НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Проектування і розробка криптографічних систем

Лабораторна робота №2

Дослідження реалізацій протоколів IPSec

Виконали:
Волинець Сергій ФІ-42мн
Сковрон Роман ФІ-42мн
Молдован Дмитро ФІ-42мн

Київ – 2025

1 Мета роботи

Метою роботи є дослідження архітектури та особливостей реалізації криптографічних механізмів стеку протоколів IPSec, який призначений для забезпечення конфіденційності, цілісності та автентичності інформації на мережевому рівні. Ціль практикуму – проаналізувати протоколи AH, ESP, ISAKMP, IKE, IKEv2, KINK, розглянути використання безпечних асоціацій (Security Associations, SA), баз даних SPD та SAD, а також обробку IPSec-пакетів у транспортному та тунельному режимах.

2 Постановка задачі

Провести дослідницьку роботу з метою аналізу особливостей реалізації криптографічних механізмів протоколів IPSec. Описати основне призначення протоколів IPSec, їх місце в мережевій моделі OSI та взаємодію зі стеком протоколів TCP/IP та ін. Дослідити архітектуру стеку протоколів IPSec. Описати призначення, особливості та відмінності криптографічних механізмів протоколів AH, ESP, ISAKMP, IKE, IKEv2, KINK та ін. Проаналізувати концепцію безпечних асоціацій (SA), її особливості та бази даних SPD і SAD (їх призначення та способи заповнення і використання). Дослідити детально особливості структури заголовків протоколів AH і ESP в тунельному та транспортному режимах з повним описанням їх полів та можливих значень. Визначити особливості обробки вхідних та вихідних IPSec-пакетів для кожного з протоколів та режимів. Дослідити нижній рівень архітектури стеку протоколів IPSec – домен інтерпретації DOI. Визначити зареєстровані алгоритми автентифікації, шифрування, геш-функцій та ін. криптографічних алгоритмів для стеку протоколів IPSec. Визначити та описати особливості основних схем застосування протоколів IPSec: хост-хост, шлюз-шлюз та хост-шлюз. А також використання протоколів IPSec для побудови VPN-тунелів.

3 Теоретичний аналіз та опис дослідження

3.1 Призначення та місце IPSec у моделі OSI

IPSec (Internet Protocol Security) – це набір відкритих стандартів та протоколів, що забезпечують захист мережевого трафіку на 3-му мережевому рівні моделі OSI. Оскільки базовий протокол IP не містить вбудованих засобів шифрування або автентифікації, IPSec додає ці функції поверх IP-протоколу.

Протоколи IPSec забезпечують такі властивості:

- Конфіденційність: дані шифруються і залишаються недоступними для третіх осіб.
- Цілісність: захист від зміни даних за допомогою MAC або HMAC.
- Автентичність: підтвердження справжності відправника/одержувача.
- Захист від атак повтору.

IPSec тісно інтегрується в стек TCP/IP, працюючи безпосередньо поверх IP. Він не змінює логіку роботи транспортних і прикладних протоколів, а лише захищає дані, що надходять на IP-рівень. Стек протоколів IPSec складається з кількох компонентів, які взаємодіють для забезпечення безпеки даних на мережевому рівні. Він включає в себе шари, що виконують різні завдання, такі як автентифікація, шифрування та управління безпечними асоціаціями.

Архітектура IPSec складається з таких компонентів:

- Протоколи захисту даних: AH (Authentication Header) і ESP (Encapsulating Security Payload);

- Протоколи управління ключами: ISAKMP (Internet Security Association and Key Management Protocol), IKE (Internet Key Exchange), IKEv2, KINK (Kerberized Internet Negotiation of Keys);
- Бази даних політик та асоціацій: SPD (Security Policy Database) та SAD (Security Association Database);
- Механізми формування SA (Security Association), які визначають параметри захисту для з'єднання.

