Выводы

Замена группы выходных отверстий вскрытых на боковой поверхности раздаточного трубопровода эквивалентным отверстием приводит к погрешности гидравлического расчёта, которая возрастает с увеличением количества заменяемых выходных отверстий и уменьшается с увеличением перепада давлений воздуха на выходных отверстиях.

Количество воздуха вытекающего из раздаточного трубопровода при эквивалентировании выходных отверстий уменьшается.

1. *Альтшуль А. Д.* Гидравлические сопротивления. – 2-е изд. перераб. и доп. М., Недра, 1982, с 224.
2. *Батурин В. В.* Основы промышленной вентиляции. – М.: 1 – я типография Профиздата, 1956. – 528 с.
3. *Баулин К. К.* Исследование равномерной раздачи воздуха из прямых трубопроводов. – Отопление и вентиляция, № 7, 1934.
4. *Быстров П. И.*, *Михайлов В. С.* Гидро – динамика коллекторных тепло – обменных аппаратов//М. 1982 г. 223 с.
5. *Гримитлин М. И.* Гидравлический расчёт, приточных перфорированных трубопроводов на заданную степень равномерности раздачи// Промышленная энергетика, труды ЛИОТ 1958г.
6. *Идельчик И. Е.* Справочник по гидравлическим сопротивлениям// Под ред. М. О. Штейнберга. – 3-е изд., перераб. доп. – М.: Машиностроение, 1992 г. – 672 с.:ил.
7. *Талиев В. Н.* Аэродинамика вентиляции. – М.:Стройиздат, 1979.–295 с.
8. *Ханжонков В. И.* Сопротивление истечению через отверстия в стенке в присутствии проходящего потока//Промышленная аэродинамика. М., ЦАГИ, 1959 г. № 15 с. 5 – 19.

Поступила 19.03.2014р.

УДК 004.056.5

А.Ю.Головін, ІСЗЗІ НТУУ «КПІ»

МЕТОДИ ВИЯВЛЕННЯ ПРИХОВАНИХ КАНАЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Анотація. У статті розглянуто методи виявлення і протидії прихованим каналам витоку та передачі інформації в комп'ютерних мережах. Розглянуто статистичний метод, застосування штучних нейронних мереж, метод опорних векторів, система «процес-подія», метод нормалізації та поведінкового аналізу трафіку. Наведено переваги та недоліки кожного методу.

Аннотация. В статье рассмотрены методы обнаружения и противодействия скрытым каналам утечки и передачи информации в компьютерных сетях. Рассмотрены статистический метод, использование искусственных нейронных сетей, метод опорных векторов, система «процесс-

событие», методы нормализации и поведенческого анализа трафика. Показаны преимущества и недостатки каждого метода.

Ключові слова: прихований канал передачі інформації, TCP, IP, статистичний метод, штучні нейронні мережі, метод опорних векторів, система «процес-подія», нормалізатори трафіку, поведінковий аналіз.

Постановка проблеми. У результаті значного поширення телекомунікаційних мереж у всі сфери діяльності організацій і держаних інституцій різних рівнів для мережевих адміністраторів та фахівців із захисту інформації постає задача захисту конфіденційної інформації та виявлення спроб її несанкціонованої передачі. За матеріалами дослідження компанії InfoWatch [1] за 2012-2013 роки є стійка тенденція до зростання кількості зареєстрованих фактів витоку конфіденційної інформації із органів державної влади та комерційних організацій. У 2013 році значно зросла (у 2 рази порівняно із 2012 р.) частка витоку конфіденційної інформації через мережу.

Виклад основного матеріалу.

На рис. 1 схематично зображено класифікацію прихованих каналів за такими ознаками і характеристиками: механізм створення і передачі інформації, пропускна здатність, спосіб перетворення інформації, використання рівнів інформаційної моделі *OSI*, характеристики інформаційного потоку та механізм використання каналу.

