УДК 004.056.5 (045)

Труш О. В., к.т.н. (Державний університет телекомунікацій, +380 66 612 25 24, trush-viti@mail.ru)

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ IP-ТЕЛЕФОНІЇ ДЛЯ ПРИХОВАНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Труш О. В. Використання технологій IP-телефонії для прихованої передачі інформації. У статті порівнюються сучасні методи цифрової стеганографії, які використовують для вбудовування прихованої інформації потокові в контейнери, а саме: пакети передачі даних в реальному часі, застосовувані в IP-телефонії. Метою статті є висвітлення сучасних досягнень фахівців з використання IP- телефонії для прихованої передачі даних на великі відстані, які підтверджені проведеними експериментами. Аналіз останніх досліджень і публікацій з організації прихованих віртуальних каналів в телекомунікаційних мережах на базі стека протоколів TCP/IP показав, що в даний час цей напрям мало вивчено.

Ключові слова: IP-телефонія, передача даних, стеганографія, потоковий контейнер, прихований віртуальний канал, прихована передача інформації, стеганоаналіз, VoIP

Труш А. В. Использование технологий IP-телефонии для скрытой передачи информации. В статье сравниваются современные методы цифровой стеганографии, которые используют для встраивания скрытой информации в потоковые контейнеры, а именно: пакеты передачи данных в реальном времени, применяемые в IP - телефонии. Целью статьи является освещение современных достижений специалистов по использованию IP- телефонии для скрытой передачи данных на большие расстояния, которые подтверждены проведенными экспериментами. Анализ последних исследований и публикаций по организации скрытых виртуальных каналов в телекоммуникационных сетях на базе стека протоколов TCP / IP показал, что в настоящее время это направление мало изучено.

Ключевые слова: IP-телефония, передача данных, стеганография, потоковый контейнер, скрытый виртуальный канал, скрытая передача информации, стеганоанализ, VoIP

Trush O. V. Use of IP-telephony technologies for the secure data transmission. In this article it was made a comparison between the modern digital steganography methods which are used to insert hidden information into the flow containers, namely the data packets in real time used in IP- telephony. The aim of the paper is to highlight the present-day achievements of the experts related to the IP- telephony use for a hidden data transfer over long distances which were proved by the conducted experiments. The recent researches and publications analysis related to the provisioning of hidden virtual circuits in the telecommunication networks based on the TCP/IP protocols stack show that at present this area is studied insufficiently.

Keywords: IP-telephony, data transmission, stegonography, flow containers, methods of , containers,hidden virtual circuits, hidden transmission of data,steganalysis, VoIP

Вступ. Постановка задачі. Хоча методи стеганографії відомі вже багато століть, в наш час, завдяки розвитку комп'ютерної техніки і телекомунікаційних технологій, отримав стрімкий розвиток новий вид прихованої передачі даних – цифрова стеганографія.

Нагадаємо, що стеганографія – це наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі. Цифрова стеганографія ґрунтується на прихованої імплантації додаткової інформації в цифрові об'єкти (як правило, мультимедійні файли – цифрові зображення, відео, аудіо). При цьому відбувається деяке спотворення цих об'єктів, але на рівні, що знаходиться нижче межі сприйняття людиною, яке не призводить до помітних змін цих об'єктів і ускладнює їх викриття.

З розвитком і вдосконаленням технологій передачі інформації комп'ютерними мережами, з'являються нові різноманітні методи непомітної передачі інформації. Це відкриває великі перспективи для тих, хто хоче непомітно передавати повідомлення через будь-які кордони і створює небезпеку для установ, що займаються захистом інформації від несанкціонованого витоку.

Метою статті є висвітлення сучасних досягнень фахівців з використання IP-телефонії для прихованої передачі даних на великі відстані, які підтверджені проведеними експериментами. Аналіз останніх досліджень і публікацій з організації прихованих віртуальних каналів в телекомунікаційних мережах на базі стека протоколів TCP/IP показав, що в даний час цей напрям мало вивчено.

IP-телефонія, як прихований носій інформації, був виявлений дослідниками досить пізно. Ці методи стеганографії були розроблені з двох різних за походженням досліджень: *по-перше,* з традиційних графічних і звукових стеганографічних контейнерів; *по-друге,* з прихованих каналів, створених у різних мережевих протоколах (наприклад, протокол сигналізації SIP, транспортний протокол RTP та протокол управління RTCP) [1].

