Научная статья
Original article
УДК 004.056

ОЦЕНКА СКРЫТЫХ КАНАЛОВ ПО ПАМЯТИ В ПРОТОКОЛЕ QUIC И МЕТОДЫ ИХ ОБНАРУЖЕНИЯ

EVALUATION OF HIDDEN CHANNELS FROM MEMORY IN THE QUIK PROTOCOL AND METHODS OF THEIR DETECTION

Симачев Антон Юрьевич, студент Бакалавриата, НИЯУ МИФИ

Simachev Anton Yuryevich, undergraduate student, National Research Nuclear University MEPhI, simachev.anton@mail.ru

Аннотация. В последнее время из-за роста сфер применения и распространения информационных технологий стало более явным увеличение количества конфиденциальных материалов в информационных системах. Как следствие, обострилась проблема обеспечения безопасности информации. Одним из способов скрытого получения информации является передача информации по скрытым каналам. Цель работы – повышение защищенности информационных систем путем обнаружения утечки информации по скрытым каналам в протоколе QUIC. В процессе работы было проведено исследование скрытых каналов протокола UDP, описаны их ключевые особенности. Был исследован протокол QUIC, рассмотрены ключевые особенности данного протокола. Были описаны свойственные протоколу QUIC скрытые каналы. Были проанализированы методы обнаружения скрытых каналов при помощи машинного обучения в протоколе QUIC, а также выявлены признаки скрытых каналов. В результате была оценена пропускная способность рассмотренных в ходе работы скрытых каналов.

Определено направление дальнейших исследований, включающее разработку и тестирование реализованных скрытых каналов в моделях машинного обучения для выявления наиболее точного метода, применимого на практике, и реализацию программного комплекса для обнаружения скрытых каналов при помощи нейронных сетей.

Abstract. Recently, due to the growth of the fields of application and dissemination of information technologies, the increase in the number of confidential materials in information systems has become more pronounced. As a result, the problem of information security has become more acute. One of the ways to obtain information covertly is to transmit information through hidden channels. The purpose of the work is to increase the security of information systems by detecting information leakage through hidden channels in the QUIC protocol. In the process of work, a study of hidden channels of the UDP protocol was conducted, their key features were described. The QUIC protocol was investigated, the key features of this protocol were considered. Hidden channels peculiar to the QUIC protocol were described. Methods of detecting hidden channels using machine learning in the QUIC protocol were analyzed, and signs of hidden channels were also identified. As a result, the throughput of the hidden channels considered in the course of work was evaluated. The direction of further research is determined, including the development and testing of implemented hidden channels in machine learning models to identify the most accurate method applicable in practice, and the implementation of a software package for detecting hidden channels using neural networks.

Ключевые слова: скрытый канал, протокол QUIC, кадры, заголовки, скрытый канал по памяти, машинное обучение

Keywords: hidden channel, QUIC protocol, frames, headers, hidden channel in memory, machine learning

1. Введение

Под скрытым каналом (СК) передачи информации понимают любой канал связи, не предназначенный напрямую для передачи информации [1-4]. Существуют следующие типы СК:

- СК по памяти, в которых информация передаётся через доступ отправителя на запись и получателя на чтение к одним и тем же ресурсам или объектам;
- СК по времени, которые характеризуются доступом отправителя и получателя к одному и тому же процессу или изменяемому во времени атрибуту.

По приказу 76 ФСТЭК для сертификации средств защиты информации, соответствующих четвертому уровню доверия, должны быть проведены идентификация и анализ СК по памяти, основанных на использовании ресурсов памяти, в которые записывается защищаемая информация [5].

Незадекларированные возможности технологий позволяют злоумышленникам передавать данные по СК, не беспокоясь о том, что они будут обнаружены системами безопасности.

Используемый на транспортном уровне новый протокол QUIC [6, 7] отличается уменьшенным временем задержки, чем используемый повсеместно TCP. Работающий поверх UDP, QUIC был создан инженерами Google, как замена TCP. Уход от традиционных этапов взаимодействия при создании соединения позволяет увеличить скорость соединения и уменьшить трафик, что является особенно актуальным в беспроводных сетях. В настоящее время QUIC уже применяется компаниями Google и Cloudflare [8, 9].