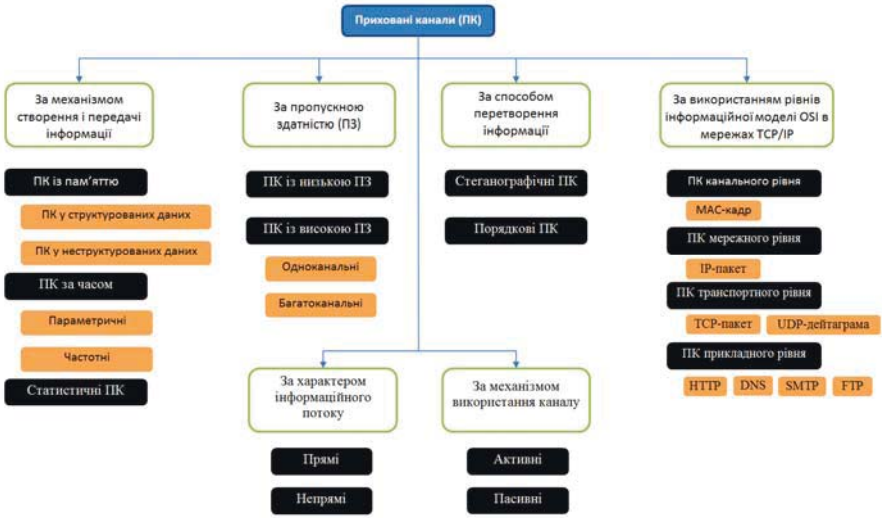

Рис. 1. Класифікація прихованих каналів

На практиці для організації несанкціонованої передачі інформації програмними засобами створюється прихований канал двох узагальнених типів: *за часом (timing covert channel)* та *із пам'яттю (storage covert channel).*

Для організації прихованого каналу із пам'яттю необхідно реалізувати

процедуру внесення змін в пакет даних (або у заголовок пакету, в залежності від реалізації), для чого потрібні адміністративні привілеї користувача в системі.

Приховані канали за часом реалізовуються на рівні ядра операційної системи (шляхом написання відповідного модулю).

Більшість прихованих каналів передачі інформації із пам'яттю достатньо просто реалізовуються на мові програмування високого рівня, але навіть найпростіший прихований канал досить складно виявити без використання спеціальних методів. Розглянемо далі методи виявлення прихованих каналів передачі інформації в телекомунікаційних мережах.

Простий аналіз трафіку

Деякі приховані канали виявляються шляхом простого аналізу мережевих пакетів. На рис. 2 схематично зображено заголовки *IP*- та *TCP*-пакетів, рамкою обведено поля заголовків які можливо використати для прихованої передачі інформації.

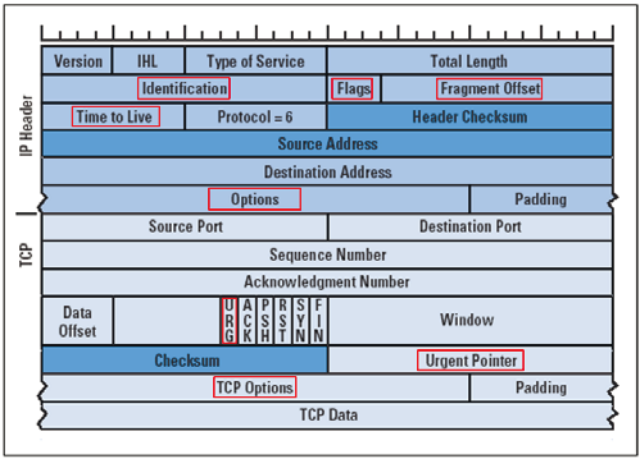

Рис. 2. Заголовки IP- та TCP-пакетів

Наприклад, простим аналізом пакетів можливо виявити приховану передачу інформації якщо відсутній прапорець *URG TCP*-пакета, але поле *Urgent Pointer* не порожнє. Так само виявляється використання поля *Fragment Offset* при відсутній фрагментації пакетів.

В різних операційних системах алгоритми генерації поля *Identification* є різними. Одні реалізують глобальне зростання значення *Identification*, інші використовують незалежні лічильники для кожного з'єднання. Значення поля *Identification*, які не відповідають цим алгоритмам вказують на наявність прихованого каналу.

