УДК 004.772

К.т.н., доцент Орлова М.М., магістрант Арехта О.О.

**Національний технічний університет України
«Київський політехнічний інститут»**

СПОСОБИ ТА ЗАСОБИ ОРГАНІЗАЦІЇ ЗАХИЩЕНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЇ MPLS

Abstract

Mariia M. Orlova, assoc. prof., PhD; Olga Arekhta, student
Methods and techniques of MPLS-based protected networking

This paper describes methods of protection for MPLS-based networks. A master structure of MPLS network has been examined. The main challenges of MPLS network protection have been determined.

Вступ

MPLS (Multiprotocol Label Switching) - сучасна, перспективна технологія передачі даних, яка характеризується гарантованою якістю обслуговування QoS (Quality of Service), ефективним управлінням трафіком, високою масштабованістю та інтеграцією з IP-сервісами. Але з розвитком технологій передачі даних з'являються проблеми такого роду, як захист комп'ютерних мереж і програмних застосувань від несанкціонованого доступу.

Постановка задачі

Метою даної роботи є дослідження та аналіз способів організації захищеного з'єднання, побудованого на базі технології MPLS, та модифікація процедур з'єднання, що встановлюється між кінцевими станціями, за рахунок призначення IP-адресам міток та їх подальшим кодуванням.

Особливості MPLS-мереж

У традиційних IP-мережах маршрутизація пакетів здійснюється на основі IP-адреси призначення. Кожний маршрутизатор в мережі має інформацію про те, через який інтерфейс і в якому напрямку необхідно направити IP-пакет. В той же час в MPLS-мережах кожному IP-пакету

призначається деяка мітка. Маршрутизатори приймають рішення про передачу пакета наступному пристрою на підставі значення мітки. Ця процедура займає значно менше часу, ніж порівняння IP-адреси відправника з найбільшим адресним префіксом в таблиці маршрутизації, яке використовується при традиційній маршрутизації. Саме тому однією з переваг MPLS-мереж є висока пропускна спроможність.

Однак, на даний момент, для MPLS-мереж не розроблені способи захисту інформації, що передається. У той же час вони, як і IP-мережі, вразливі для всіляких мережевих атак. Виходячи з цього, важливим питанням є організація захисту таких мереж від зловмисників.

Актуальність поставленої задачі

Можна виділити чотири основні групи загроз, які найчастіше виникають у сучасних мережах передачі даних: вірусні атаки; розсилка спаму; атаки типу “відмова в обслуговуванні”; атаки з використанням вразливостей ПЗ (програмного забезпечення) відкритих інформаційних сервісів, помилок програмування і налаштування.

Засоби та методи боротьби з цими загрозами засновані на принципі установки різноманітних “інформаційних бар'єрів” - міжмережевих екранів і мережевих фільтрів, систем виявлення вторгнення, активного аудиту, сканерів безпеки. Засоби та методи побудови віртуальних приватних мереж VPN (Virtual Private Network) відрізняються від наведеного вище підходу. Вони дозволяють створювати виділені (або приватні) мережеві канали на базі розподіленої мережевої інфраструктури і таким чином реалізувати випереджаючу стратегію захисту мережі.

Особливості технології MPLS VPN

Технологія MPLS може функціонувати на другому (канальному) і третьому (мережевому) рівнях моделі OSI (Open Systems Interconnection), що надає їй додаткову гнучкість при об'єднанні локальних мереж віддалених офісів та їх підключенні до централізованих серверів головного офісу.

Технології MPLS L2 VPN (MPLS-based Layer 2 VPN) дозволяють організувати канали другого рівня через розподілену опорну мережу, яку використовують, крім MPLS VPN, традиційні IP-сервіси. Фактично, за своєю функціональністю, сервіс MPLS L2 VPN є повноцінною альтернативою традиційним виділеним каналам зв'язку.

Основна відмінність L2 VPN від L3 VPN (MPLS-based Layer 3 VPN) - їх прозорість на мережевому рівні. В результаті, у користувача з'являється

певна гнучкість в управлінні своїм VPN. Мережі MPLS L3 VPN створюються на основі розподілу таблиць маршрутизації.

