Безпека операційних систем і комп'ютерних мереж

Лекція 20

Віртуальні приватні мережі - VPN

План

- Поняття про віртуальні захищені (приватні) мережі (VPN)
- Види віртуальних приватних мереж
- Сервіси VPN
- Способи утворення захищених тунелів
- Рівні реалізації VPN
- Протоколи: SSL, SOCKS, IPSec, PPTP, L2F, L2TF

Захист інформації в процесі передавання її відкритими каналами зв’язку

базується на виконанні таких функцій:

- автентифікація сторін, що взаємодіють;
- криптографічне закриття інформації, яка передається;
- підтвердження справжності й цілісності доставленої інформації;
- захист від повтору, затримки та видалення повідомлень;
- захист від відмовлення від фактів відправлення й одержання повідомлень.

Поняття про віртуальні приватні мережі (VPN)

- Об’єднання локальних мереж і окремих комп’ютерів через відкрите зовнішнє середовище передавання інформації в єдину віртуальну мережу, яка забезпечує захист інформації, що в ній циркулює, називається захищеною (або приватною) віртуальною мережею (англ. – *Virtual Private Network*, VPN)
- Термін “віртуальна” означає, що така мережа формується як деяка підмножина реальної мережі, з каналами зв’язку, що моделюються реальними каналами
- Особливою ознакою віртуальної приватної (захищеної) мережі є її відокремлення від реальної мережі, яке повинне бути достатньо надійним для гарантування конфіденційності та цілісності інформації, що в ній передається, а також для забезпечення автентифікації сторін і унеможливлення відмовлення від авторства (англ. – *Non-Repudiation*)

Види віртуальних приватних мереж

- виділяють такі основних види віртуальних приватних мереж:
  - VPN віддаленого доступу (англ. – *Remote Access VPN*)
  - корпоративні VPN (англ. – *Intranet VPN*)
  - міжкорпоративні VPN (англ. – *Extranet VPN*)

VPN віддаленого доступу

- Віртуальні приватні мережі віддаленого доступу дозволяють значно скоротити витрати на використання комутованих та виділених ліній
- Принцип їх роботи:
  - користувачі встановлюють з'єднання з місцевою точкою доступу до глобальної мережі (точкою присутності провайдера Інтернет)
  - дані, які передають користувачі, "тунелюються" через Інтернет, що дозволяє уникнути плати за міжміський та міжнародний зв'язок
  - дані від усіх користувачів концентруються на спеціальних пристроях – шлюзах віртуальної приватної мережі – и передаються у корпоративну мережу
- Перевага: суттєва економія від застосування цього типу VPN
- Небезпека: використання відкритого Інтернету в якості магістралі для транспорту чутливого (конфіденційного) корпоративного трафіка приймає погрожуючі розміри
- Механізми захисту інформації є життєво важливими елементами цієї технології

Корпоративна мережа VPN

- Організації, що бажають організувати для своїх філій та відділень доступ до централізованих сховищ інформації, звичайно підключають віддалені вузли через виділені лінії або з використанням технології Frame Relay (MPLS over IP)
  - Використання виділених ліній означає зростання поточних витрат по мірі збільшення смуги пропускання та відстані між об'єктами
  - Витрати на зв'язок по виділеним лініям перетворюються в одну з головних статей витрат на експлуатацію корпоративної інформаційної системи
- Для скорочення витрат організація може з'єднати вузли за допомогою віртуальної приватної мережі
  - Треба відмовитись від використання дорогих виділених ліній, замінивши їх більш дешевим зв'язком через Інтернет
  - Це суттєво скорочує витрати, оскільки в Інтернеті відстань ніяк не впливає на вартість з'єднання