Також ознаками наявності прихованого каналу можуть бути неіснуючі опції у полі *Options IP*- та *TCP*-пакетів, різні значення полю *TTL*, або

ненульовий відступ (*Padding*). Прихований канал передачі інформації, який ігнорує наведені правила і алгоритми досить легко виявляється.

Ймовірністно-статистичний аналіз

Приховані канали із пам'яттю.

Згідно стандарту *RFC-793* поле *SN TCP*-пакета повинне мати випадкове значення. У разі використання поля *SN* для кодування інформації *у* прихованому каналі, накопичивши певний обсяг статистичної інформації, за допомогою ймовірністно-статистичного аналізу можливо виявити факт того, що випадкові значення генеруються лише в межах певної підмножини.

Приховані канали за часом.

Ймовірністно-статистичний аналіз затримок між пакетами дає змогу визначити інтервали часу для кодування логічної одиниці і логічного нуля поміж нормального розподілу значень часових затримок. У разі накопичення достатньо великого обсягу статистичної інформації (головна вимога роботи методу) детектуванню підлягають також приховані канали із застосуванням механізму сортування пакетів, оскільки велика ентропія значень часових затримок не є нормою в реальній мережі.

Система «процес-подія»

Система «процес-подія» *(Process Query System, PQS* [2]) аналізує мережеву активність процесів в системі і формує зв'язки «процес-подія». За допомогою PQS для сукупності подій можливо визначити процес, який генерує певну подію.

PQS складається із декількох елементів:

- потік подій, що спостерігається системою;
- сукупність моделей, які описують потенційний процес-генератор подій;
- алгоритми відстеження, що аналізують події і визначають який процес їх створив;
- ядро PQS, що об'єднує попередні елементи і дає ймовірністну оцінку потоку подій.

В якості моделей для опису динамічних систем використовують наступні абстракції: прихована марковська модель, кінцевий автомат із прихованими станами, мережа Петрі, а в якості алгоритму відстеження - алгоритм Вітербі.

В роботі [3] PQS використовується для виявлення прихованих каналів за часом із бінарними кодами (кодування за допомогою алфавіту із «0» та «1»). Ефективність методу поки що є непідтвердженою, деякі моделі для опису процесів показують високий рівень хибних спрацювань, але, із слів авторів, метод є досить перспективним і підлягає подальшому дослідженню.

Штучні нейронні мережі

Штучні нейронні мережі (ШНМ) активно використовуються у задачах розпізнавання образів і послідовностей. ШНМ можна навчити розпізнаванню характеристик, притаманних прихованим каналам у мережах TCP/IP. Перевага використання ШНМ в тому, у процесі навчання нейронна мережа

здатна виявляти складні залежності між вхідними даними і вихідними, а в подальшій роботі виконувати узагальнення та прогнозування результатів.

В роботі [4] ШНМ застосовуються для виявлення прихованих каналів *NUSHU* (прихований канал із пам'яттю, використовує поле *SN TCP*-пакета для кодування інформації). Значення *SN*, які генерує *NUSHU* відрізняється від таких, що генерує класичний стек *TCP/IP Linux*, саме тому за допомогою ШНМ цю різницю можна помітити. В експерименті [4] застосований метод ШНМ має показник хибних спрацювань 0,1%, що показує його високу ефективність.

ШНМ можуть використовуватися для виявлення багатьох типів прихований каналів, недоліком їх застосування є необхідність попереднього навчання та налаштування (складність визначення оптимальної кількості нейронів).

Метод опорних векторів

Метод опорних векторів (Support vector machines, SVM) за ознаками схожий із ШНМ, але замість методів розпізнавання образів, дискримінантного аналізу та кластеризації використовуються метод роздільної класифікації. Систему на базі методу опорних векторів також потрібно навчати перед початком класифікації.

В роботі [5] SVM застосовуються для виявлення прихованих каналів із використанням поля *ID* в заголовку *IP*-пакета та поле *SN TCP*-пакета для кодування інформації без застосування шифрування вхідної інформації (тобто просте перетворення *ASCII* символів у значення *ID та SN*). Навчання *SVM* виконувалось на 10 тис. пакетах і в результаті проведення тестів *SVM* мав показник виявлення 99%. Але треба зазначити, що метод створення прихованих каналів був досить простий і їх також можна було виявити ймовірністно-статистичним методом, або навіть методом простого аналізу трафіку.

