієї інформації. На криптографічний захист покладається вирішення завдань запобігання несанкціонованого доступу (НСД) до інформації та системних ресурсів. Загальновизнаним є той факт, що необхідна якість криптографічного захисту забезпечується тільки при використанні спеціальних засобів криптографічного захисту інформації [6, 7]:

- апаратних, програмних, програмно-апаратних засобів, що реалізують криптографічне перетворення інформації;

- апаратних, програмних, програмно-апаратних засобів забезпечення цілісності та справжності інформації, у тому числі засобів імітозахисту та цифрового підпису, що здійснюються за допомогою криптографічного перетворення інформації;

- апаратних, програмних, програмно-апаратних засобів, призначених для управління ключовими даними, включаючи генерацію ключових даних та виготовлення ключових документів;

Рис. 1. Схема побудови каналу обміну даними

- апаратних, програмних та програмно-апаратних засобів захисту інформації від НСД, що використовують криптографічні алгоритми перетворення інформації.

У якості спеціальних засобів криптографічного захисту інформації під час розробки методу обробки та передачі захищених даних з використанням стандартних протоколів TCP/UDP були розроблені програмні засоби, які на відміну від відомих дозволяють (з використанням існуючого програмного забезпечення), обробляти дані згідно з одним з кроків метода, що пропонується. Таким чином забезпечується захист даних абонентів під час інформаційного обміну. Можливість такої реалізації обумовлена особливістю інкапсуляції властивостей між рівнями OSI, завдяки чому стає можливим, не враховуючи програмного а/або апаратного забезпечення мережі, розробити метод обробки та передачі з метою захисту даних з використанням стандартних протоколів TCP/UDP.

Основна частина

Розроблений метод базується на таких основних кроках.

1. Аналіз мережі

На першому кроці методу здійснюється аналіз мережі, який передбачає можливість маніпулювання часовими затримками. Під часовими затримками пакету у мережі будемо розуміти час, необхідний пакету щоб досягти отримувача з моменту його відправки. При цьому під часовим вікном розумітимемо найбільше значення штучного збільшення часової затримки пакету між отриманими та відправленими пакетами даними. У ході досліджень мережі з використанням сучасних програмних засобів обміну даними, було встановлено, що часове вікно не повинне перевищувати 20 мілісекунд, що є розумним компромісом між надійністю і невизначеністю вбудованих затримок за допомогою будь-якого сканера мережевих пакетів, які, як правило, використовуються для моніторингу активності у мережі. Кожний мережевий пакет, який має штучно збільшену часову затримку назвемо несучим пакетом. Результатом аналізу мережі може бути мережевий дамп пакетів, під час інформаційного обміну за допомогою будь-якого програмного забезпечення, що використовує протоколи TCP/UDP. На основі цього дампу будується гістограма розподілення міжпакетних затримок, що візуально відображує розподіл часових вікон між пакетами (рис. 2).

Візуальне відображення розподілу дозволяє серед усіх пакетів обрати саме ті, що найбільше задовольняють вимогам до часового вікна. Якщо такі пакети існують, то визначаються властивості цих пакетів, згідно яких обираються наступні пакети для подальшого використання на послідуючих кроках.

