«Поліграфічні, мультимедійні та web-технології», 17-19 жовтня 2018 р.: матеріали конференції. Львів : УАД, 2018. – С. 49-51.
3. *Заде Л. А.* Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. А. Заде. – М.: Мир, 1976. – 165 с.
4. *Гавенко С. Ф.* Інтегральний прогноз якості книжкових видань / С. Ф. Гавенко, В. М. Сеньківський, Н. Є. Сеньківська // Наукові записки [Української академії друкарства]. – 2012. – № 1. – С. 144-148.
5. *Кудряшова А. В.* Формування інтегрального показника якості процесу структурування видання / А. В. Кудряшова, Н. М. Литовченко // Поліграфія і видавнича справа [Української академії друкарства]. – 2018. – № 1 (75). – С. 82-89.
6. *Сеньківський В. М.* Формування інтегрального показника якості реалізації процесу проектування видання / В. М. Сеньківський, А. В. Кудряшова // Поліграфія і видавнича справа [Української академії друкарства]. – 2017. – № 2 (74). – С. 11–18.
7. *Сеньківський В. М.* Алгоритм імітаційної моделі оцінювання якості реалізації монтажних спусків / В. М. Сеньківський, І. В. Піх, О. В. Литовченко, Т. С. Голубник, Ю. І. Петрів // Наукові записки [Української академії друкарства] – 2015. – № 1. – С. 7-15.
8. Методика визначення обсягу авторського і видавничого оригіналів [Електронний ресурс]: К.: Кн. палата України, 1998. – 3 с. – Режим доступу: https://www.twirpx.com/file/983011/ – 12.09.2018. – Загол. з екрану.
9. *Мельников О. В.* Технологія плоского офсетного друку: [підручник] / О. В. Мельников. – Львів : Афіша, 2003. – 388 с.
10. *Заде Л.* Роль мягких вычислений и нечеткой логики в понимании, конструировании и развитии информационных интеллектуальных систем. / Л. Заде // Новости искусственного интеллекта. – Москва. – 2001. – № 2–3. – С. 7–11.

Поступила 17.09.2018р.

УДК 519.7:004.9

О.В. Тимченко [1, 2], д.т.н., професор,
О.О. Тимченко [2], аспірант,
Б.М. Гавриш [2], к.т.н., ст. викл.

ВИКОРИСТАННЯ СТЕГАНОГРАФІЇ В МЕРЕЖАХ TCP/IP

Вступ

Сучасний світ далекий від досконалості. Часто ми маємо деякі важливі дані, які можуть викликати інтерес у людей, фірм, установ, які не мають повноважень на доступ до цієї інформації. Дані, що зберігаються та передаються, наражаються на перехоплення та читання, що є небажаним і може бути небезпечним (з міркувань безпеки, фінансової тощо). Для того,

[1] Uniwersytet Warmińsko-Mazurski w Olsztynie
[2] Українська академія друкарства

щоб захистити наші дані і запобігти їх читання сторонніми особами, криптографічні методи використовують надійні алгоритми шифрування і гарантують практичну неможливість злому і читання захищених даних без знання ключа і, таким чином, забезпечують безпеку даних.

З цих причин буде корисною техніка, яка дозволить, крім шифрування даних, приховати цей факт від сторонніх осіб. Якщо не можна приховати той факт, що надсилаються деякі дані, то можна зробити так щоб вони виглядали невинними. Існуюча для цього техніка називається стеганографією.

Динамічний розвиток комп'ютерних мереж та одночасне поширення шахрайства та злочинів зумовлюють створення дедалі кращої та більш складної мережевої безпеки. Всі об'єкти, для яких необхідний доступ до глобальної мережі, повинні захистити свої системи і дані, ізолювати себе від Інтернету використанням брандмауера, проксі-сервера, і т.д. Вони хочуть переконатися, що немає небажаного вихідного або вхідного трафіку у внутрішній мережі. З іншого боку вони створюють проблеми для стеганографії: як в звичному і «невинному» мережевому трафіку (наприклад, передача HTTP з загальнодоступного веб-сервера) зашивати дані, які не повинні потрапити всередину мережі? Як надсилати дані у світ із такої захищеної мережі, якщо всі можливості передачі даних були заблоковані адміністраторами?

