УДК 004.056.55

Кудревич В.І.

Салієва О.В.

УДОСКОНАЛЕННЯ ПРОТОКОЛУ TLS НА ОСНОВІ НЕЙРОННОЇ МЕРЕЖІ

Вінницький національний технічний університет

Анотація

У даній роботі розглянуто питання покращення захисту криптографічного протоколу TLS з використанням нейронної мережі. Проведено аналіз сучасних методів захисту інформаційних ресурсів, охарактеризовано особливості TLS-протоколу та визначено ключові проблеми, пов'язані з виявленням підозрілих сертифікатів під час передавання пакетів даних між користувачами. Розроблено алгоритми динамічної перевірки пакетів й сертифікатів та адаптивної системи блокування передачі даних, що забезпечують виявлення та протидію несанкціонованим спробам доступу.

Ключові слова: кібербезпека, протокол, нейронна мережа, TLS-протокол.

Abstract

This paper examines the enhancement of the security of the TLS cryptographic protocol through the use of a neural network.. An analysis of modern methods for protecting information resources is carried out, the features of the TLS protocol are characterized, and key problems associated with detecting suspicious certificates during the transmission of data packets between users are identified. Algorithms for dynamic packet and certificate verification and an adaptive data transmission blocking system are developed, which ensure the detection and counteraction to unauthorized access attempts.

Keywords: cybersecurity, protocol, neural network, TLS-protocol.

Вступ

У сучасному цифровому середовищі, де переважна більшість комунікацій, транзакцій та обміну даними здійснюється через мережу Інтернет, особливого значення набуває питання безпеки передавання інформації. Протокол Transport Layer Security є основним стандартом захищеної комунікації, який забезпечує шифрування, автентифікацію сторін та цілісність даних. Однак, попри свою зрілість, TLS залишається вразливим до низки сучасних кіберзагроз — від підробки цифрових сертифікатів і компрометації центрів сертифікації до атак типу man-in-the-middle та отруєння кешу OCSC. Традиційні методи перевірки сертифікатів, такі як CRL чи OCSP, є статичними та не забезпечують гнучкої адаптації до нових типів ризиків [1].

Це створює потребу у впровадженні динамічних підходів до перевірки сертифікатів і TLS-сесій, здатних реагувати на аномалії у режимі реального часу. Одним із перспективних напрямів є поєднання криптографічних механізмів із методами машинного навчання, що дозволяє формувати моделі поведінки безпечних і потенційно шкідливих з'єднань. Актуальність дослідження зумовлена необхідністю створення інтелектуальної системи контролю TLS, яка поєднує криптографічну надійність із гнучкістю адаптивного аналізу, забезпечуючи підвищений рівень захисту інформаційних обмінів у мережевих застосунках.

Результати дослідження

Традиційні підходи до забезпечення безпеки TLS базуються на статичних правилах перевірки сертифікатів – перевірці підпису, ланцюга довіри, строку дії та статусу відкликання через CRL або OCSC. Проте ці механізми мають низку обмежень. Вони не дозволяють оперативно реагувати на нові види загроз, не враховують поведінкові характеристики клієнта або сервера, а також не забезпечують автоматичної

адаптації до змін у мережевому середовищі. Ще однією проблемою є відсутність уніфікованого журналу подій TLS, який би дозволяв здійснювати аудит і аналітику з урахуванням історії ризиків. Це знижує прозорість моніторингу, ускладнює навчання моделей і підвищує ймовірність повторних інцидентів без виявлення першопричин. Тому актуальним є створення інтегрованих рішень, що поєднують запам'ятовування сесій, аналіз ризиків, систему сповіщень та механізми донавчання нейронної мережі на основі розмічених прикладів. Нейронні мережі, особливо багаторівневі та рекурентні, показують високу ефективність у задачах класифікації мережевого трафіку та виявлення аномалій у TLS-сесіях [2].

При аналізі журналів TLS-з'єднань нейронна мережа може навчитися розпізнавати легітимний трафік від аномального і порівнювати нові сесії з відомими шаблонами. У разі виявлення відхилення від типових параметрів система може автоматично змінити політику. Тому для підвищення рівня безпеки варто удосконалити протокол TLS шляхом інтеграції нейронної мережі, врахувавши такі особливості його роботи:

1. Рішення системи може змінюватися динамічно, залежно від оновлення оцінки ризику або появи додаткових даних.

