МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ІНСТИТУТ МЕХАНІКИ ТА АВТОМАТИКИ АПВ НААН
ДЕРЖАВНИЙ БІОТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ

X Міжнародної науково-технічної конференції з нагоди 116-ї річниці від дня народження
доктора технічних наук, професора,
члена-кореспондента ВАСГНІЛ,
віцепрезидента УАСГН
КРАМАРОВА
Володимира Савовича
(1906-1987)

«КРАМАРОВСЬКІ ЧИТАННЯ»

23-24 лютого 2023 року
м. Київ

4. Кушлик-Дивульська О. І., Поліщук Н. В., Орел Б. П., Штабалюк П. І. (2014) Теорія ймовірностей та математична статистика: навч. Посіб. К: НТУУ «КПІ» 212 с.

5. Гринченко А.С., Алферов А.И. (2017) Прогнозирование надежности элементов машин при случайном пуассоновском потоке экстремальных нагружений. Науковий журнал «Технічний сервіс агропромислового, лісового та транспортного комплексів». 7, 141-148

УДК 004.771

СИСТЕМА ЗАХИСТУ ПЕРЕДАЧІ ДАНИХ ЗА ДОПОМОГОЮ VPN-З'ЄДНАННЯ

П. О. МАЛЬЧЕНКО, магістрант
Чорноморський Національний Університет імені Петра Могили,
м. Миколаїв, Україна
Г. О. ІВАНОВ, канд. техн. наук, доцент,
Миколаївський національний аграрний університет
М. Миколаїв, Україна
E-mail: twink1337zhab@gmail.com**,** ivanovgo0708@gmail.com

В даний час все більшої популярності набувають вбудовані системи, наприклад – одноплатні комп'ютери. Більшість із них не дорогі, і вони корисні в широкому діапазоні проектів DIY, від досить простих до досить складних.

Хорошим прикладом такого проекту може бути власний VPN-сервер на основі SoC. VPN або віртуальна приватна мережа дозволяє зберігати захищений тунель між віддаленими пристроями, щоб мати доступ один до одного, як локальна мережа.

Вбудовані платформи, очевидно, менш потужні, ніж стаціонарні комп'ютери, їх використання більш ніж раціонально для цілей, для яких вони використовуються в промисловості. Деякі з цих пристроїв також є чудовими інструментами для експериментів і навчання завдяки своїй низькій вартості та простоті. Завдяки простоті, низькій вартості, енергоспоживанню та сумісності з іншими апаратними та програмними вбудованими пристроями також чудово підходить для експериментальних чи навчальних цілей [1].

Механізми захисту VPN використовують шифрування та аутентифікацію. Шифрування гарантує, що внутрішній трафік не може бути скомпрометований і залишається приватним. Аутентифікація підтверджує ідентичність джерела даних і складається з двох частин [2]:

1. Аутентифікація користувача та системи, що забезпечує доступ до авторизованого сервера. Облікові дані користувача представлені у вигляді цифрового сертифіката, пари ключів або комбінації пароля для входу. Правила

для конкретних користувачів можна запропонувати в налаштуваннях вашої VPN, таким чином можна обмежити доступ до вашої мережі для обмеженої кількості довірених користувачів, указаних у конфігураційних файлах.

2. Внутрішній захист трафіку — кожен відправлений пакет зашифрований і аутентифікований. Зазвичай у реалізації VPN використовуються форми шифрування «аутентифіковане шифрування» (AE) або «аутентифіковане шифрування з пов‘язаними даними» (AEAD), які одночасно забезпечують конфіденційність і автентичність даних. Шифрування за допомогою алгоритмів AE або AEAD генерує «код аутентифікації повідомлення» (MAC) і додає його до згенерованого зашифрованого тексту. Будь-які зміни в зашифрованому тексті призводять до пошкодження MAC. Таким чином він запобігає можливій модифікації трафіку, атакам «Людина посередині» (MITM) і «Відмова в обслуговуванні» (DDoS).

Отже, безпека механізмів віртуальної приватної мережі вимагає сучасної криптографії, механізмів аутентифікації та шифрування, проектування мережі та конфігурації системи. Правильно налаштована конфігурація обмеження доступу до вашої VPN, механізмів цілісності та конфіденційності дозволяє запобігти можливому витоку даних і досягти безпечного з‘єднання навіть у ненадійних мережах.