Метою роботи є аналіз використання стеганографії в комп'ютерних мережах, зокрема найчастіше використовуваними мережами TCP/IP. Висновки, представлені в роботі, стосуються як локальних мереж TCP/IP, так і глобальної мережі – Інтернету.

Аналіз протоколів TCP/IP

Елементи, які можуть бути використані для створення прихованих каналів, можна вказати на кожному рівні моделі ISO/OSI (рис.1). Методи, які використовуються для цієї мети різні і залежать від характеристик моделей рівня, а більш конкретно – характеристик, що використовуються на цьому рівні мережевого протоколу, апаратних засобів і програмного забезпечення [1].

TCP/IP це загальна назва двох основних протоколів мережі Інтернет. Виникла через з'єднання назв TCP і IP. Протокол TCP/IP (ang. Transmission Control Protocol/Internet Protocol) є «програмним протоколом мережевої комунікації» (ang. *software-based communications protocol used in networking*). TCP/IP відкриває доступ до методів трансмісії інформації між окремими комп'ютерами в мережі, обслуговуючи помилки, що з'являються, а також створюючи додаткову інформацію, що вимагається для трансмісії.

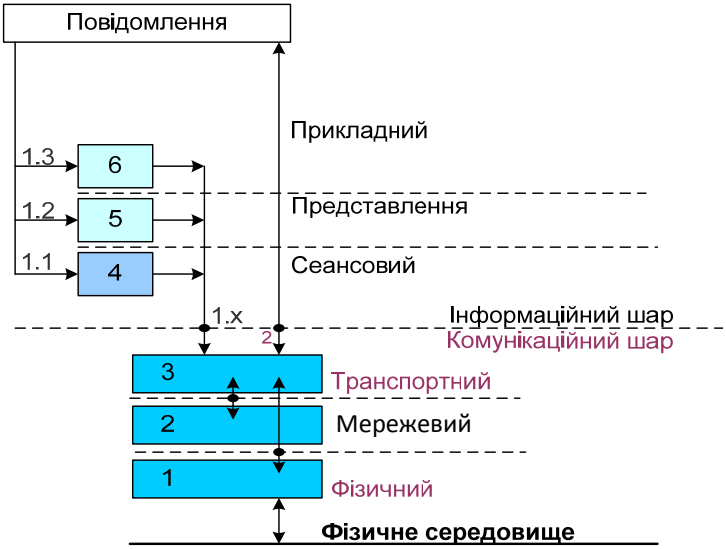

Рис. 1. Мережева модель передачі даних

Проаналізуємо особливості протоколів IP та TCP. Відповідь на питання про можливості передачі даних в захищених мережевих протоколах отримаємо шляхом вивчення структури пакетів цих протоколів (рис.2). Проведено аналіз щодо придатності їх для передачі даних, відмінних від задумів розробників, в елементах заголовків протоколів IP і TCP, які можуть бути використані для створення прихованих каналів, визначено фактичну придатність, переваги і недоліки, можливості виявлення. Звернута увагу на заходи, які необхідно вжити для усунення існування окремих прихованих каналів та/або запобігання передачею через них.

Біти 0-3	**4-7**	**8-15**	**16-18**	**19-23**	**24-31**
Версія	HLEN	Тип обслуговування	Загальна довжина		
Ідентифікація			Прапорці	Зміщення фрагментації	
Час життя		Протокол	Контрольна сума заголовку		
IP-адреса відправника					
IP-адреса отримувача					
Опції					Додаток
Дані (65535 мінус заголовок)					
…					

Рис. 2. Структура IP-пакету

Ідентифікація прихованих каналів

IP протокол

При більш ретельному аналізі структури IP-пакету, який є основною транспортною одиницею на мережевому рівні протоколу IP, можна попередньо виділити кілька елементів, які можуть являти собою потенційний об'єкт для створення прихованого каналу. Не кожен з цих елементів є однаково привабливим і доцільним.

Поле Тип обслуговування (Type of Service)

Перше цікаве поле заголовка IP-датаграми – це поле типу обслуговування (рис. 1). Це 8-бітове поле, не має чітко визначеної структури і може бути по-різному витлумачене в існуючих реалізаціях IP. Ця невизначеність може бути використана для створення прихованого каналу.