З точки зору мережевої безпеки технології MPLS L2/L3 VPN надають новий рівень захисту мережевого трафіку. Незважаючи на те що пакети передаються розподіленою опорною мережею, через занесення мережевих префіксів в різні маршрутні таблиці трафік одного VPN-каналу стає ізольованим в рамках кожного маршрутизатора. В результаті атаки типу "відмова в обслуговуванні", а також атаки з використанням вразливостей прикладного ПЗ в принципі не можуть бути здійснені ззовні виділеної мережі MPLS VPN.

Але віртуальні приватні мережі, створені на основі технології MPLS, забезпечують тільки ізоляцію поширення мережевого трафіку всередині певної VPN. Таким чином, через велику довжину каналів зв'язку зловмисник може здійснити атаку на ресурси інформаційного обміну при безпосередньому підключенні до каналу зв'язку. Для вирішення цієї проблеми розроблено наступний підхід.

Модифікований спосіб захисту з'єднання на базі MPLS

Відмова від протоколів мережевого рівня при передачі і шифруванні пакетів дозволяє не використовувати протоколи мережевого рівня при передачі інформації через MPLS-мережі. Коли пакет надходить до MPLS-мережі, йому призначається відповідний клас еквівалентності FEC (Forwarding Equivalence Class), що є формою представлення групи пакетів з однаковими вимогами до передачі. У технології MPLS мітка використовується для ідентифікації FEC при пересиланні, тобто мітка фактично описує мережеву адресу і додаткові параметри. Протокол IP відповідає мережевому рівню еталонної моделі OSI та є протоколом без встановлення з'єднання, це означає, що протокол IP не підтверджує доставку даних і не контролює цілісність отриманих даних. Одна з основних задач, які вирішуються протоколом IP, маршрутизація пакетів, тобто визначення шляху проходження пакету від одного вузла мережі до іншого на підставі адреси одержувача. Для цього використовуються таблиці маршрутизації, що формуються вручну або автоматично. IP-адреса є унікальним 32-бітним (в 4-ій версії протоколу IP) ідентифікатором мережевого інтерфейсу і призначається мережевому інтерфейсу при початковому налаштуванні мережі. Внаслідок того, що кількість MPLS-пристроїв в окремій мережі не значна, з'являється можливість призначення міток окремим мережевим адресам пристроїв MPLS-мережі.

Запропонований в даній роботі спосіб захисту MPLS-мереж від внутрішніх атак включає в себе:

1. Призначення окремих міток IP-адресам (рис. 1) мережевих інтерфейсів пристроїв, що працюють за технологією MPLS.

IP-адреса 1 <-> Мітка 1
IP-адреса 2 <-> Мітка 2
……..
IP-адреса N <-> Мітка N

Рис. 1. Призначення IP-адресам міток

2. Розповсюдження інформації в MPLS-мережі про прив'язку “IP-адреса – мітка” за допомогою модифікованого протоколу розподілу міток LDP (Label Distribution Protocol) [4] або модифікованого протоколу маршрутизації, наприклад, BGP (Border Gateway Protocol) [5], які повинні поширювати крім прив'язки “маршрут – мітка” ще і прив'язку “IP-адреса – мітка”. Використовуючи отриману інформацію про прив'язки “маршрут – мітка” та “IP-адреса – мітка” MPLS-пристрої організують маршрути з комутацією з використанням міток, як і в немодифікованій технології MPLS.
3. Шифрування окремо взятого мережевого пакету як при вході в MPLS-мережу, так і при створенні пакету на MPLS-пристрої всередині MPLS-мережі. Обмін секретними ключами можна реалізувати за допомогою існуючих методів і протоколів.

При роботі MPLS-мережі з використанням такого модифікованого способу зловмиснику, що здійснює атаку на протоколи інформаційного обміну при безпосередньому підключенні до каналу зв'язку, необхідно виконати криптографічний аналіз перехоплених пакетів. З високою ймовірністю можна передбачити, що першим кроком аналізу зловмисника буде класифікація перехоплених пакетів за класами еквівалентності при пересиланні, тобто за значенням мітки. Щоб ускладнити чи зробити неможливою цю операцію, необхідно виконати кодування міток.