Зараз доступно багато рішень VPN, як комерційних, так і проектів з відкритим кодом. Всіх їх можна розділити на три категорії:

1. VPN на основі протоколу IPSec
2. VPN на основі SSL/TLS
3. Самостійні (незалежні) рішення

Деякі незалежні рішення можуть використовувати частини протоколів SSL/TLS або IPSec, наприклад «OpenVPN» використовує протокол, подібний до SSL, для встановлення безпечного з‘єднання, однак він значно відрізняється від інших рішень на основі SSL/TLS.

WireGuard — це безкоштовна реалізація VPN з відкритим вихідним кодом, створена як альтернатива стандартним IPsec і OpenVPN. У січні 2020 року, після півтора років доопрацювання коду, WireGuard став частиною ядра Linux. Автором WireGuard є розробник і пентестер Джейсон Доненфілд. Йому вдалося створити набагато простішу та лаконічнішу реалізацію протоколу VPN, ніж більшість інших. Перша версія WireGuard містила менше 5000 рядків коду - порівняно з десятками тисяч рядків в інших програмах VPN. Це не робить WireGuard безпечнішим, але значно полегшує підтримку проекту. Клієнти WireGuard вже випущені для Android, iOS, MacOS, Linux і Windows. Cloudflare запустив VPN-сервіс Warp на основі WireGuard, і кілька комерційних провайдерів VPN також дозволяють користувачам використовувати WireGuard, включаючи TorGuard, IVPN і Mullvad. Використання WireGuard безпосередньо в ядрі, яке безпосередньо взаємодіє з обладнанням, має ще більше прискорити програму, а також зробити її більш привабливою з точки зору використання у вбудованих системах. WireGuard може шифрувати та дешифрувати дані

безпосередньо з мережевої карти, без необхідності передавати трафік через ядро та програмне забезпечення високого рівня.

Висновки. Вбудована платформа є відповідним рішенням для розгортання VPN. WireGuard — це безкоштовна та легка реалізація технології віртуальних приватних мереж. Він перенаправляє трафік через захищений тунель і дозволяє об'єднати віддалені пристрої в одну мережу.

У результаті проведення дослідження було створено рішення, розміщене на власному хості, яке дешевше, ніж розміщення на повнорозмірному сервері чи хмарній службі, і, звісно, користується набагато більшою довірою, ніж будь-яка безкоштовна служба VPN.

Список використаних джерел

1. Z. Bundalo, and D. Bundalo, "Embedded Systems Based on Open Source Platforms", in Introduction to Data Science and Machine Learning. London, United Kingdom: *IntechOpen*, 2019, https://www.intechopen.com/chapters/67745 doi: 10.5772/intechopen.85806.

2. A. T. Woland, V. Santuka, J. Sanbower, and C. Mitchell, Integrated Security Technologies and Solutions. Hoboken, *NJ: Cisco Press*, 2019.

УДК 004.85

АНАЛІЗ МОДЕЛЕЙ КЛАСИФІКАЦІЇ КЛІЄНТІВ БАНКУ ПРИ ОТРИМАННІ КРЕДИТУ

П. О. МАЛЬЧЕНКО, магістрант
Чорноморський Національний Університет імені Петра Могили,
м. Миколаїв, Україна
Г. О. ІВАНОВ, канд. техн. наук, доцент,
Миколаївський національний аграрний університет
М. Миколаїв, Україна
E-mail: twink1337zhab@gmail.com**,** ivanovgo0708@gmail.com

Високий рівень банкрутства є небажаним для банку, оскільки це означає, що банк навряд чи зможе окупити інвестиції. Якщо завдання прогнозування класу, категорії, майбутнього клієнту буде вирішено, то класифікаційна модель зможе визначати претендентів, які мають високий ризик банкрутства. Це дозволить банку відхиляти запити на кредит, замість того, щоб видавати гроші. Це робить дослідження щодо підбору оптимальної класифікаційної моделі для прогнозування актуальними.

Інтелектуальний аналіз даних у галузі кредитування збирає дані з минулого досвіду та аналізує їх для виявлення тенденцій та рішень для поточних ситуацій. Це ефективна аналітична методологія виявлення невідомої