Зазначене поле в мережі IP може бути використане чи ні, що залежить від обладнання (маршрутизаторів) і програмного забезпечення (операційних систем, додатків), і рішення, на практиці залежить від творців і адміністраторів мережі. Крім того, через згадану невизначеність значення, вміщене в поле ToS використовується для управління роботою мережі. У невеликих мережах, де немає потреби в додаткових сервісах контролю якості, це поле взагалі не використовується і залишається порожнім. Однак все частіше, з розвитком методів якості обслуговування *Quality of Service* (QoS), зростаючий попит на вимоги щодо якості роботи мережі і пропонованої пропускної здатності, затримки і надійності, це поле знаходить застосування. В контексті мереж, які використовують техніку QoS диференційованих послуг *Differentiated Services*, поле ToS носить назву *Differentiated Services Codepoint* (DSCP).

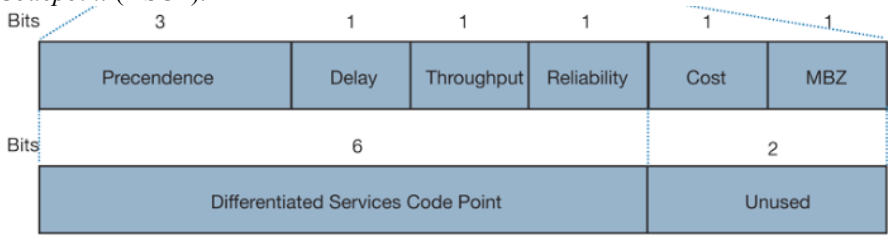

Рис.3. Дві інтерпретації поля ToS / DSCP

Поле ToS/DSCP для надсилання прихованих даних може використовуватися кількома способами.

Наприклад:

1. використання всього поля ToS (тобто всі вісім бітів) для передачі даних;

2. використання одного, невикористаного (наймолодшого) біта, щоб не впливати на значення, вже введені в поле (і не перешкоджати методу передачі);

3. використовуючи один біт, який зазвичай використовується, наприклад, біт, що вказує на невелику затримку (біт 4);

4. використання трьох лівих (найстарших) бітів поля ToS, які визначають пріоритет і на практиці ігноруються в більшості мереж;

5. використання двох наймолодших, невикористовуваних бітів поля DSCP (в мережах, що використовують техніку *DiffServ*).

Ці методи відрізняються деякими основними функціями. По-перше, що найбільш очевидно, відрізняться по обсягу (пропускної спроможності), сформований через них прихований канал – від цілого байта до одного біту на IP-пакет (тобто від 20 до 1500 байт транспортуваних в пакеті – максимальний розмір транспортної одиниці (MTU) в мережах Ethernet зазвичай встановлений до 1500 байт). По-друге, різним є ступінь прихованості створеного каналу.

Моніторинг переданих і модифікованих пакетів IP особою, яка здійснює нагляд за роботою мережі і їх аналіз виявить деякі неправильності поля ToS в першому випадку, тому що ні за яких обставин не представляється можливим використовувати все поле в «нормальній» робочій мережі IP. Крім того, використання невикористаних бітів може бути підставою для підозр. Використання бітів, які дозволяються, але не використовуються в певній мережі, буде менш підозрілим і може бути викликане помилками програмного забезпечення або конфігурації. Від ретельного аналізу трафіку, звичайно, захиститись таким чином не можна, але якщо ми приймаємо перший сценарій, у нас буде менше турбот.

Слід також згадати про відсутність опору прихованого створеного каналу від розмивання або видалення. У випадку мережі, в якій ToS-поле не використовується, маршрутизатори можуть ігнорувати їх, або обнулити в кожному пакеті, який пересилається. Якщо це поле використовується - його можна встановити в будь-якому такому пристрої відповідно до попередньо встановленої конфігурації. У випадку виявлення передачі даних за допомогою поля ToS, переривання передачі даних полягає в простому збереженні іншого значення в цьому полі.

