Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут»
Фізико-технічний інститут

Проектування, розробка та реалізація криптографічних систем

Лабораторна робота № 2

Виконали:
студенти 6-го курсу
групи ФІ-32м
Кушнір І.І.
Деркач О.Г.
Перевірив:
Фесенко А.В.

Київ 2014

Стек протоколів IPSec (Internet Protocol Security) використовується для автентифікації учасників обміну, тунелювання трафіку, забезпечення цілісності і шифрування IP-пакетів. Основне завдання протоколу IPSec – забезпечення безпечного передавання даних по мережах IP. Сумісний з протоколом IPv4 та обов'язковий для протоколу IPv6.

Захист даних за допомогою протоколів AH та ESP

Протоколи AH та ESP можуть працювати в тунельному та транспортному режимах. Для виконання своїх завдань із забезпечення безпечного передавання даних проколи AH та ESP додають до оброблюваних пакетів додаткову служебну інформацію, оформляючи її у вигляді заголовків.

Протокол AH (Authentication Header)

Протокол AH забезпечує перевірку автентичності і цілісності IP-пакетів, а також захист від відтворення раніше надісланих IP-пакетів. Не забезпечує конфіденційність даних, що передаються, тобто не призначений для шифрування даних. Цілісність і автентичність даних забезпечуються додаванням заголовку перед заголовком IP і заголовком транспортного рівня (TCP/UDP). Формат заголовку AH показаний на рисунку 1.

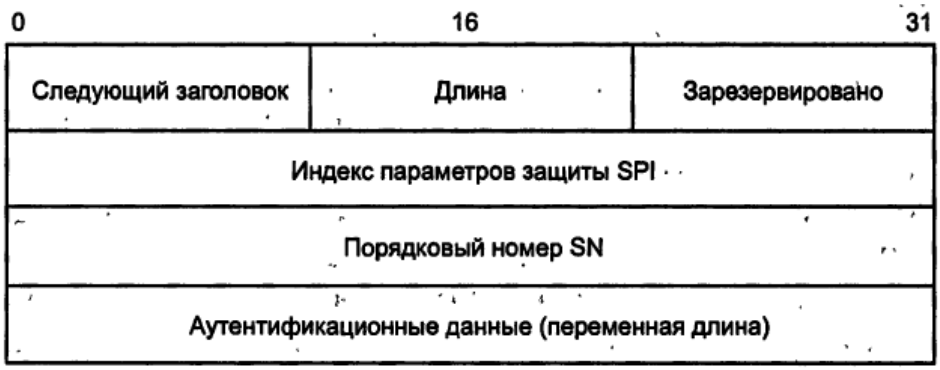

Рис. 1. Формат заголовку AH

Заголовок AH складається із наступних полів:

- наступний заголовок (Next Header) – однобайтове поле, що містить код протоколу наступного заголовку, вкладеного в IPSec-пакет, наприклад код протоколу TCP чи ESP, чий заголовок слідує за AH;

- довжина (Payload Len) – вказує довжину заголовка AH в 32-бітних словах;
- індекс параметрів захисту SPI (Security Parameters Index) – представляє собою 32-розрядну мітку безпечної асоціації SA, що містить всі параметри тунелю IPSec, включаючи типи криптографічних алгоритмів і ключі шифрування. На основі індексу SPI пакет буде правильно віднесений до однієї із існуючих асоціацій на приймаючій стороні. Якщо ж активної асоціації, на яку вказує мітка SPI, не існує, то пакет просто відкидається;
- SN (Sequence Number) – без знакове 32-бітне число, що збільшується на одиницю після передавання кожного IP-пакета, захищеного протоколом AH. Забезпечує захист від фальшивого відтворення надісланих раніше IP-пакетів. При формуванні кожного захищеного сеансу обміну інформацією в рамках протоколу IPSec сторони, що взаємодіють, роблять свої лічильники нульовими, а потім узгодженим чином збільшують їх. Отримувач перевіряє це поле з ціллю запевнитися, що пакет з таким номером ще не був прийнятий. Якщо такий пакет вже був, то він не приймається;
- автентифікаційні дані (Authentication Data) – поле змінної довжини, що містить інформацію, яка використовується для автентифікації пакету, і називається MAC-кодом (Message Authentication Code). Вміст поля обчислюється за допомогою одного із двох обов’язково підтримуваних протоколом AH алгоритмів, HMAC-MD5 і HMAC-SHA, що базуються на застосуванні односторонніх хеш-функцій із секретними ключами. Довжина MAC залежить від вибраного алгоритму, тому в загальному випадку це поле має змінну довжику.

