Основні аспекти використання протоколу TCP в мережевій стеганографії

Матвієнко Ю.С.
к.п.н., доцент кафедри математичного аналізу
та інформатики ПНПУ імені В.Г. Короленка
wasilews2009@gmail.com

Стеганографія – це наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі. Відмінною особливістю стеганографії у порівнянні з криптографією є те, що стеганографія не приховує зміст повідомлення, а приховує сам факт його передачі. При цьому контейнером для повідомлення може бути, наприклад, зображення, відеофайл або аудіофайл. Можна використовувати стеганографію в комплексі з криптографією для додаткового захисту даних.

Останнім часом набули популярності методи, коли прихована інформація передається через комп'ютерні мережі з використанням особливостей роботи протоколів передачі даних. Такі методи отримали назву «мережева стеганографія» [1]. Цей термін вперше ввів Кжіштоф Шчіпйорскі (Krzysztof Szczypiorski) в 2003 році. Типові методи мережевої стеганографії передбачають зміну властивостей одного з мережевих протоколів. Крім того, може використовуватися взаємозв'язок між двома або більше різними протоколами з метою більш надійного приховування передачі секретного повідомлення [1, 2].

Інтернет відкрив масу можливостей для прихованого зв'язку. Секретні повідомлення можуть бути приховані не лише в звичайних відкритих повідомленнях, як в традиційній стеганографії, а також в елементах управління протоколів зв'язку і в результатах зміни логіки протоколу. В Інтернет стеганографія може застосовуватися для досягнення найрізноманітніших цілей – починаючи від цілком безпечних і навіть корисних, і закінчуючи злочинними. Зокрема, одне з найбільш затребуваних незлочинних стеганографічних застосувань – захист авторського права, коли за допомогою впровадженого «водяного знаку »можна довести авторство матеріалів.

Стеганографічну систему можна використовувати для цифрового маркування матеріалів в електронних бібліотеках і сховищах. Стеганографічні вкладення можуть в деякій мірі підмінити собою електронну пошту, бо дозволяє довести цілісність переданого матеріалу. А з іншого боку, за допомогою стеганографії інсайдер може передати через канали Інтернет закриті дані, обходячи всі фільтри, встановлені в мережі організації. Стеганографія може використовуватися для приховування факту передачі заборонених матеріалів і для спілкування злочинців і

терористів. Тому методи стеганографії і стегоаналізу вимагають особливо ретельного вивчення.

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) [2]. В основі цих методів, лежать властиві бездротовим мережам недоліки, які можуть викликати невиправні спотворення в енергетичних характеристиках сигналів, що транслюються. В результаті можуть з'являтися «неправильні» пакети (пакети, контрольна сума яких не відповідає заявленій в заголовку сегмента транспортного рівня). Для реалізації такого роду методів, необхідно мати актуальну статистику мережевої активності в середовищі, що використовується, щоб не викликати аномальну мережеву активність.

– *LACK (Lost Audio Packets Steganography) стеганографія* – приховування повідомлень під час розмов з використанням IP-телефонії. Наприклад: використання пакетів, які затримуються, або навмисно пошкоджуються і ігноруються приймачем (прикладною програмою), але не стеганографічним додатком [3].

У зв'язку з тим, що найпоширенішим в мережі Інтернет є стек протоколів TCP / IP, то доцільним є організація стеганографічних каналів (СГК) саме на його основі.

TCP – це протокол транспортного рівня (тобто працює «над» IP і «під» протоколами рівня додатків, наприклад HTTP, FTP або SMTP), який забезпечує надійну доставку даних від відправника до одержувача. Надійна доставка означає, що якщо якийсь пакет загубився або прийшов із змінами, то TCP подбає про те, щоб переслати цей пакет. Відзначимо, що під змінами в пакеті тут розуміється не навмисне перекручування даних, а помилки в передачі, які виникають на фізичному рівні. Наприклад, поки пакет йшов по мідних дротах пару біт поміняли своє значення на протилежне або взагалі загубилися серед шуму (до речі для Ethernet значення Bit Error Rate зазвичай приймають рівним порядку 10-8). Втрата пакетів в дорозі також відносно часте явище в інтернеті. Відбуватися вона може, наприклад, через завантаженість маршрутизаторів, яка призводить до переповнення буферів і як наслідок відкинути всіх пакетів, які знову надходять. Зазвичай частка втрачених пакетів становить близько 0.1%, а при значенні в пару відсотків TCP взагалі перестає нормально працювати.

Таким чином ми бачимо, що ретрансмісія пакетів явище для TCP часте і в цілому потрібне. Так чому б не використати його для потреб стеганографії при тому що TCP, як вже зазначалося вище, використовується повсюдно (за різними оцінками на сьогоднішній день частка TCP в інтернеті досягає 80-95%). Суть запропонованого методу полягає в тому, щоб в повідомленні, що пересилається, відправляти не те, що було в первинному пакеті, а ті дані, які ми намагаємося

приховати. При цьому виявити таку підміну не так-то просто. Адже потрібно знати куди дивитися – кількість одночасних з'єднань TCP, що проходять через провайдера просто величезна. Якщо знати приблизний рівень ретрансмісії в мережі, то можна підлаштувати механізм стеганографічної пересилки так, що ваше з'єднання нічим не буде відрізнятися від інших.

Вперше використання TCP-сегментів і механізму RTO для передачі стенографічних повідомлень було запропоновано вченими з Варшавського університету в роботі «Retransmission steganography and its detection »у 2009 році [4]. Механізм RTO (Retransmission Timeout) передбачає повторну відправку пакетів, які були пошкоджені або загублені.

Для відстеження втрати пакетів використовується метод обробки помилок ARQ (Automatic repeat request). Коли TCP передає сегмент, що містить дані, він поміщає його копію в чергу повторної передачі і запускає таймер. При отриманні підтвердження для даного сегмента він вилучається з черги. Якщо підтвердження не отримане до закінчення дії таймера, сегмент відправляється повторно.

Звичайно цей метод не позбавлений недоліків. Наприклад, з практичної точки зору впровадити його буде не так-то просто – це потребуватиме зміни мережевого стека в операційних системах, хоча і вкрай складного в цьому нічого немає. Крім того, за наявності достатньої кількості ресурсів все одно можна виявити «таємні» пакети, для цього потрібно переглядати та аналізувати кожен пакет в мережі. Але як правило це практично неможливо, тому зазвичай шукають пакети, що чимось виділяються і з'єднання, а запропонований метод якраз і робить ваше з'єднання нічим не примітним. Та й ніхто не заважає зашифрувати таємні дані про всяк випадок. При цьому саме з'єднання може залишатися незашифрованим, щоб викликати менше підозр. При модифікації протоколу важливо зберігати його функціональність, щоб не відбувалося втрати пакетів. Втратою стеганографічних пакетів на початковій стадії можна знехтувати.

Список використаних джерел

1. Wojciech Mazurczyk, Krzysztof Szczypiorski, Steganography of VoIP Streams, Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications, 15/19 Nowowiejska Str., 00-665 Warsaw, Poland.

2. Krzysztof Szczypiorski, HICCUPS: Hidden Communication System for Corrupted Networks, Warsaw University of Technology, Institute of Telecommunications, ul. Nowowiejska 15/19, 00-665 Warsaw, Poland.

3. TelecommunSyst. – DOI 10.1007/s11235-009-9245-y. LACK—a VoIP steganographic method. WojciechMazurczyk JózefLubacz.

4. Mazurczyk W., Smolarczyk M., Szczypiorski K. Retransmission Steganography Applied, Poland: Warsaw University of Technology , 2010.