На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут комп`ютерних систем і технологій
"Індустрія 4.0" ім. П.М. Платонова
Факультет Комп`ютерної інженерії, програмування та кіберзахисту

XIX Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції. Частина 2

Одеса
22 квітня 2019 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XIX Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22 квітня 2019 р. - Одеса, Видавництво ОНАХТ, 2019 р. - 68 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Організаційний комітет

Голова – д.т.н., проф., **Єгоров Б.В.**, ректор ОНАХТ.

Співголови:

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНАХТ,
Котлик С.В. – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНАХТ,
Даріуш Долива, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м. Лодзь, Польща,
Ковалюк Т.В. - к.т.н., доц. кафедри АСОІтаУ НТУУ «Київський політехнічний інститут».

Члени оргокомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНАХТ,
Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНАХТ,
Князєва Н.О. – д.т.н., проф. кафедри КІ ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНАХТ,
Тарасенко В.П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІТАМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Жуков І. А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

АНАЛІЗ ВРАЗЛИВОСТЕЙ ТА ЯКОСТЕЙ ІСНУЮЧИХ VPN - ТЕХНОЛОГІЙ

Горбешко Артем Вікторович
Керівник – ст. викл. каф. КІ Бобрікова І.С.
Одеська національна академія харчових технологій

Доповідь присвячена вивченню різних існуючих *VPN*-технологій (*Virtual Private Network* - віртуальна приватна мережа).

Мета доповіді - провести огляд доступних варіантів *VPN* і допомогти зрозуміти, на яких принципах засновані ці технології. У доповіді розглянуті такі технології як: *OpenVPN*, *PPTP*, *L2TP*.

Технологія віртуальних приватних мереж (VPN - Virtual Private Network) є одним з ефективних механізмів забезпечення інформаційної безпеки при передачі даних в розподілених обчислювальних мережах.

Віртуальні приватні мережі є комбінацією декількох самостійних сервісів (механізмів) безпеки:

–шифрування (з використання інфраструктури криптосистем) на виділених шлюзах (шлюз забезпечує обмін даними між обчислювальними мережами, що функціонують по різних протоколах);

–екранування (з використанням міжмережевих екранів);

–тунелювання.

Для передачі даних VPN-агенти створюють віртуальні канали між захищеними локальними мережами або комп'ютерами (такий канал називається "тунелем", а технологія його створення називається "тунелюванням"). Вся інформація передається по тунелю в зашифрованому вигляді.

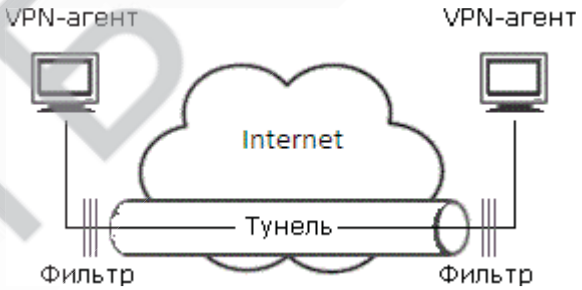

Рис.1 - Організація тунелю в VPN

Однією з обов'язкових функцій VPN-агентів є фільтрація пакетів. Фільтрація пакетів реалізується відповідно до VPN-агента, сукупність яких утворює політику безпеки віртуальної приватної мережі. Для підвищення захищеності віртуальних приватних мереж на кінцях тунелів доцільно розташовувати міжмережні екрани.

Головною вразливістю технології *VPN* - може бути довжина ключа шифрування використовуваного при створенні шифру, ця вразливість впливає на час, витрачений для злому простим перебором. *PPTP* використовується VPN-шифрування з довжиною ключа максимум 128 біт, коли *L2TP IPSec* протоколу з ключами довжиною до 256 біт. І OpenVPN він використовує

OpenSSL бібліотеку для забезпечення шифрування. OpenSSL підтримує велику кількість різних криптографічних алгоритмів, таких як 3*DES*, *AES*, *RC*5, *Blowfish*. Як у випадку *IPSec*, *CheapVPN* включає екстремально високий рівень шифрування - *AES* алгоритм з ключем довжиною 256 біт.

Що ми отримуємо на практиці: взлом 256-бітного ключа потребують в 2128 більше обчислювальної потужності, ніж злом 128-бітного ключа. Це означає, що буде потрібно 3.4x10 ^ 38 операцій (кількість комбінацій в 128-бітному ключі). Якби ми застосували суперкомп'ютер зі швидкість обчислень 10.51 пентафлопс, нам знадобилося б близько 1 мільярда років, щоб зламати 128-бітний *AES*-ключ шляхом перебору. Так що на практиці 128-бітний шифр не може бути зламаний шляхом перебору, було б правильно говорити, що ключа такої довжини більш ніж достатньо для більшості застосувань.