Поле ідентифікації

Наступним об’єктом є 16-бітне поле ідентифікації. Воно використовується для унікальної ідентифікації кожного пакету і повинно бути унікальним, але що важливо – тільки в межах однієї передачі для пари передавач-приймач (хост-передавача хост-приймача). Винятком є фрагментовані пакети – в цьому випадку кожен фрагмент має однаковий ідентифікаційний номер. Точні зміни, пов’язані з ідентифікаційними номерами наступних пакетів, залежать від реалізації стеку TCP/IP – вони зазвичай збільшуються. Однак, так як вимога унікальності застосовується тільки в одній передачі (оскільки він використовується, щоб розрізняти окремі пакети і/або їх фрагменти), і не накладається будь яких залежностей між ідентифікаційними номерами наступних блоків, існує можливість зміни значення цього поля якимось чином, який зберігає унікальну нумерацію.

Іншими словами: поки ми надаємо різні значення ідентифікаційного номера для різних пакетів, ми можемо вільно їх вибирати. Ця функція дозволяє кодувати здавалося б, незалежні, "випадкові" значення.

Якщо ідентифікаційні номери, створені незалежно від алгоритмів стеку TCP/IP, унікальні, то це не вплине на зв'язок. Аналіз IP-пакетів може дати підставу вважати, що ідентифікація була дещо модифікована, але ми не можете це сказати з впевненістю, не знаючи операційну систему машини, з якої передаються дані і точну інформацію про IP передачу через неї. Як згадано вище, спосіб генерації ідентифікаційних номерів для кожного наступного пакету залежить від реалізації стеку TCP/IP в операційній системі.

Якщо в подальшому етапі генерації послідовних значень поля ідентифікації дбати про те, щоб вони не залежать один від одного, і не буде статистичного аналізу для виявлення прихованих даних - сформований таким чином канал можна вважати відносно безпечним.

Якщо виявлена модифікація поля ідентифікації переданого пакету, атака на секретний канал набагато складніша, ніж у випадку поля ToS і вимагає більш трудомістких кроків. Не вистачає простої зміни ідентифікаційного номера, слід відслідковувати весь трафік в рамках даної передачі і повторно генерувати унікальні значення поля ідентифікації, забезпечуючи їх правильну відповідність для пакетів, які були фрагментовані.

Поле признаку фрагментації

В заголовку IP-пакету, після поля ідентифікації, є три біти признаку фрагментації, що визначають обробку датаграми маршрутизатором у випадку необхідності проведення дефрагментації і служать в якості інформації в тому випадку, коли фрагментація мала місце. Для цього використовуються два з трьох вказаних бітів. Найстаріший біт поля признаку фрагментації не використовується (це зарезервовано та часто називається *RF - Reserved Flag*), і завжди має нульове значення [2]. Однак, як показують проведені випробування, встановлення цього біта не впливає на те, як обробляються датаграми маршрутизаторами (значення цього біта не перевіряється). Таким чином, для передачі даних можна було б використовувати невикористаний біт фрагментації. Це стосується попередніх зауважень щодо виявлення та переривання прихованої передачі. Так само, як і в випадку поля ToS, викривання наявності прихованих даних є простим (в разі установки біта) і його видалення зводиться до послідовного обнулення найвищого біту фрагментації.

Поле опцій

Поле опцій в IP-пакеті може бути змінним по довжині і не використовується в більшості випадків. Деякі варіанти вважаються застарілими і не повинні використовуватися, оскільки вони були замінені іншими механізмами, а деякі з них дуже рідкісні.

Прийнятий метод поділу і варіантів нумерації залишає можливість визначити свої власні параметри IP, оскільки існування опцій дано за межами документу RFC, що описує IP [2]. Опція дозволяє створити не

використовувані до цього номери і пересиланні за їх допомогою даних. Потужність такого прихованого каналу коливається від одного біта на опцію (сигналізуючи наявність або відсутність даної опції) до декількох байтів у випадку опції з параметрами. Якщо застосована «власна» опція варіанту IP, цей обсяг обмежений тільки розміром даних, переданих датаграмою і максимальною транспортної одиниця (в мережах Ethernet 1500 байт).

Відправленим даним, що зберігаються в параметрах IP, не загрожує видалення відповідним чином налаштованих маршрутизаторів. Параметри з поза меж RFC не будуть інтерпретовані або змінені, пристрій обробки даних залишить їх без змін. Наявність таких варіантів не є порушення визначення RFC і протоколу (на відміну від методів з використанням «зарезервованого», невикористовуваного поля заголовку), тому не буде викликати тривогу, якщо пріоритетом аналізу трансляції будуть неправильні (ті, що не відповідають RFC) IP-датаграми, хоча можуть бути причиною для більш детального аналізу даної передачі.