Міжкорпоративна мережа VPN

- Extranet – це мережна технологія, яка забезпечує прямий доступ з мережі однієї організації до мережі іншої організації і таким чином сприяє підвищенню якості зв’язку, що підтримується в ході ділового співробітництва
- Мережі Extranet VPN в цілому подібні до корпоративних VPN з тією різницею, що проблема захисту інформації є для них ще гострішою
  - Коли кілька організацій приймають рішення працювати разом і відкривають одна для одної свої мережі, вони повинні потурбуватись про те, щоби їхні нові партнери мали доступ лише до визначеного кола інформації
  - При цьому конфіденційна інформація повинна бути надійно захищеною від несанкціонованого використання
  - У міжкорпоративних мережах велике значення повинно надаватись контролю доступу з використанням міжмережних екранів (англ. – *Firewalling*)
  - Також особливо важливою є автентифікація користувачів, яка повинна гарантувати, що доступ до інформації отримують лише ті, кому він дійсно дозволений
  - Розгорнута система захисту від несанкціонованого доступу повинна бути максимально прозорою і не вимагати втручання користувачів

Сервіси VPN

- Автентифікація сторін з’єднання
- Забезпечення конфіденційності
- Забезпечення цілісності даних
- Захист від повторного використання даних
- Запобігання відмовленню від авторства
- Управління ключами

Забезпечення конфіденційності

- Найпростішим і найпоширенішим способом забезпечення конфіденційності інформації є її шифрування, або криптографічне закриття
  - Незважаючи на те, що самі алгоритми шифрування дуже складні, їх реалізація великих утруднень не викликає
  - Доволі значну проблему становить керування ключами, особливо в разі значного збільшення кількості користувачів
  - В реалізації VPN керування ключами є одною з головних проблем, що потребує надійного і ефективного рішення

Застосування апаратних засобів шифрування

- Шифрування має неминучий побічний ефект – деяку втрату продуктивності
- Для уникнення втрати продуктивності можуть ефективно застосовуватись апаратні засоби
  - Апаратно реалізоване шифрування звільняє пристрої захисту від додаткового навантаження, пов'язаного з виконанням алгоритмів шифрування, і забезпечує кодування трафіка без втрати швидкості обміну
  - У разі здійснення атаки на засоби захисту VPN існує загроза підміни програмних компонентів, в тому числі саме тих, що забезпечують шифрування. Загроза несанкціонованого впливу на апаратні засоби є значно менш ймовірною
  - Для апаратної реалізації шифрування застосовуються спеціалізовані інтегральні схеми прикладної орієнтації (англ. – *Application-Specific Integrated Circuit, ASIC*)

Забезпечення цілісності

- Цілісність контролюється використанням математичних алгоритмів хешування
  - Важливо підкреслити, що криптографічні механізми не забезпечують захист цілісності, а лише дозволяють впевнитись, що цілісність не була порушена, або, навпаки, виявити порушення
- Алгоритми хешування також потребують значних ресурсів процесора
  - Це дає підстави реалізовувати виконання цих алгоритмів в апаратних засобах з використанням інтегральних схем прикладної орієнтації

Запобігання відмовленню від авторства

- Запобігання відмовленню від авторства (англ. – Non-Repudiation) – це додаткова функція, що реалізується на базі автентифікації
  - У захищеному спілкуванні часто виникають випадки, коли крім підтвердження того, що абонент є саме тим, за кого він себе намагається видати, важливо отримати незаперечні докази того, що повідомлення одержано від конкретного користувача
  - Також буває необхідним доказове підтвердження того, що певний користувач дійсно одержав деяке повідомлення
- Ці функції захисту у ряді випадків повинні бути невід'ємною складовою реалізації VPN

Способи утворення захищених віртуальних каналів

- Будь-який з двох вузлів віртуальної мережі, між якими формується захищений тунель, може належати кінцевій чи проміжній точці потоку повідомлень, який захищають. Відповідно можливі різні способи утворення захищеного віртуального каналу.
  - кінцеві точки тунелю співпадають з кінцевими точками потоку повідомлень
  - кінцевою точкою захищеного тунелю обирають брандмауер або граничний маршрутизатор локальної мережі, захищений тунель утворюється лише у публічній мережі
  - в якості кінцевих точок захищеного тунелю виступають засоби, що встановлені не на комп'ютерах користувачів, а на площах провайдерів Інтернет