Протокол AH захищає весь IP-пакет, крім деяких полів в IP-заголовку, таких як TTL (Time to Live), Type of Service, що можуть змінюватися в процесі передавання пакета мережею. Протокол AH забезпечує захист від змін IP-адрес в заголовку пакета.

Протокол AH може використовуватися в тунельному та транспортному режимах.

В транспортному режимі заголовок вихідного IP-пакету стає зовнішнім заголовком, за ним сліду заголовок AH, а потім – всі дані пакету, який захищається. Протокол AH захищає весь отриманий таким чином пакет, включаючи заголовок IP і власне сам заголовок AH. Таким чином, будь-яка зміна даних в пакеті буде помічена.

В тунельному режимі в якості заголовку зовнішнього IP-пакету створюється новий заголовок IP. IP-адреси відправника і отримувача можуть відрізнятися від адрес в заголовці вихідного IP-пакету. В захищеному IP-пакеті внутрішній (початковий) IP-заголовок містить містить цільову адресу пакету, а зовнішній IP-заголовок – адресу кінця тунеля. За новим заголовком зовнішнього IP-пакету слідує заголовок AH, а потім і весь вихідний пакет (заголовок IP і самі дані). Як і у випадку транспортного режиму, протокол AH захищає весь створений пакет (два заголовки IP, заголовок AH і дані), що також дозволяє виявити будь-які зміни в пакеті. Як і в транспортному режимі, сам пакет не захищений від перегляду.

На рисунку 2 зображено розміщення заголовку AH в транспортному і тунельному режимах.

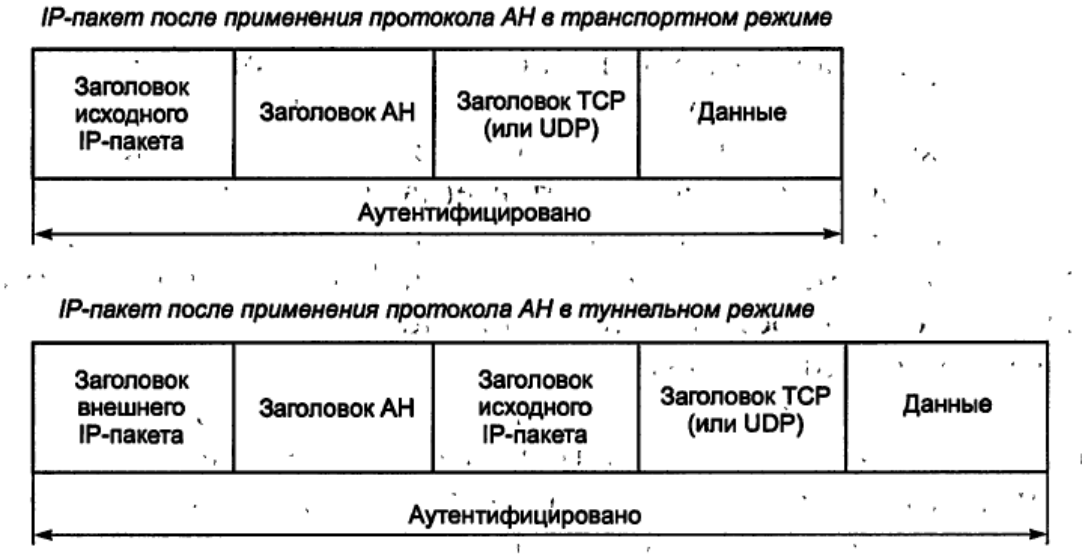

Рис.2. IP-пакет після застосування протоколу AH

Автентифікація по протоколу AH не допускає маніпулювання основними полями IP-заголовку пакета. Тому цей протокол не можна застосовувати в середовищах, де використовується механізм NAT (Network Address Translation), оскільки для його роботи необхідне маніпулювання IP-заголовками.

Протокол AH може застосовуватися самостійно і в комбінації з протоколом ESP чи навіть з пакетом, що вже містить AH-заголовок (вкладене застосування).

