УДК 621.391

Іван Никифорович Мєшков
Володимир Анатолійович Мусієнко
Володимир Володимирович Малишкін
Сергій Петрович Срібний

МОЖЛИВОСТІ ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ В ПРОВОДОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Постановка проблеми та її зв'язок із важливими науковими і практичними завданнями

Віддалені атаки на інформаційні ресурси через мережі передачі даних несуть в собі загрозу національній безпеці багатьох держав світу. Ця загроза настільки серйозна, що змушує уряди країн йти на додаткові адміністративні заходи щодо захисту інформації аж до відключення державних установ від міжнародних мереж передачі даних загального користування. Так, наприклад, "...Суб'єктам міжнародного інформаційного обміну в Російській Федерації заборонено здійснювати включення інформаційних систем, мереж зв'язку і окремих персональних комп'ютерів, в яких обробляється інформація, що містить відомості, що складають державну таємницю, і службову інформацію обмеженого поширення, а також для яких встановлені особливі правила доступу до інформаційних ресурсів, до складу засобів міжнародного інформаційного обміну, у тому числі в міжнародну асоціацію мереж Інтернет." (Указ Президента РФ від 12.05.2004 № 611 "Про заходи щодо забезпечення інформаційної безпеки Російської Федерації в сфері міжнародного інформаційного обміну").

Одними з головних причин, що провокують ріст мережевої злочинності є недосконаліть існуючих засобів і методів мережевого захисту інформації.

Аналіз останніх досліджень і публікацій. Формулювання мети статті

За звітами Міжнародного центру безпеки Інтернет CERT кількість уразливостей, що виявляються щорічно в програмному забезпеченні (ПЗ) систем мережевого захисту, з 1995 р. зросло більш ніж в 20 разів, причому спостерігається стійка тенденція їх зрісту. Згідно з даними спеціалізованого сайту по безпеці Zone-H, 31,4% успішних інформаційних атак через мережу загального користування відбувається через незакриті відомі уразливості, 24,2% — із-за помилок в налаштуваннях, 21,1% — через раніше невідомі уразливості, 16,3% атак здійснюються із застосуванням "грубої сили" і, нарешті, 4,7% доводиться на інші атаки. Як видно з приведених даних, 52,5% злочинів в мережах здійснюється за рахунок помилок в проектуванні і специфікації ПЗ і 24,2% - із-за помилок адміністрування (наприклад, згідно з дослідженнями проведеним асоціацією ICSA, до 70% усіх міжмережевих екранів мають різні помилки в конфігурації). Для "закриття" такого роду уразливостей системи мережевого захисту, які побудовані за принципом розмежування і контролю доступу, малоефективні. Якщо деякий інформаційний сервіс відкритий і доступний через мережу (за помилкою адміністратора або згідно встановленої політики безпеки), то, за наявності уразливістей в тому ПЗ, що реалізує цей сервіс, мережева атака з їх використанням може бути успішно проведена. Відмічені вище тенденції щодо посилення хакерської активності, збільшення числа помилок в програмному коді і налаштуваннях мережевих систем захисту ведуть до постійного росту економічних втрат. Таким чином, можна зробити наступний висновок, що більшість порушень в області інформаційної безпеки в мережах не можна повністю контролювати тільки традиційними засобами захисту на основі розмежування і контролю доступу (міжмережеві екрани і т. п.), незалежно від того, відбуваються порушення із-за наявності помилок в мережевому ПЗ або в налаштуваннях системи захисту. Тому необхідно приймати превентивні заходи щодо забезпечення мережевого захисту і розробляти політику мережевої безпеки на базі технологій, що дозволяють реалізувати упереджувальні стратегії захисту.

Виклад основного матеріалу

Одною з найбільш перспективних мережевих технологій фахівці називають технологію MPLS. Однак пріоритетом MPLS є швидкість просування пакету, а не QoS. У MPLS немає поняття безпеки у відмінності від ATM, де безпека визначається на

логічному рівні. Також MPLS не завжди сумісна з устаткуванням різного виробництва.

Хоча технологія MPLS захищає користувачів приватних мереж один від одного, вона не в силах забезпечити призначений для користувача трафік від цілеспрямованого перехоплення. Якщо зловмисник має адміністративні права або фізичний доступ до мережі передачі даних, він в змозі записати будь-який трафік, який передається у відкритому вигляді. Зрозуміло, оператор зв'язку може організаційно-технічними засобами зменшити вірогідність нелегітимного прослуховування, але повністю виключити перехоплення йому не вдасться.