Кінцеві точки тунелю співпадають з кінцевими точками потоку повідомлень

- Цей варіант є найкращим з міркувань безпеки
- Приклади кінцевих точок:
  - сервер у центральному офісі компанії і робоча станція користувача у віддаленій філії
  - портативний комп'ютер співробітника, який перебуває у відрядженні
- Перевагою такого варіанту є те, що захист інформаційного обміну забезпечується на всьому шляху пакетів повідомлень
- Суттєвий недолік цього варіанту – децентралізація керування
  - Засоби утворення захищених тунелів повинні встановлюватись і належним чином налаштовуватись на кожному клієнтському комп'ютері, що у великих мережах є занадто трудомісткою задачею

Кінцева точка захищеного тунелю – брандмауер або граничний маршрутизатор локальної мережі

- Захищений тунель утворюється лише у публічній мережі
- Якщо відмовитись від захисту трафіка всередині локальної мережі (або локальних мереж), що входить до складу VPN, можна досягти помітного спрощення задач адміністрування
  - Захист трафіка всередині локальної мережі може забезпечуватись іншими засобами
    - наприклад, реєстрація дій користувачів і організаційні заходи

Кінцеві точки захищеного тунелю – засоби, що встановлені на теренах провайдерів Інтернету

- Переваги:
  - Виключається найскладніша задачу – адміністрування засобів утворення захищених тунелів, що встановлені на комп'ютерах (в тому числі портативних пристроях), з яких здійснюється віддалений доступ
  - Підвищена масштабованість і керованість мережі
  - Прозорість доступу
- Аргументація на користь припустимості такого зниження захищеності:
  - Саме Інтернет, як і інші мережі з комутацією пакетів, є найбільш вразливими для дій порушників
  - Канали телефонної мережі та виділені лінії, які використовуються між кінцевими вузлами віддаленого доступу і провайдерами, і які в цьому випадку є незахищеними, не настільки вразливі
- Одночасно з економією коштів на адмініструванні кінцевих вузлів зростають витрати на послуги провайдерів, крім того, провайдеру при цьому необхідно довіряти

Рівні реалізації VPN

- Реалізація VPN можлива на різних рівнях і різними протоколами:
  - GRE тунелі
  - MPLS VPN
  - VPN на базі PPP
    - PPP over SSH
    - PPP over SSL/TLS
    - PPPoE
    - PPTP
  - Інші протоколи канального рівня (L2F, L2TP)
  - IP Security (VPN мережного рівня)
  - Web VPN (SSL/TLS VPN) – VPN сеансового рівня
  - SOCKS (також сеансового рівня)

Системи шифрування на прикладному рівні

- Системи шифрування на прикладному рівні не розглядаються як VPN
- Такі системи реалізуються:
  - у деяких прикладних протоколах (SHTTP тощо)
  - деякими спеціальними прикладними програмами (наприклад, PGP)
- Зазначені засоби здатні забезпечити захист інформаційного обміну, але вони
  - не є прозорими для прикладних програм
  - як правило, вони не забезпечують усіх необхідних функцій
  - тому вони не відносяться до засобів утворення VPN

Тунелювання мережного трафіка

- Протокол інкапсуляції GRE (General Routing Incapsulation, RFC 1701, 1702, 2784, Protocol #47)
- Інкапсуляція пакета на мережному рівні з новим IP-заголовком

IP delivery hdr	GRE hdr	Original payload

Захист віртуальних каналів на канальному рівні

- Утворення захищених тунелів на канальному рівні моделі OSI забезпечує незалежність від протоколів мережного рівня і всіх вищих рівнів
  - Таким чином досягається максимальна прозорість VPN
- Недоліки:
  - Ускладнюються задачі конфігурації і підтримки віртуальних каналів
  - Ускладнюється керування криптографічними ключами
  - Зменшується набір реалізованих функцій безпеки
- В якості протоколів на цьому рівні використовуються:
  - PPTP (англ. – *Point-to-Point Tunneling Protocol*)
  - L2F (англ. – *Layer-2 Forwarding*)
  - L2TP (англ. – *Layer-2 Tunneling Protocol*)
- Усі названі протоколи не специфікують протоколи автентифікації та шифрування