Протокол TCP

Початковий номер послідовності

Невід'ємною частиною транспортного протоколу TCP є концепція тристороннього трафіку, механізм, який використовується для запуску TCP-з'єднання. Початковий номер послідовності (*ang. Initial Sequence Number, ISN*), обраний на самому початку з'єднання, розміщується в першому сегменті, який надсилається стороною, що нав'язує з'єдннання TCP. Значення ISN є випадковим, воно повинно бути змінено незалежно від існуючих (нав'язаних) з'єднань [3] таким чином, що їх неможливо передбачити статистично. У існуючих реалізаціях стеків TCP/IP основний акцент робиться на останньому, щоб протидіяти атакам, спрямованим на захоплення сеансу та підробки [4], [5].

Крім початкового номеру немає необхідності унікальності для ISN в інших з'єднаннях. Він використовується лише один раз під час підключення. Тому, враховуючи повну випадковість цього поля, можна використати його для відправки прихованих даних один раз. Поле ISN у заголовку сегмента TCP становить 32 біти, тому можна одночасно надсилати до 4 байтів даних. Недоліком цього рішення є те, що в останній частині передачі не можуть бути приховані дані, але може виявитися корисним в разі одночасної передачі декількох з'єднань для передачі даних. Прикладом цього може бути операція протоколу HTTP на рівні додатку – перегляд веб-сторінок, багатих графічними елементами призводить до відкриття кількох з'єднань TCP, по одному для кожного з переданого ресурсу (HTML, стиль CSS листа, зображення, звуки і т.д.).

Виявлення прихованої передачі через початковий послідовний номер важке. Необхідно контролювати всі TCP-з'єднання та здійснювати ISN-аналіз для кожного з'єднання. Запобігати прихованій передачі, без переривання відповідного TCP-з'єднання, вимагає використання проксі-технологій для

всіх з'єднань, які можуть бути носіями прихованих даних. Це обтяжливо і може вимагати (залежно від інтенсивності передачі) значних ресурсів для виконання цих функцій.

Зарезервоване поле

5-бітове поле, зарезервоване в заголовку сегмента TCP, відповідно до документа RFC, що визначає протокол [3], завжди має значення нуль. Це поле в даний час не використовується, хоча існують різні ідеї щодо його використання. Прикладом є RFC 3168 [6], в якому запропоновано використання двох наймолодших бітів цього поля для підтримки механізмів запобігання блокадам.

Так само, як у випадку невикористовуваних бітів поля ToS і зарезервовані біти фрагментації заголовка датаграми IP, так і у випадку зарезервованого поля його можна використати для передачі. Як випливає з експериментів, воно ігнорується в існуючих мережах, а сегменти TCP із значенням цього поля, яке відрізняється від нуля, надсилаються без будь-яких проблем.

Як і в попередніх випадках (поле ToS і біти RF) виявлення і запобігання прихованій передачі відносно просте і не представляє серйозних проблем в реалізації (просто скинути «підозрілий» пакет, що не змінює обробку пакета маршрутизаторами).

Слід зазначити, що в деяких випадках існує ризик того, що маршрутизатори відхилятимуть TCP-пакети з ненульвим резервним полем. Ця поведінка не відповідає RFC 793 [3], але іноді це може статися.

Індикація важливості

У заголовку сегмента TCP є 16-бітове поле, яке називається Покажчиком важливості (*ang. Urgent Pointer*). В даний час воно використовується дуже рідко, не спостерігається в трафіку TCP пакети, що мають встановлене значення цього поля. Відповідно до визначення протоколу [3], це поле застосовується тільки тоді, коли біт URG встановлений у заголовку сегмента TCP. Концепція використання цих 16 бітів (як правило, невикористаних) для передачі прихованих даних полягає в тому, щоб записати передане значення у поле важливості, одночасно залишаючи нульовим біт URG. Тоді доказ важливості не буде інтерпретований. Пакети з таким модифікованим заголовком (невірні з точки зору відповідності RFC) – як показано в експериментах, надходять без перешкод.