У розробленому методі за основу функції ущільнення взята функція зі стандартного алгоритму RSA (абревіатура від прізвищ Rivest, Shamir та Adleman). Загальний вид цієї функції: $h_i=F(h_{i-1}, M_i , x) \bmod p$, де h_0, x, p – секретні параметри, F() – секретний поліном, M_i – блок даних. Для кожного маршруту з таблиці маршрутизації необхідно задавати такі параметри p і h_0, щоб при обчисленні значення мітки не було отримано однакових значень закодованих міток. У випадку зміни параметрів p і h_0, кодування міток виконується знову. При пересиланні пакетів мережею MPLS значення параметрів p і h_0 необхідно змінювати для кожного класу еквівалентності при пересиланні через певний час. Час зміни секретних параметрів визначається експериментально.

Реалізація наведеного вище підходу, передбачає внесення певних змін в архітектуру MPLS-пристроїв. У модифікованій архітектурі необхідно реалізувати нові функціональні модулі:

1. Модуль кодування і декодування значень міток. Цей модуль призначений для наповнення модифікованої інформаційної бази пересилання за мітками закодованими значеннями міток. Обчислення закодованих значень міток виконується за допомогою односпрямованої функції, яка достатньо просто обчислюється в одному напрямку (прямому), але викликає складності при обчисленні в протилежному (зворотному), і секретних параметрів, що використовуються при кодуванні. Початковими даними для отримання закодованого значення мітки може бути інформація з таблиці маршрутизації та інформація з немодифікованої інформаційної бази пересилання по мітках.
2. Модуль шифрування і дешифрування, який відповідає за криптографічний захист мережевих пакетів і повинен підтримувати як симетричне шифрування, так і несиметричне.
3. Модуль обміну секретними ключами, необхідними для шифрування пакетів і кодування міток.

Крім цього, при реалізації даних методів зміниться і структура інформаційної бази міток. У модифікованій інформаційній базі міток повинні міститися всі закодовані за допомогою секретних параметрів значення міток. Запис в інформаційній базі пересилання з використанням міток складається з безлічі закодованих значень вхідних міток і одного або більше вкладених записів. Кожний вкладений запис складається з множини закодованих вихідних міток, номера вихідного мережевого інтерфейсу і адреси наступного переходу.

Висновок

Технологія VPN MPLS надає високий ступінь захисту від зовнішніх загроз. Вона дозволяє створювати провайдерам окремі структуровані мережі, не пов'язані між собою, у складі глобальної мережі провайдера. Однак мала захищеність від злому через велику довжину каналів - один з недоліків таких мереж. Запропонований вище спосіб допомагає поліпшити їх захищеність шляхом кодування не лише пакетів, що передаються в мережі, але й міток, які використовуються при побудові маршруту. Кодування значень міток ускладнює або унеможливлює класифікацію перехоплених пакетів зловмисником за класами еквівалентності при пересиланні.

Література

1. *Вивек Олвейн*. Структура и реализация современной технологии MPLS: Пер. С англ. / Вивек Олвейн // М.: Издательский дом «Вильямс», 2004. – С.23-99.

2. *Михаил Захватов*. Построение виртуальных частных сетей (VPN) на базе технологии MPLS // Cisco Systems, 2001. – С. 7-16.

3. *Гольдштейн А.Б.* Технология и протоколы MPLS / Гольдштейн А.Б., Гольдштейн Б.С. // СПб.: БХВ-Санкт-Петербург, 2005. – С.20-110 с.

4. RFC 3035. MPLS using LDP and ATM VC Switching. Davie B., Lawrence J., McCloghrie K., Rosen E., Swallow G., Rekhter Y., Doolan P., 2001.

5. RFC 3107. Carrying Label Information in BGP-4. Rekhter Y., Rosen E., 2001.