AH (Authentication Header)

Даний протокол забезпечує автентифікацію та цілісність даних, але не забезпечує конфіденційність, оскільки дані не шифруються. AH додає заголовок до пакетів, щоб гарантувати, що дані не були змінені під час передачі. Він не забезпечує шифрування, тому інформація залишається видимою, але підтверджується справжність. Протокол використовує MAC (Message Authentication Code) для перевірки цілісності й автентичності пакету. Сам AH хедер не включається в шифрування. AH у транспортному режимі захищає IP-пакет. Оригінальний IP-пакет не інкапсулюється, а AH заголовок просто додається після IP-заголовка. У тунельному режимі AH повністю інкапсулює оригінальний IP-пакет у новий IP-пакет. Заголовок AH містить наступні поля: Next Header, Payload Length, SPI, Sequence Number, Authentication Data.

ESP (Encapsulating Security Payload)

Використовується для забезпечення конфіденційності, цілісності та автентифікації даних. Навідміну від AH, ESP шифрує дані в пакеті і забезпечує їх автентифікацію, інтегруючи шифрування й автентифікацію в одному процесі. Використовує MAC для автентифікації. ESP є найбільш поширеним механізмом у IPSec. ESP у транспортному режимі інкапсулює лише транспортні дані (TCP/UDP-пакет). ESP у тунельному режимі щифрує весь оригінальний IP-пакет, створюючи новий IP-заголовок. ESP-структура: SPI, Sequence Number, IV, Encrypted Payload, Padding, Authentication Data (опціонально).

ISAKMP (Internet Security Association and Key Management Protocol)

Даний протокол визначає правила для обміну ключами та управління асоціаціями безпеки (SA). Він відповідає за обмін ключами та параметрами між сторонами, які встановлюють безпечний зв'язок. Використовується для обміну протоколами IKE та IKEv2. Він не має специфічних криптографічних механізмів але забезпечує структуру для обміну інформацією про захист. ISAKMP задає основу для створення та керування SA.

IKE (Internet Key Exchange)

Протокол забезпечує створення і управління безпечними асоціаціями через обміни ключами для протоколів AH та ESP. Працює на основі протоколу ISAKMP. IKE відповідає за автентифікацію учасників і узгодження параметрів для створення захищених каналів зв'язку. IKE (Internet Key Exchange) виконує взаємну автентифікацію, обмін ключами, формування SA. Протокол має два режими роботи: основний режим, що вважається більш захищеним, але є повільнішим, та агресивний, що складається з меншої кількості повідомлень а тому вважається менш безпечним але швидшим.

IKEv2

Покращена версія протоколу IKE з покращеною безпекою та підтримкою мобільних пристроїв. Включає більш ефективні механізми для управління підключеннями, відновлення сеансів і адаптацію до зміни мережі. Підтримує функцію перезапуску після втрати зв'язку.

KINK (Kerberized Internet Negotiation of Keys)

Протокол призначений для налаштування асоціацій безпеки (SA) в IPsec. KINK використовує протокол Kerberos, що дозволяє централізовано управляти аутентифікацією пірів та політиками безпеки за допомоги довірених третіх осіб. Основна мета KINK полягає в наданні альтернативи Internet Key Exchange (IKE), в якій учасникам потрібно використовувати сертифікати X.509 для аутентифікації та обмінюватися ключами за допомогою алгоритму Диффі-Хеллмана. Учасники KINK повинні лише однаково аутентифікуватися з відповідним сервером аутентифікації, тоді як розподіл ключового матеріалу здійснюється через центр розподілу ключів (KDC). KINK є state-less протоколом. Кожна команда або відповідь не потребує зберігання стану, на відміну від IKE, який декілька обмінів пакетами для встановлення асоціацій безпеки.

