НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Лабораторна робота 2

предмета: **Проектування розробка і реалізація криптографічних систем**
на тему: **«Дослідження реалізацій протоколів IPSec»**

Виконали:
студенти II курсу, групи ФІ-42мн
Буржимський Ростислав
Недождій Максим

Київ — 2025

1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТА АРХІТЕКТУРА IPSEC

1.1 Призначення та місце в моделі OSI

IPSec (англ Internet Protocol Security) — це набір протоколів, розроблений Internet Engineering Task Force, який забезпечує безпеку передачі даних на мережевому рівні (англ. Network Layer) L3 еталонної моделі OSI. Основною метою IPSec є забезпечення конфіденційності, цілісності та автентифікації даних, що передаються через IP-мережі.

У контексті стека протоколів TCP/IP, IPSec займає ключове місце безпосередньо над протоколом Internet Protocol. Це дає йому важливу перевагу над іншими протоколами безпеки:

– **Прозорість для додатків:** На відміну від SSL/TLS, які працюють на транспортному/прикладному рівнях L4-L7 і вимагають підтримки з боку програмного забезпечення, IPSec захищає будь-який трафік, що проходить через мережевий інтерфейс. Додатки, такі як веб-браузери, поштові клієнти, бази даних, що не потребують модифікації для використання IPSec.

– **Універсальність:** Оскільки IPSec працює на рівні IP-пакетів, він може захищати протоколи вищих рівнів, такі як TCP, UDP, ICMP, а також протоколи маршрутизації.

У моделі взаємодії відкритих систем IPSec функціонує на 3-му рівні. Він інкапсулює IP-пакети або їхнє корисне навантаження, додаючи криптографічні заголовки. Це дозволяє створювати віртуальні приватні мережі, забезпечуючи захищений тунель через публічні, незахищені мережі, такі як Інтернет.

1.2 Архітектура стеку протоколів IPSec

Архітектура IPSec — це модульна система, яка чітко розділяє функції обробки трафіку та функції керування ключами. Згідно з RFC 4301, архітектура базується на наступних ключових компонентах:

Security Association - Асоціація безпеки

SA є фундаментальним поняттям в IPSec. Це логічне з'єднання між двома пристроями, яке визначає, як саме буде захищатися трафік. SA є односпрямованою. Для двостороннього зв'язку необхідно створити дві асоціації безпеки. Кожна SA ідентифікується унікальною комбінацією трьох параметрів:

1) **Security Parameter Index:** 32-бітне число в заголовку пакету IPSec, яке дозволяє отримувачу знайти відповідну SA у своїй базі даних.
2) **IP-адреса призначення:** Адреса вузла, до якого надсилається пакет.
3) **Ідентифікатор протоколу безпеки:** Вказує, який протокол використовується AH або ESP.

Бази даних політик та асоціацій

Функціонування IPSec у ядрі операційної системи спирається на дві бази даних:

– **SAD (Security Association Database):** Містить активні параметри для кожної встановленої SA, такі як ключі шифрування, алгоритми, лічильники послідовності пакетів та час життя ключів. Коли пакет надходить на інтерфейс, система перевіряє SPI та шукає відповідний запис у SAD для розшифрування.

– **SPD (Security Policy Database):** Визначає правила обробки трафіку. Для кожного пакету вирішується одне з трьох дій:

1. `DISCARD` - відкинути пакет.
2. `BYPASS` - пропустити без шифрування.
3. `PROTECT` - застосувати IPSec шифрувати або підписати.

2 ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ

2.1 Протоколи захисту даних: AH та ESP

В IPSec використовуються два основних протоколи для обробки самих даних. Вони можуть використовуватися окремо або разом, проте використання разом недоцільне через через надлишковість захисту.

Authentication Header

Протокол AH, що визначений у RFC 4302, забезпечує цілісність даних, автентифікацію джерела та захист від атак повторного відтворення.

– **Призначення:** Забезпечує цілісність даних, автентифікацію джерела та захист від атак повторного відтворення.

– **Особливість:** AH не забезпечує конфіденційності, оскільки дані передаються у відкритому вигляді.

