Міністерство освіти і науки України
Національний Технічний Університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Комп'ютерний практикум 2
з дисципліни
«Проектування, розробка і реалізація криптографічних систем»
Тема:
«Дослідження реалізацій протоколів IPSec»

Виконав:
Студент групи ФІ-22мн
Кушнір Олександр
Перевірив:
Селюх П. В.

Київ – 2023

IP-безпека (IPSec) дозволяє забезпечувати захист внутрішніх мереж, а також створювати безпечні рішення на базі віртуальної приватної мережі для зв'язку через зовнішні мережі (Інтернет). Технологія IPSec була розроблена групою IETF (Internet Engineering Task Force) і є галузевим стандартом шифрування трафіку TCP/IP.

Оскільки конфіденційна інформація постійно пересилається по мережі, мережні адміністратори забезпечити захист цього трафіку від:

- зміни даних при пересилці;
- перехоплення, перегляду і копіювання;
- несанкціонованого уособлення певних ролей;
- перехоплення і повторного використовування пакетів для отримання доступу до конфіденційних ресурсів (для цього звичайно застосовується зашифрований пароль).

Служби безпеки IPSec призначені забезпечити цілісність, конфіденційність і перевірку автентичності даних, а також захист від їх повторного використання для отримання доступу.

Протокол IPSec (Internet Protocol Security) є протоколом безпеки, включеним до стеку протоколів TCP/IP. IPSec отримав визнання як стандарт для надійної комунікації по IP. Він використовується як розширення IPv4 і є невід'ємною складовою частиною IPv6.

Протокол IPSec іноді ще називають протоколом тунелювання третього рівня (Layer-3 Tunneling). Тунель IPSec між двома локальними мережами може підтримувати безліч індивідуальних каналів передачі даних, внаслідок чого додатки даного типу одержують переваги щодо масштабування в порівнянні з технологією другого рівня. Протокол IPSec може використовуватися спільно з протоколом L2TP. Спільно ці два протоколи забезпечують найвищий рівень гнучкості при захисті віртуальних каналів. Специфікація IPSec орієнтована на протокол IP і, таким чином, даремна для трафіку будьяких інших протоколів мережного рівня. Протокол L2TP відрізняється незалежністю від транспортного рівня, що може бути корисне в гетерогенних мережах, що складаються з IP-, IPX- сегментів.

Протокол IPSec застосовується головним чином в рішеннях VPN (Virtual Privat Network) в двох областях:

- для організації захищених з'єднань між офісами (філіями);
- для захисту віддаленого доступу користувачів.

У разі VPN між офісами, трафік між двома локальними мережами проходить через міжмережеві екрани (Firewall), маршрутизатори чи крипто-шлюзи з підтримкою IPSec з обох боків з'єднання. Шлюз шифрує пакети IP і відправляє їх через загальнодоступну мережу далі до шлюзу призначення, де ті розшифровуються і аутентифікуються. У разі віддаленого доступу шифрування і подальшу передачу пакетів бере на

себе клієнтська програма на віддаленій робочій станції. Створення захищеного тунелю виконують компоненти віртуальної мережі, що функціонують на вузлах, між якими формується тунель. Ці компоненти прийнято називати ініціатором та термінатором тунелю. Ініціатор тунелю інкапсулює (вбудовує) пакети в новий пакет, що містить разом з початковими даними новий заголовок з інформацією про відправника і одержувача. Хоча всі пакети, які передаються по тунелю, є пакетами IP, пакети, що інкапсулюються, можуть належати до протоколу будь-якого типу, включаючи пакети протоколів, які не маршрутизуються, наприклад, NetBEUI. Маршрут між ініціатором і термінатором тунелю визначає звичайна мережа IP, яка може бути і мережею, відмінною від Internet. Термінатор тунелю виконує процес, зворотній інкапсуляції, - він виділяє нові заголовки і направляє кожний початковий пакет в локальний стек протоколів або адресату в локальній мережі. Сама по собі інкапсуляція ніяк не впливає на захищеність пакетів повідомлень, які передаються по тунелю VPN. Але завдяки інкапсуляції з'являється можливість повного криптографічного захисту пакетів, що інкапсулюються. Конфіденційність пакетів, що інкапсулюються, забезпечується шляхом їх криптографічного закриття, тобто зашифрування, а цілісність і автентичність – шляхом формування цифрового підпису.

AH and ESP

IPSec використовує два різні протоколи: заголовок аутентифікації (AH) та інкапсуляцію корисних даних безпеки (ESP), визначених IETF.

Протокол AH надає лише механізм автентифікації. AH забезпечує цілісність даних, автентифікацію джерела даних та додаткову службу захисту від повторного відтворення. Цілісність даних забезпечується використанням дайджесту повідомлення, створюваного таким алгоритмом як HMAC-MD5 або HMAC-SHA. Аутентифікація джерела даних забезпечується використанням загального секретного ключа створення дайджеста повідомлення. Захист від повторного відтворення забезпечується використанням поля порядкового номера із заголовком AH. AH автентифікує заголовки IP та їх корисні дані, за винятком певних полів заголовків, які можуть бути законно змінені під час передачі, таких як поле часу життя (TTL).