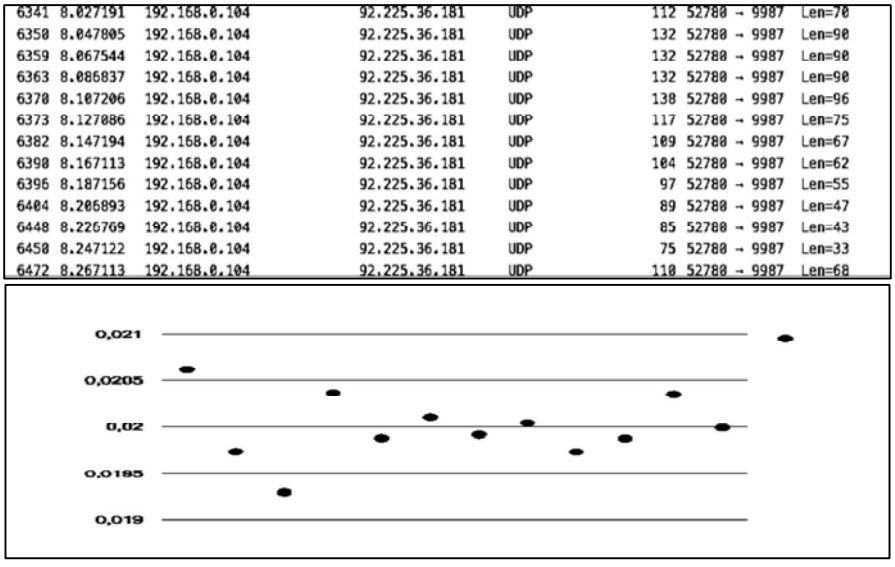

Рис. 2. Розподіл часових вікон між пакетами під час інформаційного обміну за допомогою програми Team Speak

2. Розробка математичної моделі

Для передачі одного біту інформації в мережі між абонентами будемо використовувати загальну схему каналу обміну даними (рис. 1). Для того, щоб реалізувати управління часовими затримками необхідно, крім елементів, що надані на рис. 1, додатково використовувати аналізатор пакетів між клієнтом та мережевим стеком операційної системи. Аналізатор пакетів являє собою по суті UDP proxy, що здійснює аналіз пакетів на можливість вбудування затримок на основі обробки та перевірки пакетів за їх властивостями, за результатами аналізу струму мережевих даних, який був проведений на першому кроці методу. Таким чином, схема каналу обміну даними на основі управління часовими затримками буде мати вигляд, що наведений вказаний на рис. 3.

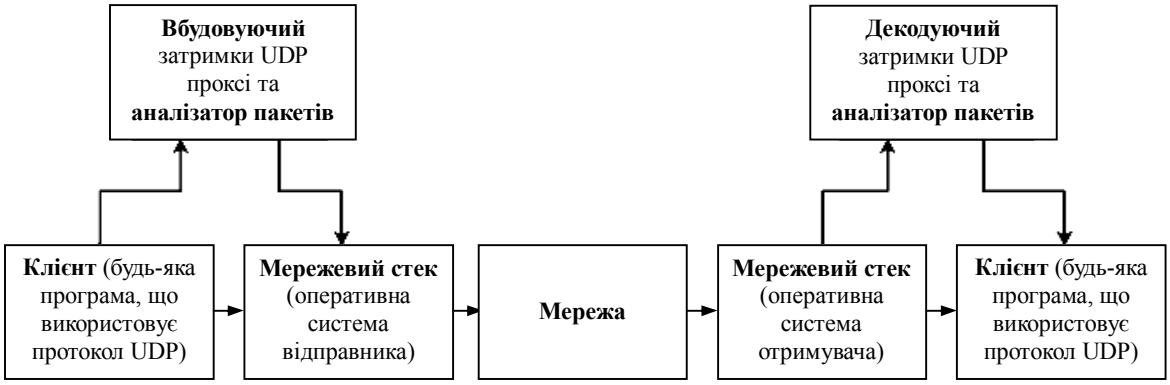

Рис. 3. Схема побудови каналу обміну даними на основі управління часовими затримками

Процес обміну даними здійснюється наступним чином. UDP proxy починає очікувати пакети, які за алгоритмом визначаються як несучі пакети, для того щоб вбудувати часові затримки. Як тільки клієнт намагається передати пакет через мережу, здійснюється обробка пакету та пакет перевіряється на придатність до вбудовування затримки.

Якщо пакет класифікується як непридатний для затримування (тобто він не є несучим пакетом), він відправляється одразу ж у мережу.

Якщо це перший придатний для затримування пакет (несучий пакет), то він також одразу ж пропускається в мережу, при цьому запам'ятовується його часова мітка.