– **Механізм роботи:** AH обчислює значення перевірки цілісності (англ Integrity Check Value) на основі вмісту пакету та незмінних полів IP-заголовка.

– **Проблема NAT:** Оскільки AH включає поля IP-заголовка, зокрема IP-адреси, у хеш-суму, будь-яка зміна IP-адреси при проходженні через Network Address Translation порушує цілісність хешу. Тому AH несумісний з NAT.

Encapsulating Security Payload

Протокол ESP (Encapsulating Security Payload) стандартизовано в RFC 4303. На відміну від AH, який орієнтований насамперед на контроль цілісності й автентифікацію та може охоплювати незмінні поля IP-заголовка, ESP в першу чергу призначений для забезпечення *конфіденційності* трафіку за рахунок шифрування корисного навантаження, а також може додатково забезпечувати цілісність, автентифікацію та захист від повторного відтворення.

– **Призначення:** ESP забезпечує конфіденційність і, за потреби, цілісність, автентифікацію та захист від повторів.

– **Механізм роботи:** ESP додає заголовок і трейлер, шифрує корисне навантаження та опціонально додає дані автентифікації/контроль цілісності; на відміну від AH, він не призначений для автентифікації зовнішнього IP-заголовка.

– **Сумісність з NAT:** ESP зазвичай працює через NAT, тоді як AH часто несумісний з NAT через перевірку полів IP-заголовка.

Характеристика	**AH (Authentication Header)**	**ESP (Encapsulating Security Payload)**
Номер протоколу IP	51	50
Шифрування даних	Ні	Так (DES, 3DES, AES)
Автентифікація	Так (весь пакет + IP заголовок)	Так (тільки payload + ESP заголовок)
Робота через NAT	Неможлива	Можлива

Таблиця 2.1 – Порівняння AH та ESP

2.2 Протоколи керування ключами: ISAKMP, IKE та KINK

Для автоматичного встановлення Security Associations (SA) та обміну криптографічними ключами в архітектурі IPSec розроблено спеціалізовані протоколи керування, які розв'язують узгодження параметрів безпеки й безпечну генерацію сесійних ключів через публічну мережу.

2.2.1 ISAKMP: Фреймворк для узгодження параметрів

ISAKMP (RFC 2408) є фреймворком, що визначає формати повідомлень, процедури і синтаксис для узгодження параметрів безпеки. На практиці ISAKMP використовується разом з протоколом IKE, який реалізує алгоритми обміну ключами на основі груп Діффі-Хеллмана чи еліптичних кривих. Таким чином: ISAKMP визначає «як передавати», а IKE — «яку математику» використовувати.

2.2.2 IKEv1: Двофазне встановлення

IKEv1 (RFC 2409) будується на двоетапній архітектурі:

– **Етап 1:** Встановлення захищеного каналу ISAKMP SA. Два режими: Main Mode — 6 повідомлень, краще конфіденційність та Aggressive Mode — 3 повідомлення, швидше, але передає хеш ID.

– **Етап 2:** Узгодження параметрів для IPSec SA: алгоритми, час життя під захистом каналу з Етапу 1.

2.2.3 IKEv2: Мінімалістична архітектура

IKEv2 (RFC 7296) об'єднує обидві етапи в один процес:

– **Швидкість:** 4 повідомлення — 2 пари запит-відповідь замість 6–9 у IKEv1, що суттєво скорочує затримку встановлення.

– **NAT-Traversal:** Автоматичне виявлення NAT та переведення на UDP-інкапсуляцію.

– **MOBIKE:** Дозволяє змінювати IP-адресу клієнта під час активної сесії без розриву з'єднання.

– **Захист від DoS:** Механізм cookies перевіряє реальність клієнта перед ресурсомісткими обчисленнями.

2.2.4 KINK: Інтеграція з Kerberos

KINK (RFC 4430) — альтернатива IKE для корпоративних мереж з Kerberos. Замість асиметричної криптографії або PSK використовує квитки Kerberos для автентифікації та генерації IPSec ключів. Переваги: централізоване керування через KDC, менші вимоги до ресурсів, ніяких окремих сертифікатів. Недолік: вимагає Kerberos і менш універсальна за IKEv2.