Потужність прихованого каналу, отриманого таким способом, теоретично становить 2 байти, але його все одно варто обмежити. Як згадувалося, поле важливості є зміщенням, вказує на останній «дійсний» байт у сегменті та додано до послідовного номера, що містяться у заголовку сегмента TCP. Через обмеження розміру IP-датаграми до розміру, визначеного MTU, індекс не може бути занадто великим. У випадку мережі на основі протоколу Ethernet, значення MTU, як правило 1500 октетів. Таким чином, щоб значення, яке вписано в поле, було імовірним та надійним, має бути менше 1460 (1500 мінус мінімальні розміри заголовків IP та TCP).

Виявлення прихованої передачі через поле важливості не є надто складним. Перш за все, це поле, як уже згадувалося, використовується порівняно рідко, тому збереження його можна вважати винятковою ситуацією. По-друге, ніколи не повинно відрізнятись від нуля в сегменті з нульовим бітом URG. Таким чином, виявлення прихованого каналу полягає в тому, щоб спостерігати передачі та виловлювати сегменти без встановленого біту URG, а з індикатором важливості відмінним від нуля.

Поле опцій

В заголовку сегменту протоколу TCP розробники передбачили простір для опцій TCP, як і у випадку з протоколом IP. Однак у відмінності від IP опцій, опції TCP знаходять застосування і може містити, щонайменше, одну з трьох опцій: *Maximum Segment Size (MSS)*, *SACK-Permitted*, *No Operation*, які зазвичай надсилаються під час встановлення (нав'язування) TCP-з'єднання.

Також у випадку опцій TCP автори RFC, що визначає протокол, залишають можливість створювати власні параметри. Використовуючи цей факт, а також те, що багато параметрів TCP не використовується, можна спробувати використовувати поле опції TCP для передачі даних. Також у цьому випадку обмеженням розміру є лише максимальна довжина сегменту TCP, проте слід враховувати ризик зацікавленості пакетами, що містять «екзотичні» опції.

Кодування даних

Серед вищезазначених, потенційні приховані канали, що існують в заголовках IP та TCP, авторами вибрані два, найбільш перспективні та привабливі для програмної реалізації.

Використання каналів, що пропонують потужності один або кілька бітів (менше 8), недоцільно. Це пов'язано з труднощами, які виникатимуть під час читання даних, що надсилаються в пункт призначення. Оскільки призначення стегосистеми – надсилання коротких текстових повідомлень, в результаті ми повинні перетворити отримані дані в 8-бітні символи. Оскільки IP є протоколом без встановлення з'єднання, втрата одного або більше бітів (в цьому випадку мережа сильно часто завантажена) унеможливлює правильно зчитувати символ – один біт з датаграми.

Перед описом використаних каналів слід звернути увагу на проблему, важливу з точки зору безпеки прихованої передачі.

Передані дані (символи) не повинні передаватися у публічній формі. Якщо передача виявлена, звести до мінімуму шанси на читання перехоплених даних. Тому дані повинні бути зашифровані та досить ефективними, щоб не зламати шифр, наприклад, криптоаналізом з використанням статистики (аналіз частоти виникнення окремих символів) [7]. Таким чином, кожен символ має бути зашифрований незалежно один від одного. Це є суттєвою перешкодою використання вказаних каналів передачі у випадку значної частини втрат переданих датаграм. Крім того, передача даних одностороння, немає можливості повторно передавати втрачені символи. У випадку

кодування символу, який використовує значення попередніх символів, втрата одного символу в будь-який момент не дасть змоги прочитати всі символи, що слідують за ним. Кодування доцільно виконувати таким чином, щоб 8-бітний символ отримав 8-бітове закодоване значення. Цю величину потім передавати через прихований канал передачі.

Поле Ідентифікації в заголовку IP

З заголовку IP-датаграми було вибрано поле, яке пропонує прихований канал з найбільшою ємністю - 16-бітове полем ідентифікації. Для того, щоб забезпечити унікальність ідентифікаційного номера та його унікальності, дані використовуються тільки для старшого байта (вісім старших біт) поля ідентифікації, в той час як молодші байти випадкові.

В рамках цього каналу було використано два різні підходи:

1. передача 8 біт закодованого символу в одній датаграмі;

2. розділити 8-бітове значення на дві частини з 4 біт і відправити їх у дві послідовні датаграми.

Перший спосіб простий і полягає в кодуванні переданого символу і розміщенні восьми отриманих бітів у старшому байті поля ідентифікації.