Коли передається несучий пакет, UDP proxy розраховує, на який мінімальний час цей пакет можна затримати таким чином, щоб деяке попередньо задане числове значення дорівнювало міжпакетному часу, яке визначається таким чином:

$$\left(t_2' - t_1'\right) \bmod \omega, \qquad (1)$$

де t_1' – дійсний час передачі попереднього несучого пакета; t_2' – дійсний час передачі поточного несучого пакета; а $\omega = 20000\mu s$ є розміром часового вікна.

Значення кожного біту інформації (0 або 1) кодується так званими бітчасовими значеннями, які знаходяться в інтервалі від 0 до значення розміру часового вікна.

Бітчасові значення обираються таким чином, щоб різниця між ними дорівнювала половині часового вікна.

Єдиним обмеженням для вибору бітчасових значень для кожного з бітів 0 або 1 є наступні рівняння:

$$\begin{aligned} b_0 &= (b_1 + \omega / 2) \bmod \omega; \\ b_1 &= (b_0 + \omega / 2) \bmod \omega, \end{aligned} \qquad (2)$$

де b_0 – бітчасове значення біта 0; b_1 – бітчасове значення біта 1.

Таким чином, b_0 та b_1 повинні знаходиться в інтервалі $[0, \omega)$, і кожен з цих двох b_0 та b_1 бітчасових значень однозначно визначається довільним вибором бітчасового значення протилежного біту (для 0 буде 1 і навпаки).

Наприклад, довільний вибір $b_0 = 7000\mu s$ однозначно визначає значення b_1, що дорівнює $17000\mu s$, з урахуванням часового вікна у $20000\mu s$.

Розрахована затримка використовується при виконанні "холостого" циклу (циклу, який не передбачає вбудування часової затримки) до тих пір, поки відповідний час затримки не пройде. Час завершення "холостого" циклу розраховується за формулою

$$t_2' = t_c + (b_i - (t_c - t_1') \bmod \omega) \bmod \omega,$$

де $i \in \{0,1\}$; t_c – поточний час, а b – бітчасове значення біту.

Для синхронізації даних необхідно використовувати дев'яти бітову послідовність, іменовану як FSS (frame synchronization sequence). Основною метою FSS є не розбивання шифрованого потоку бітів на кадри, а поліпшення визначення початку послідовності несучих пактів і відкидання усіх попередніх пакетів, що надіслані "клієнтом". Як тільки FSS виявлена в потоці затримок, "клієнт" отримувача стає готовим для декодування корисних даних з затримок. Щоб компенсувати можливі втрати даних закодованих у вигляді затримок, одні й ті ж дані відтворюються повторно в затримках, як проста міра протидії пошкодженню даних, що виникли в результаті мережевого шуму. Як тільки всі необхідні закодовані дані відправлені через прихований тимчасової канал, передачу даних слід повторити, починаючи з FSS. Це повинен враховувати "клієнт" отримувача.

3. Аналіз та вибір криптографічних засобів захисту при передачі даних

Для вирішення задачі криптографічної стійкості до відомих атак під час передачі даних через мережу необхідно, щоб прихований канал не містив даних в явному вигляді. Часове значення можна динамічно змінювати для кожної затримки, що кодується згідно деякої псевдовипадкової послідовності. При цьому необхідно враховувати, що псевдовипадкова послідовність повинна бути синхронізована з "клієнтом" отримувача. Знання обраної послідовно-

сті бітчасових значень дозволить виявити прихований канал передачі даних. Відповідно ця послідовність повинна бути закритою по відношенню до всіх крім учасників обміну даними. Спільний секрет дозволяє запобігти виявленню каналу, при використанні засобів аналізу мережевого трафіку під час передачі даних.

З метою забезпечення захисту від криптографічних атак та для генерації бітчасових значень може бути використаний генератор псевдовипадкової послідовності CMWC (complementary multiply with carry) Marsaglia [8].

Найпростіший приклад генератора з періодом більше 2^{285} вимагає 291 біт стану генератора, при цьому, з них, - мінімум 256 біт можна використовувати як сід [9]. Даний генератор псевдовипадкової послідовності використовується в комбінації з SHA-256 [10].