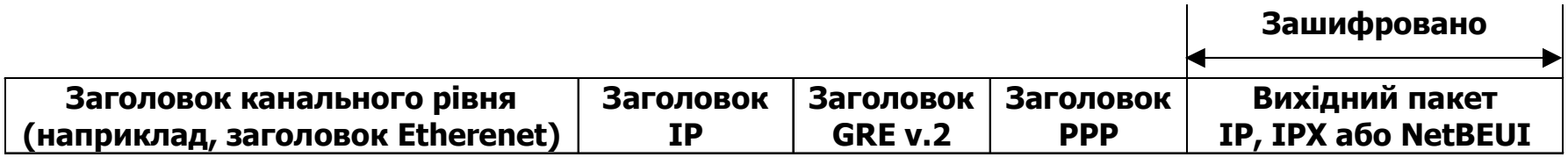
Протокол PPTP

- Протокол PPTP (англ. – Point-to-Point Tunneling Protocol) був розроблений компанією Microsoft за підтримки компаній Ascend Communications, 3Com/Primary Access, ECI-Telematics та US Robotics
- Фактично, цей протокол є розширенням протоколу PPP (англ. – Point-to-Point Protocol), яке дозволяє створювати криптозахищені тунелі на канальному рівні моделі OSI
- IETF RFC-2637, Point-to-Point Tunneling Protocol (PPTP) / K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn. – July 1999
- Протокол PPTP отримав статус проекту стандарту Internet, однак в якості стандарту так і не був затверджений.
- Головне призначення протоколу – організація доступу віддалених користувачів до локальних мереж як у випадку прямого з'єднання віддаленого комп'ютера з публічною мережею, так і у випадку підключення до публічної мережі по телефонній лінії через провайдера
  - При цьому для віддаленого користувача, який підключений до локальної мережі через сервер віддаленого доступу (RAS), імітується знаходження його комп'ютера безпосередньо в локальній мережі. Це досягається завдяки тунелюванню пакетів повідомлень.

Автентифікація в PPTP

- Для автентифікації в PPTP можуть застосовуватись різні протоколи
- В реалізації PPTP від Microsoft підтримуються протоколи:
  - PAP (англ. – Password Authentication Protocol – протокол автентифікації за паролем)
    - Передбачає передачу ідентифікаторів і паролів у відкритому вигляді
  - CHAP (англ. – Challenge-Handshaking Authentication Protocol – протокол автентифікації за процедурою рукостискання)
    - Передбачає одержання від сервера випадкового числа і шифрування на ньому пароля
    - Таким чином, не лише пароль не передається по мережі у відкритому вигляді, але й зашифровані образи пароля кожного разу різні

Структура пакетів PPTP



- Вихідні пакети (IP, IPX або NetBEUI), якими здійснюється інформаційний обмін між комп'ютером віддаленого користувача і локальною мережею, зашифровуються та інкапсулюються у пакети PPP
- Протокол PPP є стандартним протоколом віддаленого доступу, і в протоколі PPTP він застосовується:
  - для взаємодії віддаленого комп'ютера з RAS провайдера
  - для його взаємодії через тунель з RAS локальної мережі
- Пакет PPP разом з додатковою інформацією, що міститься у заголовку GRE, інкапсулюються у пакет IP