2. Всі події системи: створення сесії, зміна статусу, блокування, оцінка ризику, ручні дії користувача фіксуються у таблиці audit_log.

3. Записи мають тип події, опис, рівень ризику та часову мітку. Це забезпечує повну прозорість функціонування системи та можливість відтворення будь-якої події у майбутньому [3].

Взаємодію модулів організуємо за моделлю, у якій дані передаються послідовно між рівнями системи, а результати аналізу повертаються для корекції політик або повторного навчання моделі:

- при ініціації нового TLS-з'єднання middleware фіксує метадані сесії;
- сертифікат перевіряється базовими методами;
- дані передаються на ML-сервіс для оцінювання ризику;
- на основі результату модель формує рекомендацію;
- Middleware застосовує відповідну політику та створює запис у журналі подій;
- підозрілі випадки автоматично заносяться до таблиці alerts, а їхні параметри використовуються під час наступного навчання моделі.

Таким чином формується замкнений цикл моніторингу, який поєднує збір, аналіз, реагування та донавчання [4].

Запропонована архітектура відрізняється від традиційних засобів безпеки TLS тим, що:

- не вимагає модифікації стандартного протоколу або SSL-бібліотек;
- дозволяє аналізувати поведінку сесій у динаміці;
- реалізує концепцію Policy-Driven Security, де рішення приймаються автоматично на основі ризику;
- підтримує адаптивне навчання моделі на основі накопичених даних;
- надає зручний веб-інтерфейс для перегляду, редагування та аналітики.

Таким чином, запропонований middleware виступає інтелектуальним надбудовним шаром над TLS, який перетворює протокол із пасивного механізму шифрування на активну систему контролю безпеки з можливістю самонавчання. Розроблена система являє собою інтелектуальний проміжний рівень між користувачем і стандартним протоколом TLS. Її головна ідея – аналізувати та контролювати поведінку TLS-сесій у реальному часі, не змінюючи сам протокол [5]. Коли користувач або застосунок встановлює TLS-з'єднання, middleware фіксує метадані і передає їх у базу даних MySQL.

Висновок

Удосконалений підхід до моніторингу та захисту TLS-сесій демонструє, що поєднання класичних механізмів перевірки сертифікатів із машинним навчанням значно підвищує адаптивність і точність системи безпеки. Інтеграція запису сесій в журнал, аналізу ризиків і динамічного коригування політик забезпечує безперервний цикл контролю, у якому кожне відхилення від нормальної поведінки використовується для оновлення моделі та зменшення ймовірності повторення інцидентів. Такий підхід

робить систему здатною реагувати на нові загрози у реальному часі та зберігати повну історію рішень, що створює прозоре й відтворюване середовище аудиту.

Запропонований middleware демонструє, що без потреби модифікації TLS можна створити інтелектуальний надбудовний шар, який перетворює стандартний протокол на активну систему управління ризиками. Адаптивне навчання моделі, використання централізованого журналу подій та можливість коригування політик у відповідь на результати аналізу формують гнучку архітектуру, придатну для сучасних сценаріїв кіберзахисту. У підсумку система забезпечує більш глибоке розуміння поведінки трафіку, підвищує стійкість до аномальних впливів і створює підґрунтя для подальшого розвитку методів інтелектуального захисту мережевих комунікацій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016. 775 с.
2. Russell S., Norvig C. Artificial Intelligence: A Modern Approach. 4th ed. Pearson, 2021. 1152 с.
3. Chollet F. Deep Learning with Python. 2nd ed. Manning Publications, 2021. 504 с.
4. Murphy K. Machine Learning: A Probabilistic Perspective. 2nd ed. MIT Press, 2022. 1280 с.
5. Alpaydin E. Introduction to Machine Learning. 4th ed. MIT Press, 2020. 640 с.

Кудревич Вадим Ігорович – студент групи 2КІТС-24М, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: 777kudron777@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Kudrevich Vadym I. – student of 2KITS-24m group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: 777kudron777@gmail.com

Supervisor*:* ***Saliieva Olha V.*** – Doctor of Philosophy (PhD) in specialty 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, email: salieva8257@ vntu.edu.ua