НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ № 2

з дисципліни:

«ПРОЕКТУВАННЯ, РОЗРОБКА І РЕАЛІЗАЦІЯ КРИПТОГРАФІЧНИХ СИСТЕМ»

Дослідження реалізацій протоколів IPSec

Виконала:

Студентка групи ФІ-22мн

Калитюк Дар’я

КИЇВ 2023

Мета роботи: дослідження особливостей реалізації криптографічних механізмів протоколів IPSec.

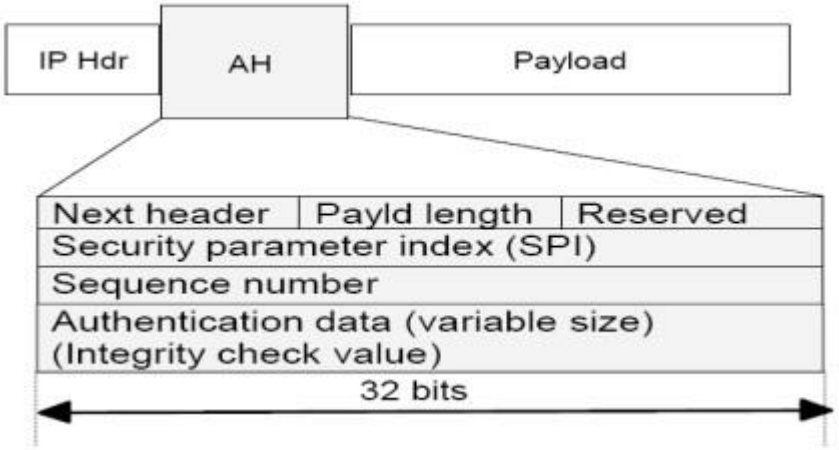
Хід роботи

IPsec — це стек протоколів і стандартів, які визначають механізми забезпечення цілісності і конфіденційності для комунікацій на мережевому та транспортному рівнях, що дозволяє використовувати його для захисту будь-яких протоколів, що базуються на стеку протоколів TCP/IP (ICMP, UPD тощо). IPSec може працювати в двох режимах: тунельному та транспортному. Тунельний режим використовується для захисту всього пакету даних, який включає в себе заголовок та корисне навантаження (payload). Весь пакет обгортається новим заголовком (тунельним заголовком), і такий "запакований" пакет передається через мережу. Тунельний режим широко використовується для створення віртуальних приватних мереж (VPN). Транспортний режим застосовується для захисту самого тіла (payload) IP-пакету, залишаючи незахищеним заголовок оригінального пакету.