Схеми застосування протоколу PPTP

- У протоколі PPTP передбачені три схеми його застосування:
  - пряме з’єднання комп’ютера віддаленого користувача з Інтернет
  - комп’ютер віддаленого користувача з’єднується з Інтернет по телефонній лінії через провайдера, криптозахищений тунель утворюється між сервером провайдера і граничним маршрутизатором локальної мережі
  - комп’ютер віддаленого користувача з’єднується з Інтернет по телефонній лінії через провайдера, криптозахищений тунель утворюється між кінцевими точками взаємодії

Пряме з’єднання комп’ютера віддаленого користувача з Інтернет за протоколом PPTP

- Вимагає встановлення:
  - на комп’ютері віддаленого користувача
    - клієнта RAS
    - драйвера PPTP
  - на сервері віддаленого доступу локальної мережі
    - сервера RAS
    - драйвера PPTP
- В продуктах Microsoft відповідні програмні компоненти реалізовані

Криптозахищений тунель утворюється між сервером провайдера і граничним маршрутизатором локальної мережі

- Ця схема передбачає захист трафіка, що проходить через Інтернет, але не захищає обмін між комп'ютером віддаленого користувача і провайдером Інтернет
- Недоліки:
  - необхідність довіряти провайдеру
  - підвищення витрат на послуги провайдера
  - сервер віддаленого доступу провайдера повинен підтримувати протокол PPTP
    - PPTP є "рідним" для продуктів Microsoft, а провайдери, як правило, обирають в якості RAS інші засоби

Криптозахищений тунель утворюється між кінцевими точками взаємодії

- Від провайдера нічого додаткового не вимагається
- Ця схема менш зручна для кінцевого користувача, оскільки він має двічі встановлювати з'єднання:
  - спочатку за протоколом PPP з RAS провайдера (виконуючи необхідну процедуру автентифікації)
  - потім, після отримання доступу до Інтернет, за протоколом PPTP з RAS локальної мережі (подібно до першої схеми)
  - Єдиний вихід, який при цьому пропонують – використовувати написання сценаріїв, які автоматизують дії користувача
    - Але при цьому паролі вписуються у сценарій

Протокол L2F

- Розроблений компанією Cisco Systems за підтримки компаній Shiva та Northern Telecom
- IETF RFC-2341, Cisco Layer Two Forwarding (Protocol) «L2F» / A. Valencia, M. Littlewood, T. Kolar. – May 1998
- На відміну від PPTP, L2F значно зручніший для провайдерів Інтернет
- L2F підтримує різні мережні протоколи
  - крім протоколу PPP для зв'язку комп'ютера віддаленого користувача із сервером провайдера можуть застосовуватись протоколи SLIP та інші
  - публічна мережа, яка з'єднує сервери провайдера і локальної мережі, не обов'язково повинна бути IP-мережею
- В цілому, L2F дуже подібний до PPTP (аналогічна структура пакету)
- Схема застосування протоколу L2F подібна до схеми 2 застосування протоколу PPTP (Захищений тунель утворюється лише між сервером провайдера і сервером локальної мережі)
  - Це означає прозорість для кінцевих вузлів
  - Не забезпечується захист з'єднання комп'ютера віддаленого користувача із сервером провайдера
  - У цій схемі застосування протоколу PPTP передбачалось, що дані про облікові записи користувачів повинні зберігатись у провайдера, в L2F вони повинні знаходитись лише на сервері локальної мережі
- Для утворення криптозахищеного тунелю між кінцевими точками інформаційного обміну в L2F пропонується використовувати IPSec

Протокол L2TP

- Протокол L2TP розроблений організацією IETF на основі протоколів PPTP і L2F
- IETF RFC-2661, Layer Two Tunneling Protocol «L2TP» / W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter. – August 1999
- Протокол увібрав в себе кращі риси PPTP і L2F і підтримує також деякі додаткові функції
- Обмеженням протоколу, як і в L2F, є те, що не забезпечується захист з'єднання комп'ютера віддаленого користувача із сервером провайдера
  - Захищений тунель утворюється лише між сервером провайдера і сервером локальної мережі
  - Як і в L2F, пропонується використання IPSec для утворення захищених тунелів між кінцевими точками