2. Методы

Метод обнаружения скрытых каналов с использованием машинного обучения представляет особенный интерес. Использование машинного обучения позволяет находить решение широкого спектра задач, не прибегая к использованию непосредственно алгоритмических решений. Прогнозы и поиск решения в данном случае производятся путем построения математической модели на основе тренировочных данных [10].

Обученная на основе предыдущих событий нейронная сеть может определить следующие события. Тренировка машинного обучения проводится на основе большого количества данных, содержащих в себе легитимный и нелегитимный трафик.

Применение машинного обучения для определения СК в трафике протокола QUIC позволит отличить на первый взгляд легитимный трафик, являющийся СК, от действительно легитимного. Для применения машинного обучения в обнаружении СК необходимо выявить ряд отслеживаемых признаков (таблица 1).

Таблица 1. Таблица с признаками СК в трафике QUIC

Тип СК	**Признаки СК**
С использованием бита Fixed Bit	Наличие нуля в поле Fixed Bit
С использованием кадра PADDING	Наличие кадра идущих подряд последовательностей кадров PING и PADDING
С использованием кадра PING	Количество кадров PING в пакетах инициализации

При обучении модели необходимо собрать тренировочные данные с признаками скрытых каналов со скрытым каналом и без него. Для данной задачи подойдет использование наивного Байесовского классификатора [11].

3. Результаты

Скрытые каналы Fixed Bit, PADDING и PING не использовались ранее в UDP. Их отличием от известных скрытых каналов является использование особенностей строения пакетов QUIC и использование кадра PING.

Сравнительный анализ рассмотренных скрытых каналов приведен в Таблице 2.

Таблица 2. Сравнительная таблица СК в протоколе QUIC

Тип СК	**Пропускная способность**	**Вероятность обнаружения**
С использованием бита Fixed Bit	1 бит на пакет	Высокая
С использованием кадра PADDING	Зависит от длины кадра PADDING и может достигать 1 байт на один кадр	Низкая
С использованием кадра PING	1 бит на соединение	Средняя

Во внимание принималось, что злоупотребление количеством кадров PADDING и PING, а также количеством созданных новых соединений может

влиять на обнаружение скрытого канала. В Таблице 2. приведена оценка вероятности обнаружения скрытого канала.

Большинство из этих каналов используют параметры, схожие с теми, что используются в легитимном трафике, из-за чего их обнаружение становится более трудным.

Трафик со скрытым каналом с использованием бита Fixed Bit можно проверить, включив проверку на наличие нулей в данном бите. Легитимный трафик не должен содержать в данном поле иных значений, кроме единицы. Наличие нуля в данном бите может свидетельствовать о наличии скрытого канала.

Трафик со скрытым каналом с использованием кадра PING может быть ликвидирован включением ограничения на количество соединений.

Скрытый канал с использованием PADDING представляют особую угрозу, так как является частью легитимного трафика и не может быть заблокирован. В данном случае необходимо применять другие методы обнаружения скрытых каналов.

4. Заключение

В данной работе были изучены скрытые каналы в протоколе транспортного уровня QUIC и проведена оценка их пропускной способности.

Был представлен способ реализации СК в QUIC на основе кадров PADDING, а также представлена реализация СК и использованием Fixed Bit. Дан сравнительный анализ пропускной способности каналов, сделан вывод об их опасности. Для обучения был использован наивный байевский классификатор для прогнозирования существования активного СК в системе.

Определено направление дальнейшей работы, включающее разработку и тестирование реализованных скрытых каналов в моделях машинного обучения для выявления наиболее точного метода, который может быть применен на практике, поиск СК по времени в протоколе QUIC и реализация программного комплекса для их обнаружения при помощи машинного обучения.