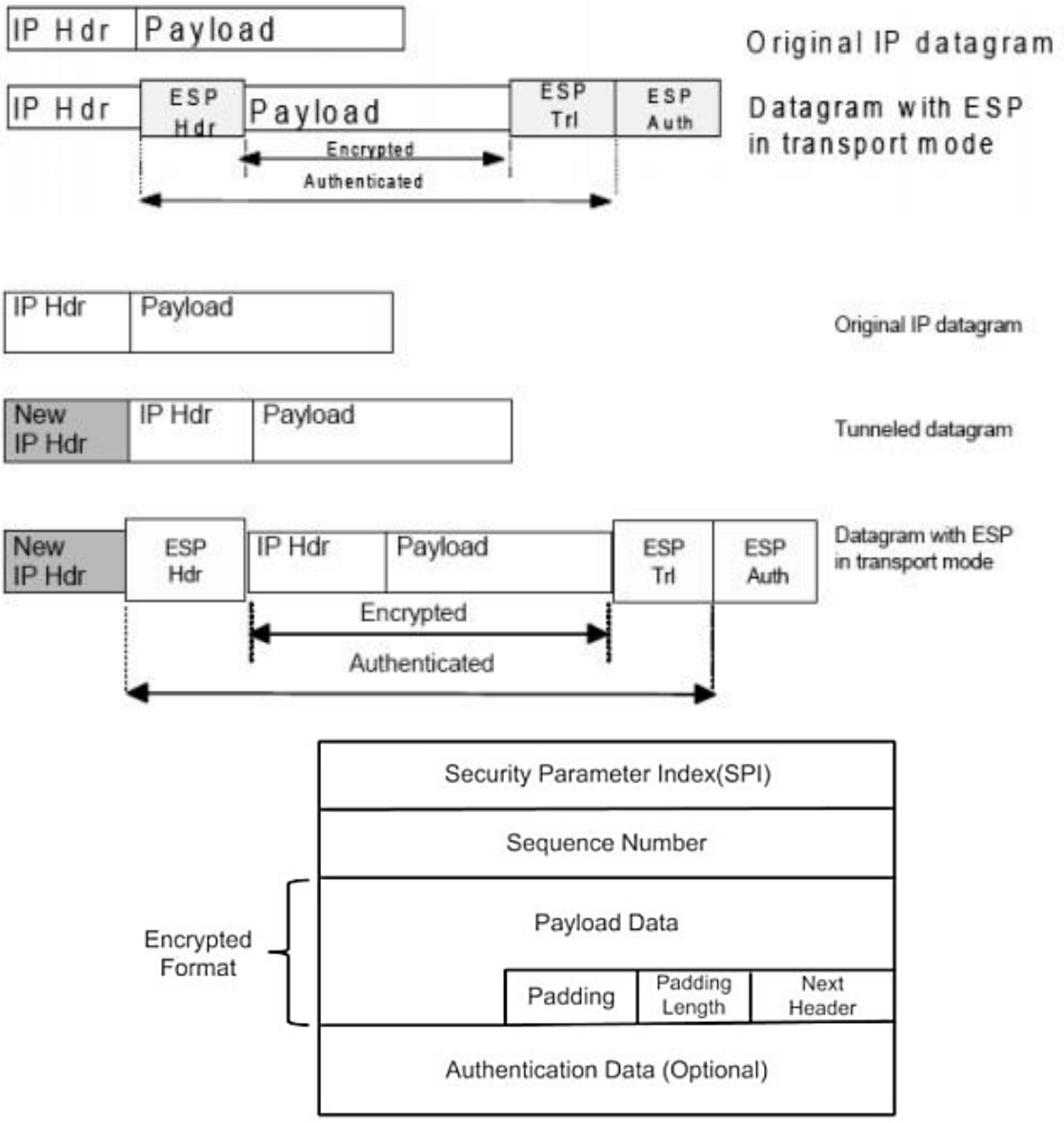
У IPsec використовуються три основні протоколи:

- Заголовок автентифікації (Authentication Header, AH)
- Безпека інкапсульованого корисного навантаження (Encapsulated Security Payload, ESP)
- Обмін ключами в Інтернеті (Internet Key Exchange, IKE)

AH слугує для підтвердження цілісності повідомлення, автентифікації джерела (які забезпечує використання HMAC) і захисту під повторного відтворення (яке забезпечується за допомогою поля порядкового номера із заголовком AH).



Протокол ESP забезпечує конфіденційність даних і автентифікацію. ESP можна використовувати лише з конфіденційністю, лише з автентифікацією або як з конфіденційністю, так і з автентифікацією. Різниця в автентифікації в протоколах AH та ESP полягає в охопленні даних: так, AH автентифікація автентифікує весь пакет, а ESP – його частину.