Encapsulation Security Protocol (ESP)

Протокол ESP забезпечує конфіденційність, автентичність, цілісність і захист від повторів пакетів даних. Конфіденційність даних протокол ESP забезпечує завжди, а цілісність і автентичність є для нього опціональними вимогами. Конфіденційність даних забезпечується шляхом шифрування вмісту окремих пакетів. Цілісність і автентичність забезпечуються шляхом обчислення MAC.

Структура заголовку ESP зображена на рисунку 3.

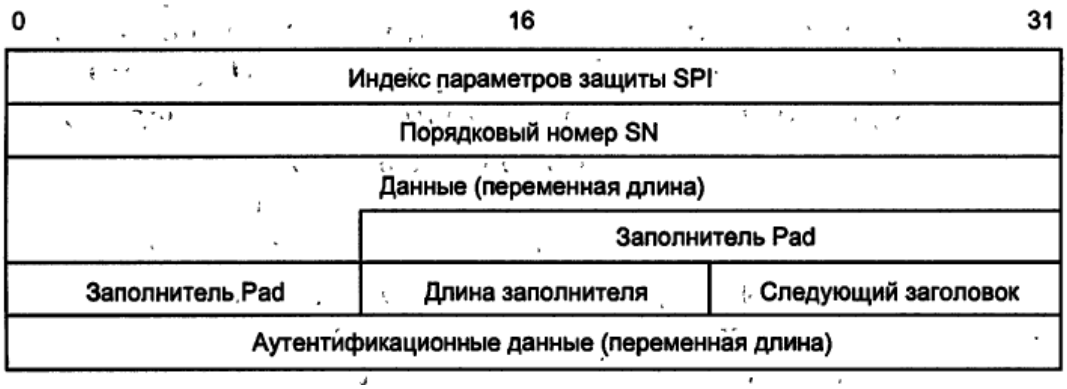

Рис. 3. Формат залоговку ESP

Заголовок ESP містить наступні поля:

- SPI (Security Parameters Index) – вказує відповідну SA;
- порядковий номер SN (Sequence Number) – забезпечує захист від повторів для SA. Представляє собою 32-бітне число, що спочатку дорівнює 1 і збільшується з кожним кроком на 1. Воно не повторюється циклічно і вказує номер пакету, що відправляється згідно даної SA;

отримувач перевіряє це поле із ціллю впевнитися, що пакет з таким номером ще не був отриманий. Якщо пакет з таким номером вже був, то він не приймається;

- дані (Payload Data);
- Padding – дописується від 0 до 255 байт для вирівнювання із розміром блоку шифру;
- Padding Length - вказує на довжину поля Padding в байтах;
- наступний заголовок (Next Header) – вказує природу даних, що передаються (наприклад, TCP чи UDP);
- Authentication Data – містить код перевірки цілісності ICV і код автентичності повідомлення, що використовуються для перевірки справжності відправника і цілісності повідомлення. Значення ICV обчислюється для заголовку ESP, даних, що передаються, і кінцевої мітки ESP. Це поле додається до заголовку ESP тільки при ввімкненій автентифікації.

Заголовок ділиться на дві частини, що розділяються полем даних Payload Data. Перша частина, що надалі буде позначатися як заголовок ESP, складається з полів SPI і SN, і розміщується перед полем даних. Решта служебник полів протоколу ESP розміщуються вкінці пакету. Безпосередньо за полем даних слідує так званий трейлер, в який входять Padding, Padding Length, Next Header. Завершує пакет поле контролю цілісності Authentication Data.

Протокол ESP може використовуватися в транспортному та тунельному режимах.

В транспортному режимі зашифровані дані транспортуються безпосередньо між хостами. В транспортному режимі протоколу ESP заголовок вихідного IP-пакету залишається зовнішнім. Заголовок ESP вставляється в пакет, що передається, після IP-заголовку. Шифруванню піддаються лише дані вихідного IP-пакету і ESP trailer. В цьому режимі ESP не шифрує заголовок IP-пакету, інакше маршрутизатор не зможе прочитати

поля заголовку і коректно здійснити просування пакету між мережами. Не шифруються також поля SPI та SN, які повинні передаватися у відкритому вигляді для того, щоб отриманий пакет можна було віднести до певної SA і захиститися від фальшивого відтворення пакету.

На відміну від протоколу AH, контроль цілісності і автентичності даних в протоколі ESP не поширюється на заголовок вихідного пакету, і тому має сенс застосування обох протоколів одночасно: ESP для шифрування і AH для контролю цілісності.