Перші стеганографічні VoIP методи, які використовували голосовий потік як прихований носій інформації були запропоновані ще в 2005 році. Була запропонована оцінка існуючої стеганографії з особливим акцентом на рішеннях, які підходять для VoIP, та описаний інструмент SteganRTP для вбудовування стеганограм, використовуючи молодший біт (LSB) з кодека G.711.

Ванг (Wang) і By (Wu) в роботі «Інформація, прихована в VoIP потоках» також запропонували використовувати молодші біти, але ці біти кодувалися з використанням кодека Speex. Запропонований аналогічний підхід, створивши прихований канал шляхом вбудовування та подальшого стиснення голосових даних у звичайному голосовому трафіку, заснований на імпульсно-кодовій модуляції. Проблеми використання потокових стеганографічних контейнерів, зокрема протоколів IP-телефонії, найбільш досліджені були фахівцями з проблем мережевої безпеки Варшавського Технологічного Університету Войцехом Мазурчеком і Кжиштофом Джіпйорским, які провели ряд експериментів з використання VoIP сервісів для передачі таємних повідомлень, про що вони доповіли на четвертій міжнародній конференції з питань глобальної електронної безпеки в Лондоні [1, 2].

При застосуванні стеганографічних методів, об'єкт, в якому міститься приховане повідомлення, називається "стеганографічним контейнером". Контейнери поділяються на фіксовані і потокові. Особливістю потокового контейнера є те, що неможливо визначити його початок або кінець. Більш того, немає можливості дізнатися заздалегідь, якими будуть наступні шумові біти, що призводить до необхідності включати біти прихованого повідомлення у потік в реальному масштабі часу, а самі приховані біти вибираються за допомогою спеціального генератора, що задає відстань між послідовними бітами у потоку. У безперервному потоку даних найбільша складність для одержувача – визначити, коли починається приховане повідомлення. При наявності в потоковому контейнері сигналів синхронізації або меж пакета, приховане повідомлення починається відразу після одного з них. У свою чергу, для відправника можливі проблеми, якщо він не впевнений у тому, що потік контейнера буде досить довгим для розміщення цілого таємного повідомлення.

Мережна стеганографія. Останнім часом набули популярності методи, коли прихована інформація передається через комп'ютерні мережі з використанням особливостей роботи протоколів передачі даних. Такі методи одержали назву «мережна стеганографія». Цей термін вперше ввів Кжиштофом Джіпйорский в 2005 році. Типові методи мережевої стеганографії включають зміну властивостей одного з мережевих протоколів. Крім того, може використовуватися взаємозв'язок між двома або більше різними протоколами з метою більш надійного приховування передачі таємного повідомлення.

Мережева стеганографія охоплює широкий спектр методів, зокрема:

– WLAN стеганографія грунтується на методах, які використовуються для передачі стеганограм в бездротових мережах (Wireless Local Area Networks). Практичний приклад WLAN стеганографії – система HICCUPS (Hidden Communication System for Corrupted Networks);

– LACK стеганографія – приховування повідомлень під час розмов з використанням IP-телефонії. Наприклад: використання пакетів, які затримуються, або навмисно пошкоджуються й ігноруються приймачем (цей метод називають LACK – Lost Audio Packets Steganography) або приховування інформації в полях заголовків, які не використовуються;

– VoIP (англ. Voice over IP) – технологія передачі медіа даних в реальному часі за допомогою протоколів TCP/IP. IP-телефонія – система зв'язку, при якій аналоговий звуковий сигнал від одного абонента дискретизується (кодується в цифровий вигляд), компресується і

пересилається по цифровому каналу зв'язку іншому абоненту, де проводиться зворотня операція – декомпресія, декодування і відтворення. Розмова відбувається у формі аудіо-потоків, за допомогою протоколів RTP (Real-Time Transport Protocol);

LACK – це метод стеганографії для IP-телефонії, який модифікує пакети з голосовим потоком. Він використовується в типових мультимедійних комунікаційних протоколах, таких як RTP. Надмірно затримані пакети вважаються приймачем втраченими і відкидаються.