3 АНАЛІЗ КОНЦЕПЦІЇ БЕЗПЕЧНИХ АСОЦІАЦІЙ ТА БАЗ ДАНИХ ПОЛІТИК

3.1 Концепція безпечних асоціацій

Безпечна асоціація SA є фундаментальним будівельним блоком архітектури IPSec. Це логічна сутність, що описує узгоджений набір параметрів безпеки, який використовується для захисту каналу зв'язку між двома вузлами. Без розуміння концепції SA неможливо зрозуміти, як саме IPSec перетворює абстрактні політики безпеки на конкретні криптографічні операції.

Ключові особливості SA

1) **Односпрямованість:** Важливою архітектурною особливістю SA є те, що вона працює лише в одному напрямку. Якщо двом хостам А та Б необхідно обмінюватися даними, вони повинні встановити щонайменше дві асоціації безпеки: одну для трафіку від А до Б, і іншу – від Б до А. Це дозволяє використовувати різні ключі або навіть різні алгоритми для вхідного та вихідного трафіку, що підвищує гнучкість системи.
2) **Унікальна ідентифікація:** Кожна SA унікально ідентифікується трійкою параметрів:
   – **SPI (Security Parameter Index):** 32-бітне число, що генерується отримувачем і додається у заголовок кожного пакету IPSec: ESP або AH. SPI слугує вказівником на конкретний запис у базі даних асоціацій.
   – **IP-адреса призначення:** Адреса вузла, який буде розшифровувати пакет (кінцева точка тунелю).

– **Ідентифікатор протоколу безпеки:** Вказує, чи це асоціація для протоколу AH (IP proto 51) чи ESP (IP proto 50).

3) **Час життя:** Кожна SA має обмежений час існування, який визначається або часовим інтервалом в 3600 секунд, або обсягом переданих даних, наприклд 100 МБ. Існують поняття «м'якого ліміту», коли система починає процес переузгодження нових ключів, і «жорсткого ліміту», коли стара SA видаляється і трафік блокується, якщо нова SA ще не створена.

3.2 База даних політик безпеки (Security Policy Database)

Якщо SA відповідає за те, як захищати дані, то SPD відповідає за те, що саме потрібно захищати. SPD — це, по суті, набір правил, аналогічний правилам firewall, який керує обробкою всіх IP-пакетів.

Селектори трафіку

Для класифікації трафіку SPD використовує набір полів заголовка пакету, які називаються селекторами. Зазвичай використовується кортеж із п'яти елементів:

– IP-адреса джерела.
– IP-адреса призначення.
– Протокол транспортного рівня (TCP, UDP, ICMP тощо).
– Порт джерела (для TCP/UDP).
– Порт призначення (для TCP/UDP).

Дії політик

Для кожного пакету, що проходить через мережевий стек, SPD визначає одну з трьох дій:

1) `DISCARD`: Пакет не відповідає вимогам безпеки або заборонений політикою (наприклад, спроба зв'язку з недовіреною підмережею).
2) `BYPASS`: Трафік не потребує захисту IPSec і передається у відкритому вигляді (clear text). Це зазвичай застосовується до службового трафіку або трафіку в локальній довіреній мережі.
3) `PROTECT`: Трафік повинен бути оброблений протоколами IPSec. Ця дія ініціює пошук відповідної SA або запуск процесу її створення.

3.3 База даних асоціацій безпеки (Security Association Database, SAD)

SAD - це репозиторій активних асоціацій безпеки. У той час як SPD містить статичні або налаштовані адміністратором правила, SAD містить динамічні дані, необхідні для шифрування та розшифрування пакетів у реальному часі.

Кожен запис у SAD (SA Entry) містить такі критичні параметри:

– **Ключовий матеріал:** Ключі шифрування та ключі автентифікації.

– **Алгоритми:** Вказівка на те, які саме криптографічні алгоритми обрано для цієї сесії.

– **Sequence Number Counter:** Поточний номер послідовності для вихідних пакетів (для захисту від атак повтору).

– **Anti-Replay Window:** Вікно для відстеження номерів вхідних пакетів.

– **Режим IPSec:** Тунельний або транспортний.

– **MTU шляху:** Дані про максимальний розмір пакету для уникнення фрагментації.