В тунельному режимі основна роль відводиться шлюзам безпеки, оскільки вважається, що клієнтські станції чи сервери можуть не підтримувати IPSec і відправляють в мережу звичайний IP-трафік. Перед тим як досягнути каналів глобальної мережі, кожен вихідний IP-пакет спочатку потрапляє в шлюз, який розміщує цей пакет повністю в «оболонку» IPSec, зашифровуючи його вміст разом із вихідним IP-заголовком. Щоб забезпечити можливість маршрутизаціх отриманого пакету, шлюз додає до нього новий IP-заголовок і тільки після цього відправляє в мережу. Шлюз, що знаходиться на протилежному кінці з'єднання, розшифровує цей пакет і передає його на кінцевий пристрій в початковому вигляді. Описана процедура називається тунелюванням. В тунельному режимі в якості зовнішнього заголовку створюється новий заголовок IP. Весь вихідний IP-пакет (і дані, і заголовок IP) і ESP trailer шифруються. Тому адресна інформація вихідного IP-пакету недоступна для перегляду. Заголовок зовнішнього IP-пакету протоколом ESP не захищається.

Розміщення заголовків ESP в тунельному і транспортному режимах зображене на рисунку 4.

Протокол ESP може застосовуватися окремо чи разом із протоколом AH. В транспортному режимі протокол AH повинен застосовуватися після протоколу ESP. В тунельному режимі протоколи AH і ESP застосовуються до різних вкладених пакетів і, крім того, допускається багаторазова вкладеність тунелів з різними початковими і/чи кінцевими точками.

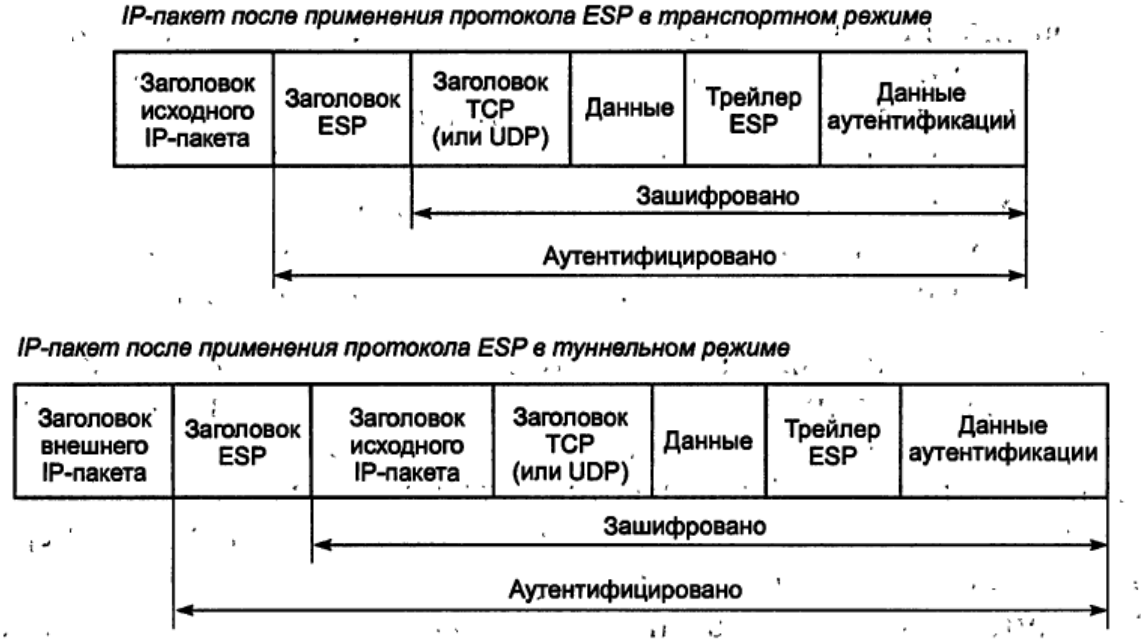

Рис. 4. IP-пакет після застосування проколу ESP в транспортному і тунельному режимах

Протокол керування ключами IKE (Internet Key Exchange)

Роль інфраструктури, яка забезпечує розподіл ключів та узгодження протоколів між учасниками обміну, виконує група протоколів IKE. Ця назва прийшла на зміну більш ранній – ISAKMP/Oakley (Internet Security Association and Key Management) в 1998 році.