Принцип дії методу LACK виглядає наступним чином (Рис. 1). Передавач вибирає один з пакетів голосового потоку і його корисне навантаження замінюється бітами таємного повідомлення – стеганограмою, яка вбудовується в пакет V3 (1). Потім вибраний пакет навмисно затримується (2). Кожен раз, коли надмірно затриманий пакет досягає одержувача, незнайомого з стеганографічною процедурою, він відкидається. Однак, якщо одержувач знає про приховану зв'язку, то замість видалення отриманих RTP пакетів, він витягує приховану інформацію [3].

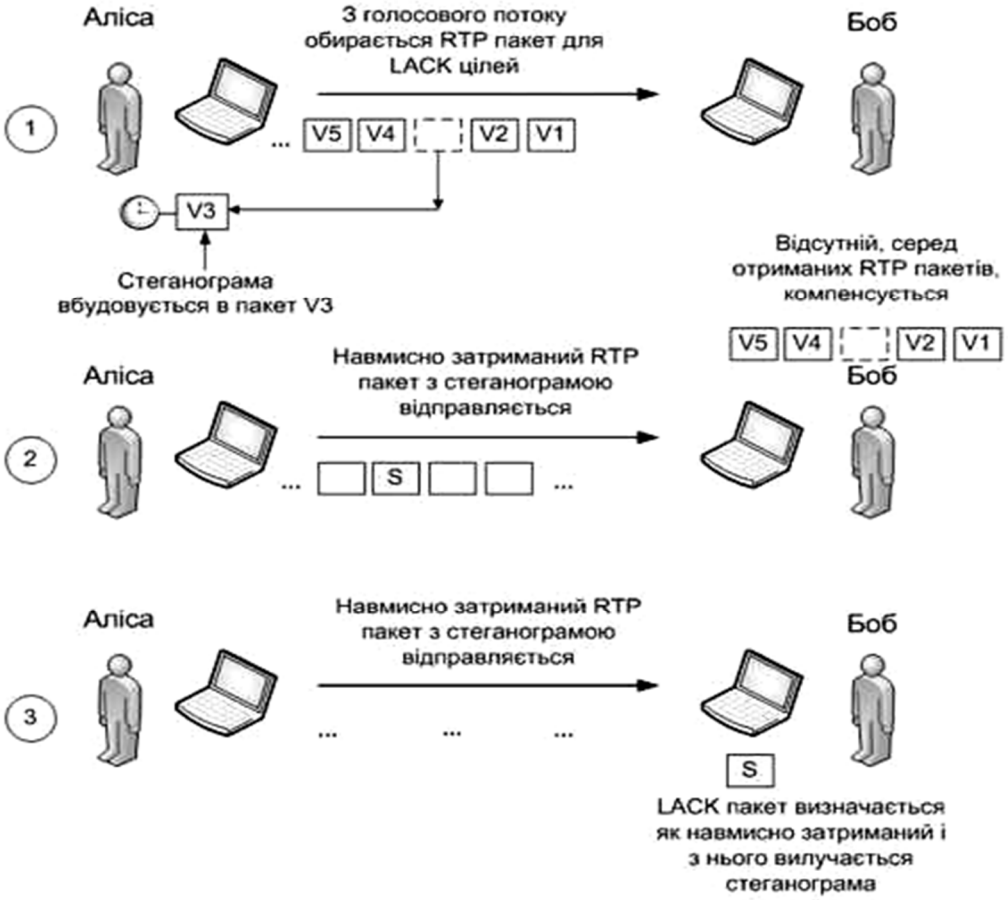

Рис. 1. Принцип функціонування LACK

Пропускна здатність цього методу дозволяє передавати до 1.3 Mb інформації за один сеанс зв'язку тривалістю близько 9 хвилин (середня тривалість викликів IP-телефонії) в обох напрямках.

Чим більше прихованої інформації вставляється в голосовий потік, тим більша вірогідність того, що вона буде виявлена скануванням потоку даних або застосуванням інших методів стеганоаналізу. Також, чим більше аудіо пакетів використовуються для вбудовування стеганограм, тим більше погіршення якості зв'язку IP-телефонії. Таким чином, процедура запровадження прихованих даних повинна бути ретельно підібрана і контролюватися, з метою зведення до мінімуму ймовірності виявлення замаскованих даних, а також для уникнення надмірного погіршення якості звуку.