Security Association (SA)

Безпечна асоціація (SA) – це набір параметрів, які визначають захищене з'єднання. Зокрема, SA включає: алгоритм шифрування, алгоритм автентифікації, ключі, SPI (Security Parameters Index), режим роботи (транспортний/тунельний), тощо. Установка SA в IPSec починається з обміну інформацією через ISEKMP у двох фазах. У першій фазі сторони аутентифікують одна одну та домовляються про параметри для спеціального ISAKMP-тунеля для обміну алгоритмами шифрування. У другій фазі вони узгоджують створення основного тунелю для даних. Після встановлення основного тунелю ISAKMP тунель залишається активним для оновлення SA, оскільки шифрувальні ключі мають обмежений термін використання, після якого відбувається їх оновлення. Для забезпечення роботи SA використовуються дві бази даних: база політик безпеки SPD (Security Policy Database) та база безпечних асоціацій SAD (Security Association Database).

SPD (Security Policy Database)

Містить правила, які визначають: який трафік захищати, як його обробляти, яким чином та які SA слід використовувати. Слугує фільтром для мережевого трафіка. Визначає три дії з трафіком:

- PROTECT – трафік додатково захищається за допомоги шифрування чи автентифікації з використанням протоколів IPSec.
- BYPASS – трафік проходить без змін.
- DISCARD – трафік повністю відхиляється.

Контретні заходи для захисту трафіку визначаються в SAD (Security Association Database).

SAD (Security Association Database)

Містить конкретні параметри захисту, тобто самі SA. Якщо у базі данних SA не знайдено, то ініціюється процес встановлення SA. Таким чином, SPD визначає, який трафік потребує захисту, а SAD надає параметри для цього захисту.

Домен інтерпретації DOI

DOI (Domain of Interpretation) визначає призначення параметрів протоколів, набори криптографічних алгоритмів та політики безпеки. Він забезпечує узгодженість між різними реалізаціями протоколів. Структура DOI:

- Ідентифікатор DOI: унікальний числовий код, що визначає домен інтерпретації. Для IPSec використовується DOI = 1.
- Протоколи: перелік протоколів, які можуть бути узгоджені в SA (ISAKMP (1), AH (2), ESP (3)).
- Перетворення: набори криптографічних алгоритмів (шифрування, автентифікація, режими роботи), дозволених для кожного протоколу.
- Атрибути SA: параметри, які описують властивості SA: довжини ключів, режими роботи алгоритмів, параметри таймінгів тощо.
- Типи ідентифікаторів: способи представлення сторін у процесі встановлення SA (IP адреси, E-mail, тощо).
- Тощо.

Криптографічні алгоритми IPSec

Для шифрування використовуються такі алгоритми шифрування: AES-CBC, AES-CTR, AES-GCM, 3DES (застарілий), ChaCha20-Poly1305.

Для автентифікації використовуються геш-функції: HMAC-SHA2, HMAC-SHA3, HMAC-MD5, AES-XCBC-MAC, GMAC.

3.2 Основні схеми застосування IPSec

Існують три основні схеми застосування IPSec:

- Хост – хост: пряме з'єднання між двома кінцевими вузлами.
- Шлюз – шлюз: застосовується у міжофісних VPN.
- Хост – шлюз: класичний варіант VPN-доступу користувача.

У Другому та третьому випадках використовується тунельний режим ESP. IPSec можна застосувати для створення віртуальних приватних мереж (VPN). Для цього використовують протоколи IPSec в тунельному режимі для інкапсуляції всього пакета. Це гарантує цілісність, конфіденційність та автентифікацію даних.

4 Висновки

У ході дослідження було встановлено, що IPSec є потужним і гнучким механізмом захисту мережевого рівня, який забезпечує конфіденційність, цілісність і автентичність IP-трафіку. Протоколи AH і ESP виконують різні, але взаємодоповнюючі функції, тоді як IKE та IKEv2 забезпечують надійну систему обміну ключами. Архітектура IPSec ґрунтується на концепції SA, які керуються базами SPD та SAD. Стек протоколів IPSec підтримує великий набір криптографічних алгоритмів та широко застосовується у VPN-рішеннях різного масштабу.