Протокол ISAMKMP дозволяє узгодити алгоритми і математичні структури для процедури обміну ключами Діффі-Хеллмана, а також процесів автентифікації. Протокол Oakley засновуй на алгоритмі Діффі-Хеллмана і слугує для організації безпосереднього обміну ключами.

Протоколи IKE виконують наступні завдання:

- здійснюють автентифікацію сторін, що взаємодіють, узгоджують алгоритми шифрування і характеристики ключів, які будуть використовуватися в захищеному сеансі обміну інформацією;
- забезпечують створення ключової інформації з'єднання і керують нею, безпосередній обмін ключами (в тому числі і можливість їх частої зміни);

- керують параметрами з'єднання і захистом від деяких типів атак, контролюють виконання всіх досягнутих домовленостей.

Встановлення SA (Security Association)

Для того, щоб протоколи AH та ESP могли виконувати свою роботу із захисту даних, між двома кінцевими точками повинна бути сформована SA. SA представляє собою домовленість про захист даними між двома партнерами, що взаємодіють.

Встановлення SA повинно починатися із взаємної автентифікації сторін. Для виконання автентифікації сторін в IKE застосовуються два основних способи. Перший спосіб базується на використанні спільного секрету. Перед ініціалізацією IPSec-пристроїв, що утворюють SA, в їх бази даних записується попередньо розподілений спільний секрет. Цифровий підпис на основі односторонньої функції, яка використовує в якості аргумента цей попередньо розподілений спільний секрет, доводить автентичність протилежних сторін. Другий спосіб базується на використанні цифрових підписів і цифрових сертифікатів стандарту X.509: кожна із сторін підписує свій цифровий сертифікат своїм закритим ключем і передає ці дані протилежній стороні. Якщо підписаний сертифікат розшифровується відкритим ключем відправника, то це підтверджує той факт, що відправник дійсно володіє відповідним закритим ключем. Сертифікат повинен бути підписаний не лише його власником, але і CA (Certification Authority).

Після проведення взаємної автентифікації сторони, що взаємодіють, можуть безпосередньо перейти до узгодження параметрів захищеного каналу. Параметри, що вибираються для SA, визначають протокол, що використовується для забезпечення безпеки передачі даних; алгоритм автентифікації протоколу AH, та його ключі; алгоритм шифрування, що використовується протоколом ESP, та його ключі; наявність чи відсутність криптографічної синхронізації; способи захисту сеансу обміну; частоту зміни ключів та ряд інших параметрів. Важливим параметром SA є так званий

криптографічний матеріал, тобто секретні ключі, що використовуються під час роботи протоколів AH та ESP.

Параметри SA повинні задовольняти обидві кінцеві точки захищеного каналу, тому під час використання автоматичної процедури встановлення SA протоколи IKE, що працюють на різних сторонах каналу, вибирають параметри в ході переговорного процесу. SA представляє собою одно направлене логічне з'єднання, тому під час двохстороннього обміну даними, необхідно встановлювати дві SA. В рамках однієї SA може працювати лише один із протоколів – або AH, або ESP, але не обидва разом.

Бази даних SAD (Security Associations Database) та SPD (Security Policy Database)

В кожному вузлі, що підтримує IPSec, використовуються бази даних двох типів: SAD та SPD.

Набори поточних параметрів, що визначають всі активні SA, зберігаються на обох кінцевих вузлах захищеного каналу у вигляді баз даних SAD. Кожен вузол IPSec підтримує дві бази SAD: одну для вихідних, а іншу для вхідних SA.

База даних SPD створює відповідність між IP-пакетами і встановленими для них правилами обробки. Під час обробки пакетів бази даних SPD використовуються разом із базами даних SAD. База даних SPD представляє собою впорядкованих набір правил, кожне із яких включає сукупність селекторів і допустимих політики безпеки. Селектори використовуються для відбору пакетів, а політики безпеки задають необхідну обробку. Така база даних формується і підтримується на кожному вузлі, де встановлене програмне забезпечення IPSec. Політика безпеки передбачає три можливих варіанта обробки IP-пакета: відкидання пакету, передача без змін та обробка засобами IPSec. Кожен вузол IPSec повинен підтримувати дві бази SPD: одну для вихідного трафіка, одну для вхідного.