УДК 004

ВРАЗЛИВОСТІ VPN: МЕХАНІЗМИ АТАК ТА МЕТОДИ ЗАХИСТУ

В. Ю. Демешко[1, a], В. В. Демчинський[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

В роботі розглянуто основні типи віртуальних приватних мереж та проведено аналіз атак, відтворено сценарії атак на деякі реалізації VPN в залежності від рівня моделі OSI, а також обгрунтовано методи захисту від даних атак.

Ключові слова: VPN (Virtual Private Network – віртуальна приватна мережа), вразливість, методи запобігання атакам

Вступ

На даний час забезпечення конфіденційності даних та захисту каналів передачі даних є дуже важливими як для бізнес структур, так і для приватних користувачів.

Загальною технологією захисту потоків даних є VPN (Virtual Private Network) – поєднання одного або декількох мережевих з'єднань, що передаються по незахищеним каналам, в логічну мережу та забезпечення конфіденційності і цілісності даних, автентифікації сторін і унеможливлення відмови від авторства.

1. Визначення та класифікація

Будемо досліджувати засоби VPN в залежності від рівня застосування та призначення. Технології віртуальних приватних мереж поділяють:

- За робочим рівнем моделі OSI: Канального рівня (використання протоколів PPTP, L2TP), Мережевого рівня (використання протоколу IPSec разом з IKE), Сеансового рівня (використання протоколів TLS - шифрування, SOCKS);
- За типом використовуваного середовища: захищені (протоколи IPSec, SSL, PPTP), довірчі (протоколи MPLS, L2TP);
- За способом реалізації: програмно-апаратні, програмні та інтегровані рішення;
- За призначенням: внутрішньокорпоративні або Intranet VPN, з віддаленим доступом або Remote Access VPN, міжкорпоративні або Extranet VPN, Internet VPN - забезпечують доступ провайдерів, Client/Server VPN

Далі зосередимо увагу на вразливостях та атаках на протоколи PPTP та IPSec.

[a] demes661@gmail.com

2. Статистика

Задля структурування можливих атак на різні протоколи VPN, аналізу відповідних статистик, аналізу частоти загроз та оцінки ризиків, звернемось до CVE [1](Common Vulnerabilities and Exposures), що налічує більше 800 записів про VPN, 718 з яких мають відношення до недоліків у прото- колах. Відповідно, було виявлено 31 вразливість у PPTP, 157 у TLS, 22 у L2TP, 106 у IPSec та 63 у SSL. Кількість вразливостей, пов'язаних з HTTPS – 313(Всі дані проілюстровано на рис. 1).

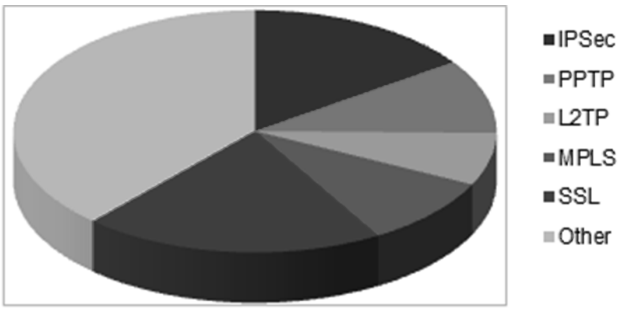

Рис. 1. Розподіл вразливостей за протоколами

3. Атака на PPTP

Протокол PPTP (Point-to-Point Tunnelling Protocol) є скандально відомим завдяки протоколу автентифікації MS-CHAPv2, який є складовою PPTP. Використання слабкої автентифікаціїї дозволяє розшифрувати трафік, але не в реальному часі, тому що розшифрування DES займає все ж таки не так мало часу. Виходячи зі статті Антона Жукова[2], в реалізації даного протокола є великі діри. Як зазначає автор, можливо зробити певну атаку – перевести передачу інформації із закритого каналу на відкритий, тобто отримати незашифрований трафік. Це вдається за допомогою неузгодженості дій протоколів маршрутизації і

спілкування хостів, використовуючи обидві версії протокола IP. Оскільки PPTP розрахований на передачу інформації в закритому вигляді по IPv4 та VPN-клієнт не сприймає IPv6, то використовуючи певні ICMPv6 запити до VPN-сервера, можна переключити канал передачі даних на сервері на IPv6 в незахищеному режимі. Використовуючи дану вразливість, посилаючи відповідні пакети для провокування такого збою і маючи припущення щодо налаштувань VPN-клієнта і VPN-сервера та відправивши пакет ICMPv6 від імені VPN-клієнта, зловмисник може отримати конфіденційну інформацію не витрачаючи час на розшифрування трафіку. Однак, в ході експерименту мною не було встановлено переключення між різними протоколами IP при передачі даних по PPTP, можливо через особливості налаштувань IPv6 інших сервісів VPN-клієнта і сервера.