Всі атаки можна [2] розділити на атаки «ззовні» і атаки «зсередини» (з магістралі MPLS).

Атаки «ззовні» можна розділити на дві складові: атаки із клієнтської мережі й атаки з Internet, тобто:

інжекція (введення) попередньо маркірованого трафіка із клієнтської мережі;

інжекція (введення) уже маркірованого трафіка з Internet.

Атаки «зсередини» на відміну від перерахованих атак передбачають знаходження зловмисника на магістралі.

Атаки «зсередини» можна розділити на наступні складові:

скомпрометовані провайдерські пристрої;

експлуатовані клієнтами пристрої PE;

зламані станції управління;

атаки на транзитні вузли між провайдерами;

неправильно сконфігуровані пристрої провайдерів;

модифікація міток на магістралі;

модифікація маршрутизації MP-BGP.

Скомпрометовані провайдерські пристрої. Даний вид атаки полягає в тому, що провайдерські пристрої можуть бути зламані, після чого зломщик (хакер) може отримати доступ до всієї конфіденційної інформації.

Експлуатовані клієнтами пристрої PE. Якщо клієнт самостійно експлуатує пристрій PE, це ставить під загрозу всю модель безпеки магістралі, оскільки в нього з'являється потенційна можливість доступу до віртуальних приватних мереж інших клієнтів.

Зламані станції управління. Якщо співробітник провайдерскї компанії входить в Internet з того ж комп'ютера, з якого він звертається до інструментів управління із графічним інтерфейсом для побудови VPN, то потенційно зловмисник може одержати доступ до системи управління — з усіма наслідками, що випливають, для безпеки VPN, що управляються.

Атаки на транзитні вузли між провайдерами. Для того щоб пропонувати віртуальні приватні мережі MPLS у світовому масштабі, багато операторів погоджують між собою контракти, завдяки яким вони можуть будувати віртуальні приватні мережі MPLS, що простираються за межі їхньої власної мережі, і одночасно обмінюватися маркірованими пакетами. RFC 2547 описує різні моделі, і серед них щонайменше одна — найбільш масштабована — може бути по своїй суті ненадійною. Окрім того, у точках обміну трафіком (Internet Exchange Points, IXP) оператори часто організовують міжз'єднання на базі Ethernet, в результаті чого потенційно створюються умови для атак на інтерфейс даних на другому рівні.

Невірно сконфігуровані пристрої провайдерів. У більшості випадків пристрої провайдерів обслуговуються людьми, які можуть робити ненавмисні помилки. За певних умов навіть стає можливим порушення цілісності магістралі MPLS. Якщо ж віртуальні приватні мережі MPLS використаються в рамках корпоративних мереж, то немає майже ніякої різниці між «клієнтськими пристроями» і «безумовно надійними провайдерськими пристроями» — щонайменше в тому, що стосується обслуговуючого персоналу.

Модифікація маршрутизації MP-BGP. Коли зловмисник знаходиться в стані вторгнення в первісний інформаційний обмін в Multiprotocol BGP, він може додавати у віртуальну приватну мережу «додаткові філії», і вже через них одержати неавторизований доступ до систем. Причому треба не тільки перебувати на магістралі, але й мати в наявності додаткові інструменти для точкового доступу до трафіка BGP, що вимагає значних зусиль.

Модифікація міток на магістралі. Цей тип атаки також передбачає знаходження атакуючого на магістралі. Якщо йому вдається змінити мітку пакета, то останній нескладно перенаправляти в іншу віртуальну приватну мережу. Крім того, в існуючі VPN можна ввести будь-які пакети.

Хоча для проведення подібних атак інструментів поки не існує, навіть однобічна інжекція пакетів у віртуальну приватну мережу може мати серйозні наслідки.

На основі наданих міркувань автор [2] зробив наступні висновки:

1. Використання технології MPLS у телекомунікаційних мережах спеціального призначення можливе лише у випадках, коли в якості середовища передавання даних використовуються волоконно-оптичні кабелі. Оскільки вони нечутливі до електромагнітних завад, виникнення подій, при яких шляхи телекомунікаційної мережі не будуть володіти властивістю живучості, стають неможливими.