3.4 Взаємодія баз даних та способи їх заповнення

Алгоритм обробки вихідного трафіку

Коли ядро операційної системи відправляє пакет:

1. Здійснюється пошук у SPD за селекторами пакету.
2. Якщо дія — `PROTECT`, система звертається до SAD, шукаючи активну SA, що відповідає цій політиці.
3. Якщо SA знайдено: пакет шифрується/підписується з використанням параметрів із SAD.
4. Якщо SA відсутня: система призупиняє пакет і ініціює процес Internet Key Exchange для створення нової SA. Після успішного створення запис додається в SAD, і пакет обробляється.

Алгоритм обробки вхідного трафіку

1. При отриманні пакету з заголовком ESP/AH, система зчитує значення SPI.
2. За значенням SPI здійснюється прямий пошук у SAD.

3. Пакет розшифровується та перевіряється його цілісність.
4. Після розшифрування «чистий» пакет перевіряється через SPD. Це необхідно для захисту від атак, коли зловмисник інкапсулює пакет, який не мав би права проходити через цей тунель. Якщо розшифрований пакет не відповідає політиці, він відкидається.

Способи заповнення SPD та SAD

Існує два основні підходи до управління цими базами:

– **Ручний метод:** Адміністратор вручну вносить записи в SPD і SAD, прописуючи ключі та SPI у конфігураційних файлах на обох сторонах. *Недоліки:* Ключі не змінюються, неможливість масштабування, високий ризик людської помилки. Використовується вкрай рідко, переважно для налагодження.

– **Автоматичний метод (IKE/IKEv2):**

– SPD заповнюється адміністратором, який визначає, що нам потрібно захистити.

– SAD заповнюється автоматично демоном IKE (наприклад, StrongSwan, Libreswan, Windows IKE service). Демон домовляється про ключі з віддаленою стороною і динамічно додає записи в ядро ОС. Коли час життя SA спливає, IKE автоматично оновлює ключі та записи в SAD.

4 ДОСЛІДЖЕННЯ СТРУКТУРИ ЗАГОЛОВКІВ ТА ОБРОБКИ ПАКЕТІВ

4.1 Протокол Authentication Header

Протокол AH (RFC 4302) забезпечує цілісність без встановлення з'єднання та автентифікацію походження даних для IP-пакетів. Крім того, він може забезпечувати захист від атак повтору за допомогою механізму змінного вікна.

Структура заголовка AH

Заголовок AH розміщується після IP-заголовка і перед заголовком протоколу транспортного рівня в транспортному режимі або перед інкапсульованим IP-заголовком у тунельному режимі. Його структура є фіксованою, за винятком поля ICV змінної довжини.

Поле	**Розмір (біт)**	**Опис та призначення**
Next Header	8	Вказує тип протоколу, що слідує за заголовком AH (наприклад, 6 для TCP, 17 для UDP, 4 для IPv4 в тунельному режимі). Значення беруться з реєстру IP Protocol Numbers.
Payload Length	8	Довжина заголовка AH у 32-бітних словах, мінус 2. Наприклад, для стандартного заголовка AH (24 байти для SHA-1) це поле дорівнюватиме 4.
Reserved	16	Зарезервовано для майбутнього використання. Повинно бути встановлено в нуль відправником та ігноруватися отримувачем.
SPI (Security Parameters Index)	32	Довільне 32-бітне значення, що разом з IP-адресою призначення та протоколом (AH) ідентифікує конкретну асоціацію безпеки (SA). Діапазон 1-255 зарезервовано IANA.
Sequence Number	32	Монотонно зростаючий лічильник пакетів. Використовується для захисту від атак повтору. Це поле є обов'язковим, навіть якщо сервіс anti-replay не активовано (хоча в такому випадку перевірка не виконується).
ICV (Integrity Check Value)	Змінний	Значення перевірки цілісності (цифровий підпис). Довжина залежить від алгоритму автентифікації (наприклад, HMAC-SHA1-96, HMAC-MD5-96). Поле вирівнюється до границі 32 біт.