Хоча PPTP зазвичай і використовується з 128-бітовим шифруванням, в наступні кілька років після включення цього протоколу до складу Windows 95 OSR2 в 1999 році були знайдені ряд вразливостей. Найбільш серйозною з яких з'явилася уразливість протоколу аутентифікації *MS-CHAP* v.2. Використовуючи цю уразливість, *PPTP* був зламаний протягом двох днів. І хоча компанією Microsoft помилка була виправлена (за рахунок використання протоколу аутентифікації *PEAP*, а не *MS-CHAP* v.2), вона сама рекомендувала до використання в якості *VPN* проколів *L2TP* або *SSTP*.

OpenVPN і *IPSec* не має відомих вразливостей і це означає вкрай високий ступінь безпеки при використанні з алгоритмом шифрування, таким як *AES*.

L2TP / *IPsec* вбудований у всі сучасні операційні системи і VPN-сумісні пристрої, і так само легко може бути налаштований як і *PPTP* (зазвичай використовується той же клієнт). Проблеми можуть виникнути в тому, що *L2TP* використовує *UDP*-порт 500, який може бути заблокований файрволом, якщо ви перебуваєте за *NAT*.

OpenVPN є досить новою технологією з відкритим кодом. Одним з його головних переваг є те, що OpenVPN дуже гнучкий у налаштуваннях .Цей протокол може бути налаштований на роботу на будь-якому порту, в тому числі на 443 *TCP*-порту, що дозволяє маскувати трафік усередині *OpenVPN* під звичайний *HTTPS*. Те, як швидко працює *OpenVPN*, залежить від обраного алгоритму шифрування, але, як правило, працює швидше, ніж *IPsec*. *OpenVPN* спочатку не підтримується операційними системами, для його використання необхідно не тільки завантажити і встановити клієнт, але і завантажити та встановити додаткові конфігураційні файли.

Список літератури:

1. Основные стандарты сетей передачи данных [Електронний ресурс]. – Режим доступу: http://www.gpntb.ru.

2. Технология виртуальных частных сетей (VPN) [Електронний ресурс]. – Режим доступу: https://helpiks.org/9-25862.html

3. Криптографические методы защиты информации [Електронний ресурс]. – Режим доступу: https://moodle.kstu.ru/mod/page/view.php?id=10125

РОЗРОБКА МОБІЛЬНОГО ДОДАТКУ ДЛЯ РОЗПІЗНАВАННЯ ЗЛОЯКІСНОГО ЗАХВОРЮВАННЯ ШКІРИ

Гусак В.Д., студент IV курсу спеціальність 5.05010101 «Обслуговування програмних систем і комплексів»
Керівник: Клименко О.Г. , викладач спеціальних комп'ютерних дисциплін
Коледж промислової автоматики та інформаційних технологій ОНАХТ

За останнє десятиліття смартфони відчутно змінили чимало аспектів нашого щоденного життя – від банківських операцій до шопінгу та розваг.Тепер на черзі стоїть медицина. Смартфони з медичними додатками несуть революційний потенціал для медицини. Унаслідок цієї революції вперше в історії її центральною фігурою замість лікаря може стати пацієнт.

Кожен рік тільки в США діагностують 5,6 млн людей з раком шкіри. Зазвичай це стається на ретельному у огляді у дерматолога, який пацієнти проходять не так вже й часто. При цьому що раніше хворобу вдається виявити, то краще: знайдену на ранніх стадіях меланому виліковують у 97% випадків, тоді як на пізніх етапах виживають лише 14% хворих. Рак шкіри відноситься до найбільш поширених різновидів раку. Частка меланоми – 1% в структурі злоякісних пухлин шкіри. Однак, статистика смертності від цього захворювання є найвищою.

Захворюваність на меланому шкіри в Україні зростає, втім, як і в усьому світі. Проте, нині спостерігається дуже позитивна тенденція у лікуванні, тому що пацієнти почали звертатися з ранніми і нульовими стадіями меланоми шкіри. Все більше людей звертають увагу на найменші зміни з родимками, і йдуть до лікарів.

Для розпізнавання захворювання на ранніх стадіях активно використовують інформаційні технології. Так у Стенфордському університеті був створений штучний інтелект, який зміг діагностувати рак шкіри настільки ж точно, як і 21 професійний дерматолог з великим досвідом. Уже на етапі розробки дослідники говорили про те, що створення мобільного додатку дозволить швидко діагностувати рак шкіри.

У 2015 році розроблено новий додаток SkinVision, який здатний визначити за фото ступінь ризику розвитку раку шкіри, повідомляє *The Daily Mail*. Повідомляється про те, що розробка виявляє злоякісне утворення на шкірі з точністю до 83%.

Додаток аналізує фотографії родимок людини і може виявити навіть ранню стадію меланоми - злоякісної пухлини. Під час оцінки використовується алгоритм аналізу ураження на основі фрактальної геометрії.