4. Методи запобігання

Захиститись від такої атаки можливо уважно налаштовуючи мережу – відключати підтримку IPv6 на інтерфейсах, через які відбуватиметься з'єднання PPTP або відповідно налаштовувати правила маршрутизації. Також можливий варіант переривання з'єднання. В такому разі потрібно слідкувати за ним за допомогою утиліт VPNetMon або VPNCheck або примусово направити весь трафік через VPN.

5. Атака на IPSec

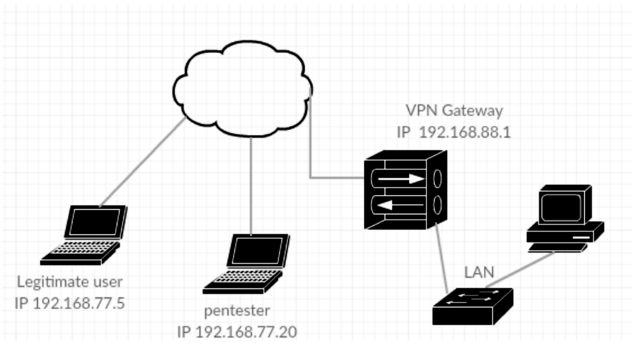

Рис. 2. Топологія мережі для атаки на IPSec

Візьмемо за основу матеріал статті Олександра Дмитренка «Анатомия IPsec. Проверяем на прочность легендарный протокол», журнал «Хакер» №196 [3]. В ній розглянута атака на протокол IPsec, під час якої можливо відтворити віддалене з'єднання з сервером. Топологія мережі показана на рис. 2. Атака відбувається на стадії узгодження криптоалгоритмів, алгоритмів хешування і т.д. Вразливість має реалізація VPN RA (Remote Access) при використанні протокола IKEv1 для даної стадії, адже цей протокол дозволяє використовувати два режими запиту з'єднання: main і agressive. Під час другого, у відкритому вигляді у мережу попадає дуже багато параметрів, наприклад PSK (Pre-Shared Key). Отримавши їх, автор знайшов пароль з PSK та провів брутфорс XAUTH з метою пошуку логіна і пароля користувача з PSK. Після цього проводиться автентифікація через звичайний VPN-клієнт. У проведеному експерименті для аутентифікації клієнта було встановлено складні логін і пароль довжиною 16 символів, що містили спеціальні символи. Як результат, брутфорс видався малоефективним, словник зайняв багато місця на ЖД і пароль знайдено не було. Також ускладнило процес атаки знаходження вірного хешу PSK. З 2005 року всі апаратні засоби CISCO повертають хеш незалежно від введеного ID. Виходячи з цього, дана реалізація атаки можлива за умови слабких даних для аутентифікації клієнта.

6. Рекомендації щодо налаштувань

З проведених мною теоретичних та експериментальних досліджень атак на протоколи VPN випливає ряд порад, направлених на унеможливлення проведення такого роду атак. Перш за все, потрібно встановити чітку політику безпеки, що диктує відповідні вимоги відносно складності паролів. Якщо використовується IKEv1, при встановленні з'єднання потрібно відключити або ігнорувати aggressive mode. Також потрібно приділяти увагу налаштуванням за замовчуванням: наприклад, відключати застарілі DES та MD4, які ще деколи зустрічаються в параметрах налаштувань. Використання AES-256 (як мінімум) значно підвищить конфіденційність потоку даних.

Рекомендації щодо запобігання вразливостей IPSec: якщо виходити з анатомії IPSec, то потрібно використовувати тільки IKEv2, тому, що він значно більш захищений відносно IKEv1. Також, надійніше використовувати аутентифікацію за RSA-ключем, бо PSK можливо підібрати брутфорсом.І загалом, якщо принциповим вразливостям VPN приділяється досить уваги, то більшу загрозу становлять вади окремих реалізацій протоколів VPN.

Висновки

В проведеній роботі було екпериментально досліджено атаки на реалізації різних протоколів VPN віддаленого доступу та надано рекомендації щодо усування або недопущення відповідних загроз.

Перелік використаних джерел

1. CVE list: `https://cve.mitre.org/`.
2. А. Жуков «Такой небезопасный VPN» — «Хакер» №170 03/2013. — С. 73 с.
3. О. Дмитренко «Анатомия IPsec. Проверяем на прочность легендарный протокол» — «Хакер» №196. — С. 80 с.