Таблиця 4.1 – Структура полів заголовка AH

Особливості обробки пакетів AH

Вихідна обробка:

1. Система визначає SA для пакета.
2. Формується заголовок AH:
   - `Next Header` встановлюється на тип наступного протоколу.
   - `SPI` копіюється з SA.
   - `Sequence Number` інкрементується.
3. Обчислюється ICV. Важливо: перед обчисленням хешу **змінні поля IP-заголовка** (mutable fields), такі як TOS, TTL, Header Checksum, занулюються, оскільки вони змінюються на маршруті. Незмінні поля та весь payload включаються в хеш.
4. Заголовок AH вставляється в пакет.

Вхідна обробка:

1. За SPI, IP призначення та протоколом AH знаходиться відповідна SA.
2. Перевіряється Sequence Number (якщо увімкнено захист від повторів): номер має потрапляти у вікно приймання і не бути раніше прийнятим.
3. Обчислюється ICV для отриманого пакета (знову занулюючи змінні поля IP).
4. Обчислене ICV порівнюється з отриманим. Якщо вони не співпадають,

пакет відкидається і подія логується.

4.2 Протокол Encapsulating Security Payload (ESP)

Структура заголовка та трейлера ESP

ESP огортає дані: заголовок йде перед даними, а трейлер та ICV — після.

1. **ESP Header (перед даними):**
   - `SPI (32 біт)`: Ідентифікатор SA.
   - `Sequence Number (32 біт)`: Лічильник для захисту від повторів.
2. **Payload Data (Змінний):** Власне дані, що захищаються: транспортний сегмент або весь IP-пакет. Дане поле шифрується.
3. **ESP Trailer (після даних, шифрується):**
   - `Padding (0-255 байт)`: Заповнювач для вирівнювання довжини даних до розміру блоку шифрування або для приховування реальної довжини трафіку.
   - `Pad Length (8 біт)`: Вказує довжину поля Padding у байтах.
   - `Next Header (8 біт)`: Тип даних, що містяться в полі Payload Data (аналогічно полю Protocol в IP).
4. **ESP ICV (в кінці, не шифрується):** Значення перевірки цілісності. Обчислюється по всьому пакету ESP (Header + Data + Trailer), але без IP-заголовка.

4.3 Порівняльний аналіз режимів роботи: Транспортний vs Тунельний

Особливості обробки вхідних та вихідних пакетів ESP

Вихідна обробка (Outbound):

1. **Інкапсуляція:** Додається Padding, щоб вирівняти дані до розміру блоку шифрування. Формується Trailer.
2. **Шифрування:** Payload Data, Padding, Pad Length та Next Header шифруються обраним алгоритмом.
3. **Автентифікація:** Обчислюється ICV по зашифрованій частині та ESP-заголовку (SPI + SeqNum). ICV додається в кінець пакета.
4. **Формування IP:** Додається IP-заголовок оригінальний або новий

тунельний.

Вхідна обробка (Inbound):

1. **Перевірка:** Заголовки перевіряються, шукається SA.
2. **Автентифікація:** Обчислюється ICV та порівнюється з отриманим. Якщо не співпадає – пакет відкидається до спроби дешифрування.
3. **Перевірка Anti-Replay:** Перевіряється Sequence Number.
4. **Дешифрування:** Якщо перевірки пройдені, дані розшифровуються.
5. **Видалення Padding:** За полем Pad Length видаляється заповнювач, відновлюється оригінальний пакет.

Режим	**Транспортний**	**Тунельний**
Призначення	Захист трафіку між двома кінцевими хостами.	Захист трафіку між шлюзами або хостом і шлюзом.
IP заголовок	Зберігається оригінальний IP-заголовок.	Створюється новий зовнішній IP-заголовок. Оригінальний пакет стає навантаженням.
Структура AH	`[Orig IP][AH][TCP/UDP Data]`	`[New IP][AH][Orig IP][Data]`
Структура ESP	`[Orig IP][ESP Hdr][TCP Data (Encrypted)][ESP Trlr][ICV]`	`[New IP][ESP Hdr][Orig IP + Data (Encrypted)][ESP Trlr][ICV]`
NAT	Проблематично для AH. ESP працює через NAT-T.	Найбільш поширений варіант для VPN. ESP працює стабільно.

Таблиця 4.2 – Структура пакетів у різних режимах