Литература

1. Шипулин П. М., Козин В. В., Шниперов А. Н. Метод организации скрытого канала передачи информации на основе протокола потоковой передачи данных //Научно-технический вестник информационных технологий, механики и оптики. – 2018. – Т. 18. – №. 5. – С. 834-842.
2. Тимонина Е. Е. Скрытые каналы (обзор) //Jet info. – 2002. – Т. 14. – №. 114. – С. 3-11.
3. Schoeneich R. O. et al. The channel for hidden data transmission in WSN //International Journal of Electronics and Telecommunications. – 2017. – Т. 63. – №. 2. – С. 209-216.
4. Natig H. G. Transmission channels of hidden information in cloud computing //The Eleventh International Conference on Eurasian scientific development. – 2016. – С. 96.
5. Приказ ФСТЭК России №76 от 02.06.2020 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к СТЗИ и СОБИТ» URL: https://zlonov.com/laws/%D0%BF%D1%80%D0%B8%D0%BA%D0%B0%D0%B7-%D1%84%D1%81%D1%82%D1%8D%D0%BA-76-%D0%BE%D1%82-02-06-2020/ (дата обращения: 25.04. 2022). – 2020.
6. McMillan K. L., Zuck L. D. Formal specification and testing of QUIC //Proceedings of the ACM Special Interest Group on Data Communication. – 2019. – С. 227-240.
7. Soni M., Rajput B. S. Security and performance evaluations of QUIC protocol //Data Science and Intelligent Applications. – Springer, Singapore, 2021. – С. 457-462.
8. Van T. et al. Empirical study for dynamic adaptive video streaming service based on Google transport QUIC protocol //2018 IEEE 43rd Conference on Local Computer Networks (LCN). – IEEE, 2018. – С. 343-350.
9. Marx R., Lamotte W., Quax P. Visualizing QUIC and HTTP/3 with qlog and qvis //Proceedings of the SIGCOMM'20 Poster and Demo Sessions. – 2020. – С. 42-43.

10. Jordan M. I., Mitchell T. M. Machine learning: Trends, perspectives, and prospects //Science. – 2015. – Т. 349. – №. 6245. – С. 255-260.
11. Сизов А. А., Николенко С. И. Наивный байесовский классификатор //DOCPLAYER. URL: https://docplayer. ru/45424867-Naivnyy-bayesovskiy-klassifikator.html (дата обращения: 25.04. 2022). – 2018.

References

1. Shipulin P. M., Kozin V. V., Shniperov A. N. Method of organizing a hidden information transmission channel based on the data streaming protocol //Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics. - 2018. – Vol. 18. – No. 5. – pp. 834-842.
2. Timonina E. E. Hidden channels (review) //Jet info. – 2002. – Vol. 14. – No. 114. – pp. 3-11.
3. Schoeneich R. O. et al. The channel for hidden data transmission in WSN //International Journal of Electronics and Telecommunications. – 2017. – Т. 63. – №. 2. – С. 209-216.
4. Natig H. G. Transmission channels of hidden information in cloud computing //The Eleventh International Conference on Eurasian scientific development. – 2016. – С. 96.
5. Order of the FSTEC of Russia No. 76 dated 06/02/2020 "On approval of Information security Requirements establishing the levels of trust in STSI and SBIT" URL: https://zlonov.com/laws/%D0%BF%D1%80%D0%B8%D0%BA%D0%B0%D0%B7-%D1%84%D1%81%D1%82%D1%8D%D0%BA-76-%D0%BE%D1%82-02-06-2020 / (accessed: 25.04. 2022). – 2020.
6. McMillan K. L., Zuck L. D. Formal specification and testing of QUIC //Proceedings of the ACM Special Interest Group on Data Communication. – 2019. – С. 227-240.
7. Soni M., Rajput B. S. Security and performance evaluations of QUIC protocol //Data Science and Intelligent Applications. – Springer, Singapore, 2021. – С. 457-462.

8. Van T. et al. Empirical study for dynamic adaptive video streaming service based on Google transport QUIC protocol //2018 IEEE 43rd Conference on Local Computer Networks (LCN). – IEEE, 2018. – С. 343-350.
9. Marx R., Lamotte W., Quax P. Visualizing QUIC and HTTP/3 with qlog and qvis //Proceedings of the SIGCOMM'20 Poster and Demo Sessions. – 2020. – С. 42-43.
10. Jordan M. I., Mitchell T. M. Machine learning: Trends, perspectives, and prospects //Science. – 2015. – Т. 349. – №. 6245. – С. 255-260.
11. Sizov A. A., Nikolenko S. I. Naive Bayesian classifier //DOC PLAYER. URL: https://docplayer . ru/45424867-Naivny-bayesovskiy-klassifikator.html (accessed: 25.04. 2022). – 2018.

© Симачев А. Ю. 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №5/2022.

Для цитирования: Симачев А. Ю. ОЦЕНКА СКРЫТЫХ КАНАЛОВ ПО ПАМЯТИ В ПРОТОКОЛЕ QUIC И МЕТОДЫ ИХ ОБНАРУЖЕНИЯ // Научно-образовательный журнал для студентов и преподавателей «StudNet» №5/2022