Протокол ESP забезпечує конфіденційність даних (шифрування) та аутентифікацію (цілісність даних, аутентифікація джерела даних та захист від повторного відтворення). ESP можна використовувати лише з конфіденційністю, тільки з автентифікацією або з конфіденційністю та автентифікацією. Коли ESP надає функції аутентифікації, він використовує самі алгоритми, як і AH, але покриття інше. Аутентифікація в стилі AH автентифікує весь IP-пакет, включаючи зовнішній IP-

заголовок, тоді як механізм автентифікації ESP автентифікує лише частину IP-дейтаграм IP-пакета.

IKE and IKEv2

IKE ґрунтується на базових протоколах безпеки, таких як безпечна асоціація SA, протокол управління ключами та контекстами безпеки ISAKMP, криптографічний протокол розповсюдження ключів SKEME та протокол визначення ключів Oakley. ISAKMP визначає основу для автентифікації та обміну ключами, але не вказує самі ключі. SKEME визначає універсальну техніку обміну ключами, яка забезпечує швидке оновлення ключів. Oakley дозволяє перевіреним сторонам обмінюватися ключами через небезпечне з'єднання, використовуючи алгоритм обміну ключами Діффі-Хеллмана. Такий метод забезпечує максимальну секретність ключів, захист ідентифікаційних даних та автентифікацію.

Протокол IKE використовує UDP порт 500, який ідеально підходить для мережевих додатків, яким критично важлива відсутність тимчасової затримки, наприклад додатки пов'язані з аудіо та відео обміном файлами або онлайн ігри. Більше того, протокол не передає службові дані, пов'язані з протоколом "точка-точка" (PPP). Це робить IKE швидше, ніж PPTP та L2TP протоколи. Крім того, IKE протокол підтримує шифрування AES та Camellia, а також використовує ключі довжиною 256 біт. Саме тому IKE вважається досить безпечним протоколом.

IKEv2 суттєво вдосконалили, що зробило його значно кращим порівняно з IKEv1. Переваги IKEv2 перед IKEv1 такі:

- Щоб встановити VPN-тунель, IKEv2 вимагає меншої кількості повідомлень, якими обмінюються кінцеві точки тунелю (чотири повідомлення для IKEv2 проти шести для IKEv1)
- IKEv2 оснащений функцією NAT-T, яка забезпечує найкращу сумісність між постачальниками
- IKEv2 підтримує Extensible Authentication Protocol (EAP)
- IKEv2 пропонує найкращу стабільність завдяки опції Keep Alive
- Для більш стабільного з'єднання IKEv2 підтримує протокол MOBIKE, також відомий як Mobility and Multi-homing. Це дозволяє IKEv2 підтримувати сеанс VPN, коли користувач перемикає IP-адреси без необхідності повторно встановлювати з'єднання. Відсутність цієї функції була серйозною проблемою безпеки в IKEv1, яка могла призвести до витоку даних. Якщо, наприклад, користувач перейшов з офісного Wi-Fi на з'єднання Ethernet, це могло перервати сеанс VPN
- Асоціації безпеки в IKEv2, також відомі як дочірні SA, можуть бути незалежно створені, видалені та змінені у будь-який час протягом життя VPN-тунелю

- IKEv2 вимагає меншої кількості асоціацій безпеки на тунель, що знижує потрібну пропускну здатність
- IKEv2 визначає всі типи повідомлень як пари запиту та відповіді, що робить протокол більш надійним
- IKEv2 підтримує асиметричну автентифікацію

SPD і SAD

База даних безпечних асоціацій (Security Associations Database, SAD) та база даних політики безпеки (Security Policy Database, SPD).

У вхідних пакетах для кожного протоколу захисту вже проставлено значення SPI, що однозначно визначає контекст. Перегляд бази SPD у такому разі не потрібний; можна вважати, що безпекова політика враховувалася при формуванні відповідного контексту. (Практично це означає, що ISAKMP-пакети потребують особливого трактування, а правила з відповідними селекторами мають бути включені до SPD.)

У заголовках AH та ESP передбачено особливе поле SPI, куди міститься покажчик на рядок бази даних SAD, в якому записані параметри відповідної SA. Це поле заповнюється протоколами AH або ESP під час обробки пакета у відправній точці захищеного каналу. Коли пакет приходить у кінцевий вузол захищеного каналу, з його заголовка ESP або AH (на малюнку із заголовка ESP) вилучається покажчик SPI, і подальша обробка пакета виконується з урахуванням всіх параметрів асоціації, заданої цим покажчиком.