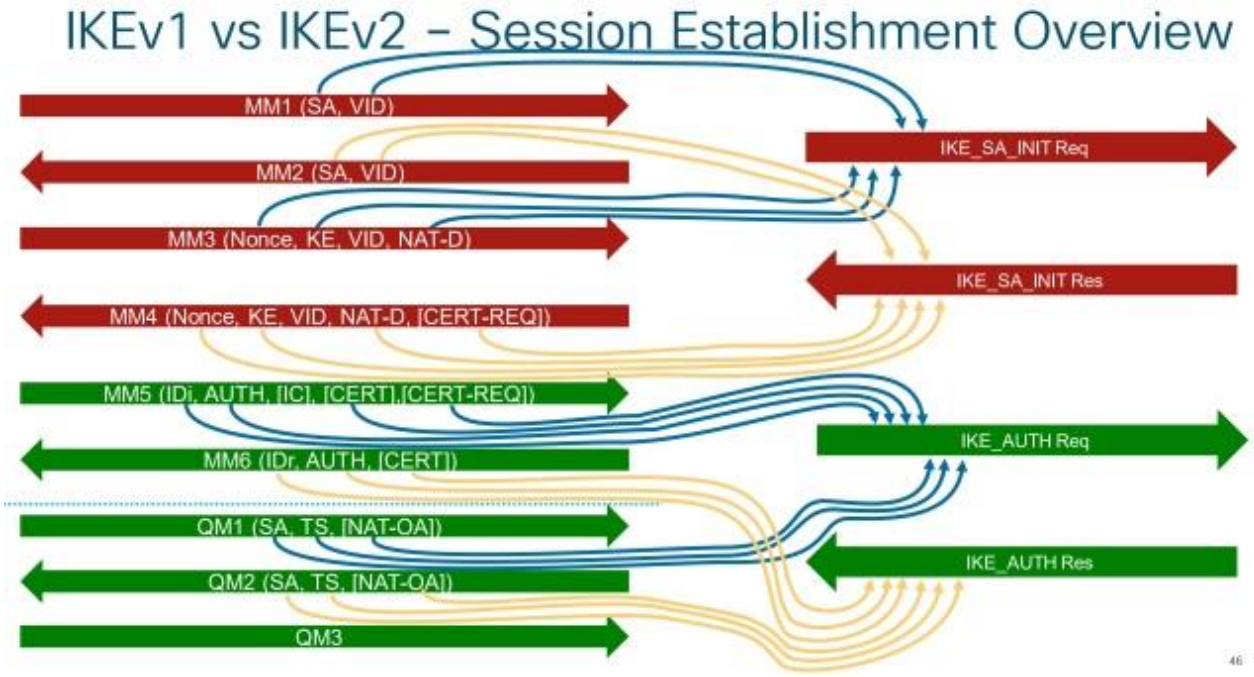
IKE (Internet Key Exchange) - це протокол обміну ключами, який використовується для автоматизації процесу встановлення безпеки в IPSec. В основному, IKE використовується разом з протоколом ISAKMP (Internet Security Association and Key Management Protocol). Протокол IKE включає дві фази роботи: Main mode і Quick (Aggressive) mode. Основна мета першої фази - це узгодження параметрів та обмін ключами для безпеки взаємодії. Друга фаза призначена для встановлення *Security Associations* (SA) для встановлення тунелю для передачі даних. SA визначає наступні елементи: протокол безпеки, алгоритми шифрування та гешування, ключі, атрибути безпеки, ідентифікатори сторін тощо. SA має обмежений "життєвий цикл" (SA Lifetime), після закінчення якого відбувається перегенерація ключів і оновлення параметрів безпеки.

Основні відмінності IKEv2 від IKEv1:

- Зменшення кількості обмінів для встановлення SA;
- вбудована підтримка обходу трансляції мережевих адрес NAT-T;
- підтримка MOBIKE (Mobility and Multi-homing Protocol);
- підтримка EAP (Extensible Authentication Protocol) автентифікації;
- підтримка протоколу IPv6;
- певний рівень захисту від DoS атак;

Kerberized Internet Negotiation of Keys (KINK):

- централізоване управління політиками безпеки;
- автентифікацію однорангових користувачів виконує довірена третя сторона – Центр Розподілу Ключів;



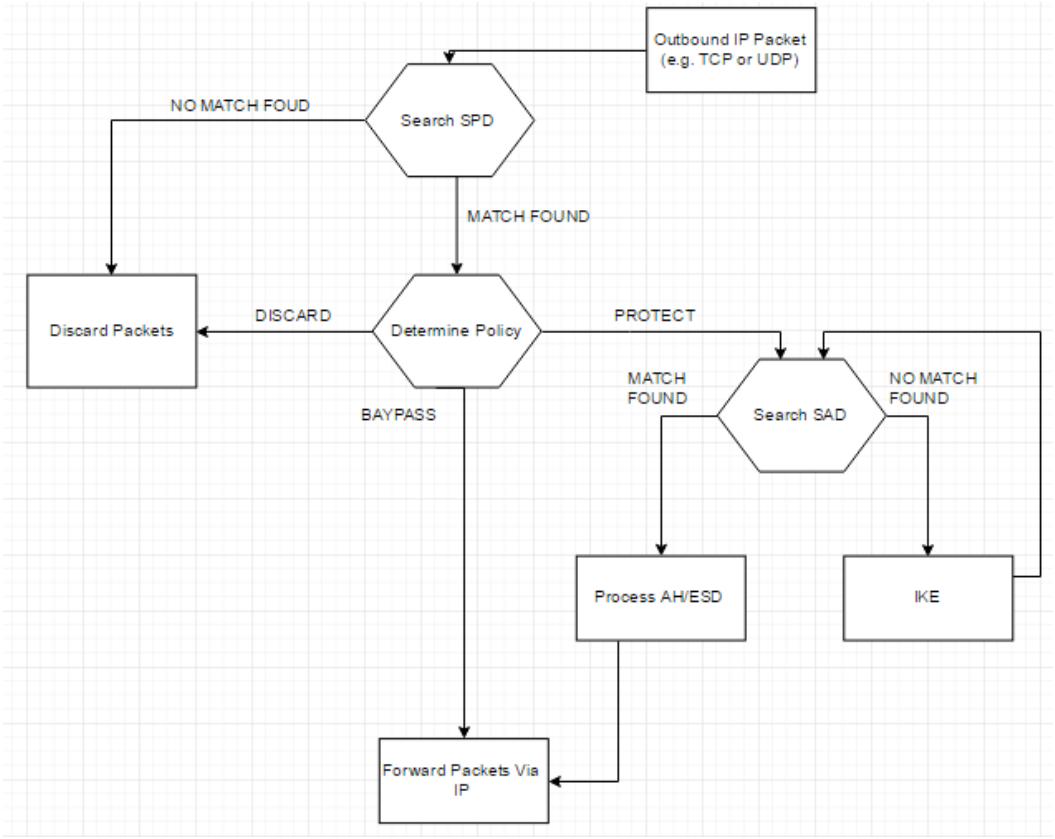
Security Association Database (SAD) – це таблиця, яка зберігає інформацію про активні SA вхідного та вихідного трафіку. SAD заповнюється динамічно під час процесу встановлення безпеки, зокрема, після встановлення SA. Кожна SA ідентифікується трьома параметрами:

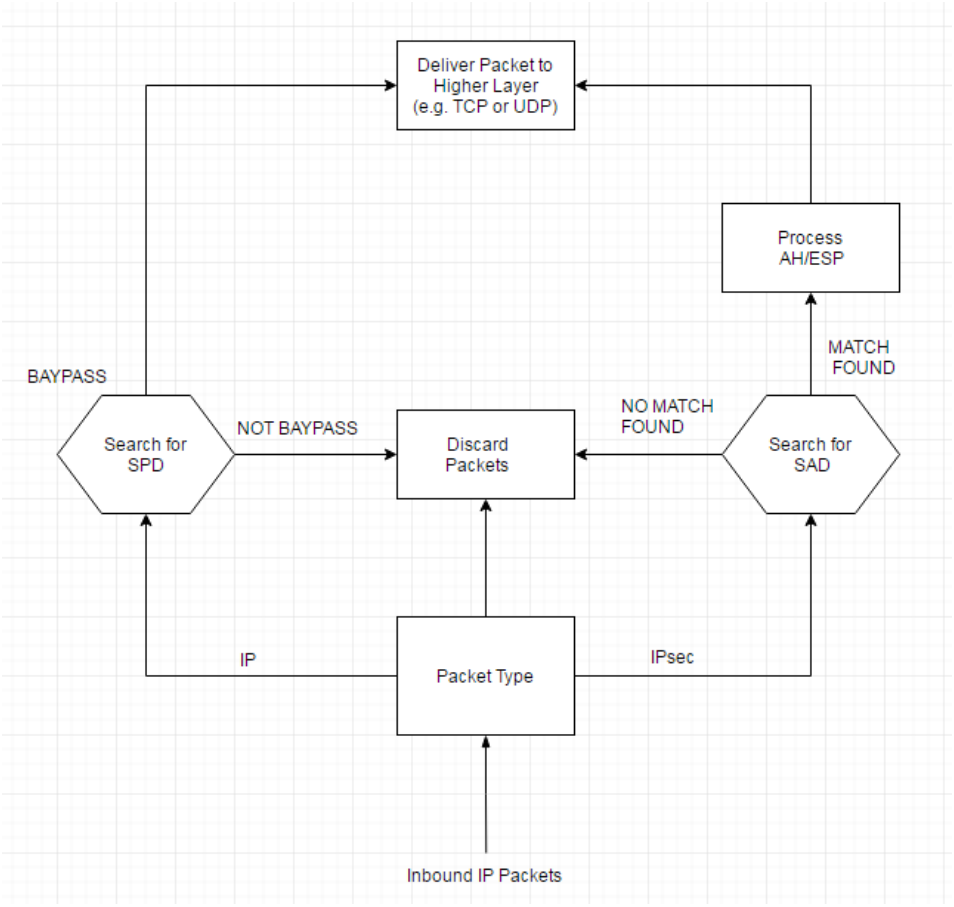
- Security Parameters Index, SPI
- Destination Address
- Ідентифікатор протокола безпеки (ESP або AH)

В SAD зберігаються наступні дані:

- Security Parameter Index
- Destination Address
- Sequence Number
- Anti-Replay Window
- IP Security Protocol
- Algorithm
- Key
- SA Lifetime
- IPSec

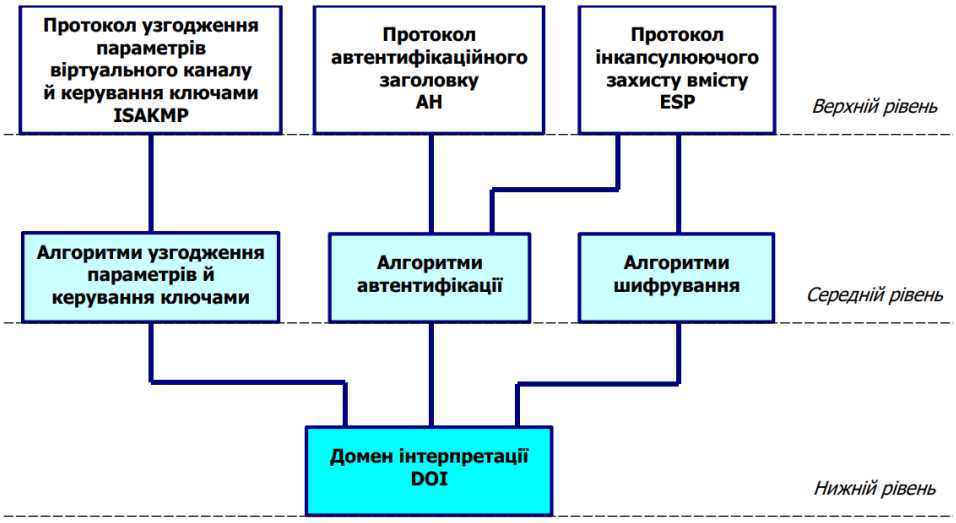
Security Policy Database (SPD) є впорядкованим набором правил і політик безпеки. SPD фільтрує IP-трафік, щоб визначити, як потрібно обробляти пакети. Для вихідних пакетів SPD і SAD визначають, який рівень захисту застосовувати. Для вхідних пакетів SPD допомагає визначити, чи прийнятний рівень захисту пакета.


Outbound IP Packet
(e.g. TCP or UDP)
Search SPD
NO MATCH FOUD
MATCH FOUND
Discard Packets
DISCARD
Determine Policy
PROTECT
BAYPASS
MATCH
FOUND
Search SAD
NO MATCH
FOUND
Process AH/ESD
IKE
Forward Packets Via
IP


Deliver Packet to
Higher Layer
(e.g. TCP or UDP)
Process
AH/ESP
MATCH
FOUND
BAYPASS
Search for
SPD
NOT BAYPASS
Discard
Packets
NO MATCH
FOUND
Search for
SAD
IP
Packet Type
IPsec
Inbound IP Packets

Архітектура засобів захисту IPsec:

- Верхній рівень: протоколи захисту віртуального каналу і узгодження параметрів захисту;
- Середній рівень: криптографічні алгоритми, що використовуються в протоколах AH та ESP, алгоритми узгодження і керування ключами, які використовує протокол IKE;
- Нижній рівень: домен інтерпретації (DOI) – база даних, яка містить інформацію про усі протоколи і алгоритми, що застосовуються в IPSec, а також про їхні параметри, ідентифікатори тощо.



Криптографічні алгоритми в IPsec

Обмін ключами	Автентифікація	Гешування	Шифрування
DH, ECDH	PSA, PSK, ECDSA	HMAC – SHA2	AES-GCM, ChaCha20-Poly1305

Особливості основних схем застосування протоколів IPSec для встановлення VPN-тунелю:

Тип з'єднання	Особливості	Приклад використання
Хост-хост	Кожен хост є кінцевим пунктом VPN–тунелю. Обидва хости повинні бути налаштовані для підтримки IPSec.	Забезпечення безпеки комунікації між конкретними комп'ютерами.
Шлюз-шлюз	VPN–тунель між двома мережами через їхні шлюзи. Кожен шлюз повинен підтримувати IPSec.	Безпечне з'єднання двох віддалених мереж через Інтернет.
Хост-шлюз	Один чи кілька хостів підключаються до центрального шлюзу. Кожен хост та шлюз повинні підтримувати IPSec.	Забезпечення безпеки комунікації між індивідуальним комп'ютером та центральним шлюзом, наприклад, в корпоративних мережах або VPN.