Крім криптографічних характеристик, вибір цього алгоритму обумовлений наявністю можливості розрахунку SHA-256 в операційній системі Windows стандартним крипто-провайдером і рівності розміру його хешу розміру його сіду. Це дозволяє у повному обсязі використовувати ентропію як алгоритму хешування так і генератора псевдовипадкової послідовності.

Таким чином хеш паролю використовується для ініціалізації генератора псевдовипадкової послідовності.

Висновки

В процесі досліджень були розроблені програмні засоби, що реалізують отриманий метод обробки та передачі захищених даних.

Крипостійкість розробленої системи визначається стійкістю генератора псевдовипадкової послідовності.

У конкретній реалізації використовується алгоритм хешування SHA-256 у поєднанні CMWC Marsaglia. При цьому спільний секрет представлений як хеш паролю, що є сідом для генератора. Реалізація розробленого метода буде ефективна на відстані до 20 хопів завдяки властивостям інкапсуляції відповідно до рівнів моделі OSI.

Для мінімізації втрат пакетів під час передачі необхідно використовувати FSS довжиною 9 біт та алгоритм повторної відправки пакету при його втраті а/або часткового руйнування.

Список літератури

1. Галицкий А.В. Защита информации в сети — анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. – М.: ДМК Пресс, 2004. – 224 с.

2. Зима В.М. Безопасность глобальных сетевых технологий / В.М. Зима, А.А. Молдовян, Н.А. Молдовян. – СПб.: БХВ-Петербург, 2001. – 180 с.

3. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон. – М.: ИЛ, 1963. – 830 с. (Раздел – Теория связи в секретных системах).

4. Вембо Мао. Современная криптография. Теория и практика. / Вембо Мао. Пер. с англ. – М.: Изд. дом «Вильямс», 2005. – 768 с.

5. Решения компании Cisco Systems по обеспечению безопасности корпоративных сетей. – М.: Московский офис Cisco Systems. Inc. 2001.

6. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування : Монографія / І.Д. Горбенко, Ю.І. Горбенко. – Х.: Форт, 2012. – 880 с.

7. Горбенко І.Д. Теоретичні основи побудови криптографічних систем абсолютної стійкості // Системи обробки інформації / І.Д. Горбенко, О.А. Замула. – Х.: ХУПС, 2013. – Вип. 4 (111). – С. 101-105.

8. Marsaglia G. (2003)/ Seeds for random number generators. Communications ACM May 2003.

9. Knuth D.E.(1998). The art of Computer Programming, Volume 2, 3rd Ed., Addison Wesley, Reading, Mass.

10. FIPS PUB 180-4, Federal Information Processing Stabdards Publication, March 2012.

Надійшла до редколегії 15.12.2015

Рецензент: д-р техн. наук проф. В.А. Краснобаєв, Харківський національний університет ім. В.Н. Каразіна, Харків.

МЕТОД ОБРАБОТКИ И ПЕРЕДАЧИ ЗАЩИЩЕННЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СТАНДАРТНЫХ ПРОТОКОЛОВ TCP / UDP

А.А. Замула, Д.А. Семченко

Представлен метод обработки и передачи защищенных данных. Приведены анализ существующих сетей, математическая модель предложенного метода и обоснованы основные требования к выбору генератора псевдослучайных последовательностей для осуществления смены часовых значений задержек. Сформулированы предложения по использованию метода в современных телекоммуникационных системах.

Ключевые слова: *генератор, безопасность, метод, протокол, сид, временные задержки, прокси, сетевой стек, пакет данных.*

METHOD FOR PROCESSING AND TRANSFER OF PROTECTED DATA USING STANDARD PROTOCOLS TCP / UDP

A.A. Zamula, D.A. Semchenko

The basic steps in which the proposed method is implemented processing and transmission of protected data. The above analysis of the existing networks, a mathematical model of the proposed method and proved the basic requirement of choice pseudo-random sequence generator to change the time values. It makes the main conclusions that reflect the characteristics of the proposed method and used in the software implementation of the proposed method.

Keywords: *generator, security, method, protocol, Sid, time delay, proxy, network stack, data package.*