Експериментальні дослідження методу LACK. Продуктивність LACK залежить від багатьох факторів, які можуть бути розділені на три наступні групи:

– пов'язані фактори: тип кодека голосу, який використовується (зокрема, його стійкість до втрат пакетів і якість голосу за замовчуванням), розмір корисного навантаження RTP пакетів і розмір джіттер – буферу;

– мережеві фактори, пов'язані із затримками пакетів і ймовірністю втрат;

– LACK фактори, пов'язані з кількістю навмисно затриманих пакетів RTP.

Кращим вибором для LACK методу в процесі експериментів виявився кодек G.711. Він може підтримувати втрати пакетів більше 5 % і при цьому забезпечити прийнятну якість голосу. Одночасно, на основі G.711 LACK забезпечує найбільші стеганографічні пропускні спроможності. Наприклад, при втраті пакетів на рівні 1% він забезпечує швидкість передачі близько 590 біт/с.

Така продуктивність досягається тим, що розмір корисного навантаження кожного пакету RTP становить 160 байт, що значно більше, ніж при використанні будь-якого іншого обраного кодека. Порівняння швидкості передачі стеганограми різними кодеками, залежно від втрати пакетів, наведені на Рис. 2 [4].

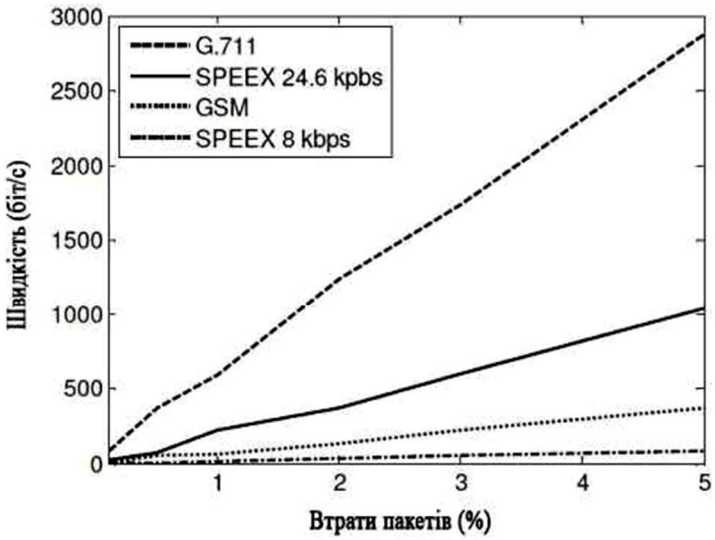

Рис. 2. Порівняння швидкості LACK залежно від методів кодування

Стеганоаналіз LACK важко виконати, оскільки втрати пакетів в IP-мережах "природне явище". Така ситуація може бути викликана, наприклад, переповненням буферу деякого проміжного пристрою, завдяки вузькому місцю в мережі. Результати дослідження показали, що при виконанні інтернет-дзвінків, близько 0,5 % пакетів RTP губляться і близько 2 % викликів призводять до переповнення буферу. Таким чином, втрати від застосування LACK нелегко виявити, якщо вони перебувати на прийнятному рівні.

Потенційні методи стеганоаналізу LACK включають в себе:

– *Статистичний аналіз втрачених пакетів для дзвінків в підмережі*. Цей тип може бути заснованим, наприклад, для інформації, яка міститься у звітах RTCP про загальну кількість втрачених пакетів при обміні між користувачами. Якщо для деяких викликів кількість втрачених пакетів вище середнього, цей критерій може бути використаний як вказівка на можливість застосування LACK.

– *Статистичний аналіз, заснований на тривалості VoIP дзвінків*. Якщо тривалість дзвінків для певної підмережі відома, то статистичний стегоаналіз може виявити VoIP джерела, які виходять за певні межі (тривалість LACK викликів може бути більше в порівнянні з не LACK викликами в результаті введення стеганографічних даних);

– *Активне спостереження*. Аналіз всіх RTP потоків в мережі може допомогти ідентифікувати пакети, які надто довго були затримані [5, 6]. Це новий вид цифрової стеганографії, який ще тільки розробляється, знаходиться на стадії експериментів і впровадження.