Другий спосіб використовує лише чотири найстаріші біти для передачі символів. Решта чотири біти використовуються для відправлення наступних даних (по модулю 16), завдяки яким при отриманні їх можна відновити правильний порядок. Таким чином, було введено захист проти читання даних від датаграм, які досягли місця призначення в іншому порядку, ніж вони залишили джерело передачі. Це часто трапляється в IP-мережах у випадку сильно завантаженої мережі.

Роль визначення правильного порядку даних приймає транспортний протокол (у описаному випадку – TCP), але в реалізації прихованої передачі, використання його послуг не представляється можливим, оскільки читання прихованих даних відбувається на мережевому рівні моделі ISO/OSI, тому отримання пакетів передається на рівень TCP.

Індикація важливості в заголовку TCP

У заголовку сегмента TCP використовується поле важливості. Відповідно до зауважень, зроблених раніше, в це поле поміщається закодоване значення, в якому використовується тільки вісім наймолодших бітів поля, щоб невластиві з точки зору RFC поля були менш очевидні. Передане значення, як і у випадку використання поля ідентифікації, кодується.

Незважаючи на те, що спочатку був застосований прихований канал, що використовує поле ToS, ідею було зкомпроментовно. В ході тестування, з'ясувалося, що інтернет-провайдер вносить зміни в заголовках переданих IP-датаграм. Тому в цій мережі використання цього каналу неможливе.

Висновки

Таким чином, пошук можливостей використання заголовків IP та TCP для передачі прихованих даних не повинен обмежуватися лише одним

прихованим каналом. Після знаходження кількох різних методів існує можливість вибору та використання їх залежно від умов у конкретній мережі. Проте, не слід використовувати гібридну комбінацію з декількох полів заголовка, щоб створити канал більшої місткості - навіть якщо не всі, то частина може бути скинута за певних обставин, що призводить до повної неможливості використовувати такий канал.

1. *Кирик М. І., Плесканка Н. М., Тимченко О. В.* Методи та моделі управління трафіком в розподілених інфокомунікаційних системах: моногр. — Львів : Укр. акад. друкарства, 2017. — 264 с. (ISBN 978-966-322-473-2)
2. *Jon Postel*. Internet Protocol – DARPA Internet Program Protocol Specification. RFC 791, september 1981. // http://www.rfc-editor.org/ rfc/rfc791.txt.
3. *Jon Postel.* Transmission Control Protocol – DARPA Internet Program Protocol Specification. RFC 793, september 1981. // http://www.rfc-editor.org/rfc/rfc793.txt.
4. *Steven M. Bellovin*. Defending Against Sequence Number Attacks. RFC 1948, may 1996. // http://www.rfc-editor.org/rfc/rfc1948.txt.
5. *Jeffrey S. Havrilla*. CERT/CC Vulnerability Note VU#498440. Multiple TCP/IP implementations may use statistically predictable initial sequence numbers, marzec 2001. // http://www.kb.cert.org/vuls/id/498440.
6. *K. K. Ramakrishnan*. The Addition of Explicit Congestion Notification (ECN) to IP. RFC 3168, september 2001. // http://www.rfc-editor.org/rfc/rfc3168.txt.
7. *Ємець В., Мельник А., Попович Р.* Сучасна криптографія. Основні поняття. - Львів: БаК, 2003. - 144 с.

Поступила 24.09.2018р.

УДК 004.62

В.Р. Сподарик, НУ «Львівська політехніка»

ВИКОРИСТАННЯ МЕТОДУ ГЛИБИННОГО НАВЧАННЯ ПРИ РОЗРОБЦІ НАЙПРОСТІШИХ СИМУЛЬОВАНИХ ОРГАНІЗМІВ

Розглянуто проблему складності побудови штучних нейронних мереж. Описано з чого складаються, як вони функціонують та для чого можуть використовуватись. Розроблено і описано систему, яка моделює штучні нейрони, які можуть керувати мікроорганізмами у симульованому мікро-світі.

Ключові слова: штучні нейронні мережі, персептрон, функція активації, сигмоїд, глибинне навчання, нейрон.

I. Постановка проблеми

За останні кілька років, частота обговорень на тему алгоритмів машинного навчання, штучного інтелекту, штучних нейромереж та інших