Перевагою даного методу є висока швидкість знаходження рішення та зростання швидкості алгоритму класифікації в процесі роботи методу. Недоліком методу є мала кількість параметрів для налаштування (єдиним варіативним параметром після фіксації ядер є коефіцієнт помилки *C*) та повільний процес навчання в порівнянні із ШНМ.

Нормалізатори трафіку

Нормалізатори трафіку в процесі роботи виправляють поля заголовків *IP*- та *TCP*-пакетів у відповідності із стандартом, поля, які мають бути порожніми (зарезервовані прапорці, поле *Urgent Pointer* при відсутньому прапорці *URG*), нормалізатор занулює. Застосовуються всі перетворення, що можуть бути виконані без спотворення семантики протоколу. Всі некоректні пакети повинні відкидатися.

Приклади використання нормалізаторів трафіку представлені в роботах [6] і [7], в [7] представлений нормалізатор видозмінював поля *ISN*, додаючи зсув значення, тим самим здійснюючи протидію прихованим каналам, що використовують дане поле для кодування інформації.

Для протидії прихованим каналам за часом нормалізатор трафіку може вносити випадкові часові затримки для пакетів.

Нормалізатори трафіку можуть використовуватись спільно із іншими методами виявлення прихованих каналів для більш ефективної роботи. На практиці майже не існує програмних реалізацій нормалізатора трафіку.

Поведінковий аналіз

Метод поведінкового аналізу передбачає аналіз профілю використання мережі. Поведінковий аналіз проводиться в режимі реального часу і дозволяє виявляти незвичну поведінку в мережі (незвичний трафік, його характер і обсяг). Виявлення аномалій засноване на порівнянні поточного характеру трафіку із стандартним сценарієм, що заздалегідь був визначений як нормальний. Наприклад, аномалією є багаторазова відправка пакету з одним і тим самим *SN*. Детально поведінковий аналіз в контексті виявлення прихованих каналів розглянуто у роботі [8]. Перевагою поведінкового аналізу є робота аналізатора в режимі реального часу та незалежність роботи аналізатора від конкретної реалізації того чи іншого прихованого каналу. Недоліком даного методу є необхідність розробки системи правил для роботи аналізатора та необхідність попереднього дослідження мережевого середовища з метою складання стандартного сценарію.

Висновки. В статті розглянуто актуальні методи виявлення прихованих каналів витоку і передачі інформації. Жоден із методів не може забезпечити гарантованого захисту в мережі від несанкціонованого витоку інформації, але гібридна система, що об'єднує в собі статистичний метод, нормалізацію трафіку та одну із систем із здатністю самонавчання, може забезпечити прийнятний показник виявлення та низький рівень хибних спрацювань.

1. Глобальное исследование утечек конфиденциальной информации в 2013 году / Аналитический центр InfoWatch. — 2014 — 23 с.— Режим доступу до джерела: (http://www.infowatch.ru/analytics).
2. Cybenko G., Berk V., Crespi V., Robert S. Gray, Jiang G. An Overview of Process Query Systems— 2004
3. Cybenko G., Berk V., Crespi V., Robert S. Gray, Jiang G. Covert Channel Detection Using Process Query Systems — 2005.
4. Tumoian E., Anikeev M. Detecting NUSHU Covert Channels Using Neural Networks — 2005.
5. Sohn T., Jung Seo J., Moon J. A Study on the Covert Channel Detection of TCP/IP Header Using Support Vector Machine — 2003.
6. Handley M., Paxson V. Network Intrusion Detection: Evasion, Traffic Normalization and End-to-End Protocol Semantics — 2001.
7. Fisk G., Fisk M., Papadopoulos C., Neil J. Eliminating Steganography in Internet Traffic with Active Wardens — 2003
8. Anjan K., Abraham J. Behavior Analysis of Transport Layer based Hybrid Covert Channel / Third International Conference on Network Security and Application — 2010.

Поступила 5.03.2014р.