Поки не можна сказати напевно, чи буде задовольною надійність і швидкість передачі прихованих даних за допомогою RTP протоколів, чи буде потреба в сталому використанні цієї технології. Але сама ідея, запропонована фахівцями з Польщі, є досить цікавою. Незважаючи на те, що ними була зроблена доповідь на міжнародній конференції в Лондоні, в нашій країні досить мало публікацій, які б узагальнили і висвітлили цю перспективну тему.

Вже з'являються в пресі припущення, що саме таким чином деякі терористичні угруповання намагаються передавати один одному матеріали, залишаючи сам факт спілкування в таємниці. Популярність голосових розмов в Інтернеті призводить до безперервного росту обсягів трафіку VoIP. Наприклад, за даними дослідницької компанії TeleGeography, на кінець 2012 року програмою для IP-телефонії Skype користуються до 240 мільйонів чоловік по всьому світу. Тому слід очікувати, що будуть стрімко розвиватися і стеганографічні методи, які використовують ці канали для прихованої передачі інформації [7].

Висновки. Аналіз тенденцій розвитку комп'ютерної стеганографії (КС) показує , що в найближчі роки інтерес до розвитку методів КС буде посилюватися все більше і більше. Передумови до цього вже сформувалися сьогодні . Зокрема , загальновідомо , що актуальність проблеми інформаційної безпеки постійно зростає і стимулює пошук нових методів захисту інформації. З іншого боку, бурхливий розвиток інформаційних технологій забезпечує можливість реалізації цих нових методів захисту інформації. І, звичайно сильним каталізатором цього процесу є лавиноподібний розвиток комп'ютерної мережі загального користування, в тому числі такі невирішені суперечливі проблеми Інтернет, як захист авторського права, захист прав на особисту таємницю, організація електронної торгівлі, протиправна діяльність хакерів і т.п.

Дуже характерною тенденцією в даний час в області захисту інформації є впровадження криптографічних методів. Однак на цьому шляху багато ще невирішених проблем , пов'язаних з руйнівним впливом на криптозасоби таких складових інформаційної зброї як комп'ютерні віруси, логічні бомби, автономні реплікативні програми і т.п. Об'єднання методів комп'ютерної стеганографії та криптографії з'явилося б хорошим виходом із ситуації. У цьому випадку вдалося б усунути слабкі сторони відомих методів захисту інформації та розробити більш ефективні нові нетрадиційні методи забезпечення інформаційної безпеки.

Література

1. Mazurczyk W. On Steganography in Lost Audio Packets [Електронний ресурс] / Wojciech Mazurczyk, Jozef Lubacz, Krzysztof Szczypiorski // Warsaw University of Technology – Режим доступу: http://arxiv.org/ftp/arxiv/papers/1102/1102.0023.pdf

2. Mazurczyk W. LACK – a VoIP steganographic method [Електронний ресурс] / Mazurczyk Wojciech, Lubacz Jozef//Warsaw University of Technology – Режим доступу: http://cygnus.tele.pw.edu.pl/~wmazurczyk/art/LACK_journal_final.pdf

3. Thurston R. Steganography developers turn their attention to hiding information in VoIP. [Електронний ресурс] / Richard Thurston // SC MAGAZINE – Режим доступу: http://www.scmagazineuk.com/steganography-developers-turn-their-attention-to-hiding-information-in-voip/article/112102/.

4. Генне О. В. Основные положения стеганографии [Електронний ресурс] / О. В. Генне // Защита информации. Конфидент. – 2008. – № 3. – 10 с. – Режим доступу : http://www.citforum.ru/internet/securities/stegano.shtml

5. Орлов В. В. Методы скрытой передачи информации в телекоммуникационных сетях: / В. В.Орлов. – Самара, 2012. – 209 с.

6. Яремчук Ю. Є. Оцінювання обчислювальної складності протоколів шифрування без посереднього розподілу ключів на основі рекурентних послідовностей / Ю. Є. Яремчук, С. В. Толюпа // Вісник Державного університету інформаційно-комунікаційних технологій. – 2013. – №2 – С. 69-77.

7. Гулак Г. М. Забезпечення безпеки програмних засобів криптографічного захисту інформації та оцінка її рівня / Г. М. Гулак // Сучасний захист інформації. – 2010. – № 2. – С. 42-48.