2. Технологію MPLS у телекомунікаційних мережах спеціального призначення необхідно використовувати лише з QoS, що надасть змогу підтримувати різні види трафіка (дані, голос і відео) у єдиній мережній архітектурі, а також надавати споживачам гарантовану якість послуг і підтримувати додатки, що мають критично важливе значення для кінцевого користувача, при цьому пограничні комутатори повинні належати сайту спеціального призначення.

В роботі [4] проведено аналіз основних характеристик телекомунікаційних мереж

спеціального призначення і зроблено висновок про недоцільність використання технологій FRAME RELAY та ATM у автоматизованих системах управління спеціального призначення внаслідок слабких властивостей цих технологій щодо надійності та захисту інформації. В роботі також наведено процес обробки інформації на комутаційних вузлах при використанні спеціалізованої технології передачі пакетів з віртуальними каналами з зазначенням її головних властивостей.

Висновки й перспективи подальших досліджень

На основі аналізу процесу обробки інформації на комутаційних вузлах, указані наступні головні властивості спеціалізованої технології передачі пакетів з віртуальними каналами:

для передавання даних використовується пакет з фіксованим розміром ячейки. Це дає змогу апаратно реалізувати функції опрацювання та маршрутизації, отже, різко зменшити тривалість опрацювання ячейки, а також нормувати її;

це технологія інтегрованих послуг, тобто у ній єдиним потоком передається інформація з різними вимогами до затримок передавання та достовірності (аудіо-, відеоінформація, дані тощо);

швидкість та якість передавання інформації задають за запитом користувача;

технологія описує тільки інтерфейсні характеристики і для передавання даних може використовувати широкий спектр реальних каналів та комунікаційних мереж. З іншого боку, для зовнішнього користувача вона може надавати сервіс багатьох мереж та протоколів (Frame Relay, X.25, TCP/IP, SPX/IPX та ін.);

ця технологія гнучка в експлуатації. Якщо трапляється збій, автоматично збільшується відносна швидкість передачі інформації, або вибираються нові шляхи передавання.

Наведені властивості повністю або частково усувають недоліки, якими володіють технології ATM, Frame Relay та MPLS, що свідчить про можливість використовувати спеціалізовану технологію передачі пакетів з віртуальними каналами в якості основної технології в проводових телекомунікаційних мережах спеціального призначення.

Література

1. Закон України "Про оборону України". **2. Криховецький Г.Я.** Оцінка можливості застосування технології MPLS в телекомунікаційних мережах спеціального призначення. Науково-практичний журнал "Сучасні інформаційні технології у сфері безпеки та оборони". Випуск – № 3(6) – К. 2009. – С. 16-21. **3. Глуцький В. І.** Вибір інтегрального показника ефективності функціонування інформаційної мережі спеціального призначення / В. І. Глуцький, С. П. Колачов // Збірник наукових праць ВІТІ НТУУ "КПІ", – Вип. № 6. – К.: ВІТІ НТУУ "КПІ", 2003. – С. 5 – 14. **4. Колачов С.П.** Спеціалізована технологія передачі пакетів з віртуальними каналами / С.П. Колачов, В.А. Мусієнко, М.А. Стах // Збірник наукових праць ДНДІА, – Вип. № 7 (14). – К.: ДНДІА, 2011. – С. 208 – 213. **5. Гаманєк В. О.**, Кисельов І. М. та ін. Проектування автоматизованих систем управління. Навчальний посібник / В.О. Гаманєк, І.М. Кисельов та ін. Під редакцією Б. П. Шохіна – К.: ВІТІ НТУУ "КПІ", 2003. – 160 с.

В статье рассмотрена возможность применения технологий MPLS, ATM, Frame Relay в телекоммуникационных сетях специального назначения. Проведен анализ возможных хакерских атак в магистрали MPLS. Определены основные характеристики специализированной технологии передачи пакетов с виртуальными каналами.

Ключевые слова: сетевая защита информации, сетевые технологии, передача данных, передача пакетов по виртуальным каналам.

In article is considered possibility of the using technology MPLS, ATM, Frame Relay in telecommunication set of the special purpose. The organized analysis possible hacker attacks in pathways MPLS. They are determined main features specialized technologies of the issue package with virtual channel.

Key words: network protection to information, network technologies, data communication, issue package with virtual channel.