Научная статья
Original article
УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ ОБНАРУЖЕНИЯ СКРЫТЫХ КАНАЛОВ В ПРОТОКОЛЕ HTTP/3

COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF HIDDEN CHANNEL DETECTION ALGORITHMS IN HTTP/3 PROTOKOL

Симачев Антон Юрьевич, студент Бакалавриата, НИЯУ МИФИ

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

Аннотация. Защита от информационных угроз является важной темой в области безопасности ядерных и промышленных информационных технологий с последнего десятилетия. Использование скрытого канала связи создает новую форму сценариев атак, для которых существующие защитные механизмы обычно неэффективны. Чтобы защитить промышленные системы управления от этих атак, необходимо понимать и понимать эти атаки. В работе рассмотрены особенности протокола передачи информации HTTP/3 в сравнении с предыдущими версиями. Проанализированы признаки скрытых каналов. В результате тестирования получена таблица эффективности алгоритмов обнаружения скрытых каналов в протоколе HTTP/3.

Abstract. Protection against information threats has been an important topic in the field of nuclear and industrial information technology security since the last decade. The use of a hidden communication channel creates a new form of attack scenarios for which existing defense mechanisms are usually ineffective. To protect industrial control

systems from these attacks, it is necessary to understand and understand these attacks. The paper considers the features of the HTTP/3 information transfer protocol in comparison with previous versions. The signs of hidden channels are analyzed. As a result of testing, a table of the effectiveness of algorithms for detecting hidden channels in the HTTP/3 protocol was obtained.

Ключевые слова: скрытый канал, кадры, заголовки, признаки, протокол HTTP/3, классификатор

Keywords: hidden channel, frames, headers, features, HTTP/3 protokol, classifier

1. Введение

Недавние результаты исследований вредоносных угроз указывают на растущее использование методов сокрытия информации в качестве нового подхода к компрометации ИТ-систем с использованием скрытых функций и скрытых каналов (СК). Особенно в контексте скрытого вторжения и утечки данных сети промышленных систем управления (ИС) являются ценной мишенью для атак, основанных на сокрытии информации [1].

Третья версия протокола передачи гипертекста (HTTP) находится на завершающей стадии стандартизации IETF. Помимо повышения безопасности и гибкости, он обещает преимущества с точки зрения производительности. HTTP/3 использует более эффективную схему сжатия заголовков и заменяет TCP на QUIC, транспортный протокол, переносимый поверх UDP, первоначально предложенный Google и в настоящее время также стандартизированный. Хотя ранние реализации HTTP/3 уже существуют, и некоторые веб-сайты объявляют о его поддержке, он был предметом нескольких исследований. В работе [2] показано, что за исключением веб-сайтов, загружающих объекты из ограниченного набора сторонних доменов (избегая устаревших протоколов), наблюдается больший прирост производительности при использовании HTTP/3. Однако эксперименты показали, что HTTP/3 обеспечивает значительные преимущества только в сценариях с высокой задержкой или низкой пропускной способностью [2].

Протокол HTTP/3 функционирует на прикладном уровне модели OSI. Он не имеет существенных отличий от HTTP/2 точки зрения семантики. Основное отличие данных двух протоколов в способе транспортировки пакетов. Улучшения производительности HTTP/3 связаны с использованием на транспортном уровне протокола QUIC, использующего в своей базе протокол UDP [3]. На рисунке 1 приведено сравнение протоколов HTTP/2 и HTTP/3.

Транспортировка пакетов в HTTP/3 осуществляется через несколько потоков в рамках QUIC соединения. Соединение в протоколе QUIC, показанное на рисунке 2, происходит путем отправки первого пакета, содержащего в себе TLS-Hello (TLC C), на который с сервера придет ответ с TLS-Hello (TLS S) [4]. После этого может быть начата передача пакетов по протоколу HTTP/3.

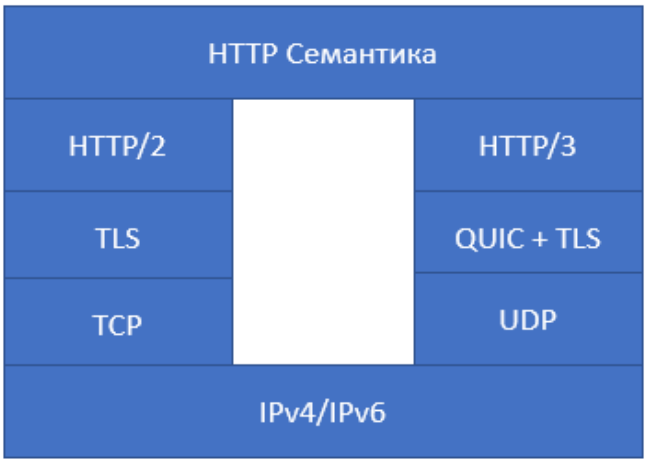

Рис. 1. Сравнение протоколов HTTP/2 и HTTP/3

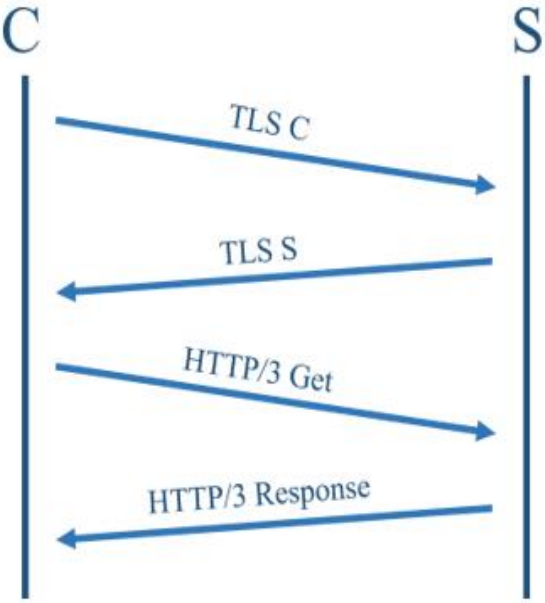

Рис. 2. Соединение QUIC

Если подключение ранее уже происходило, соединение будет установлено по QUIC 0-RTT, как показано на рисунке 3.

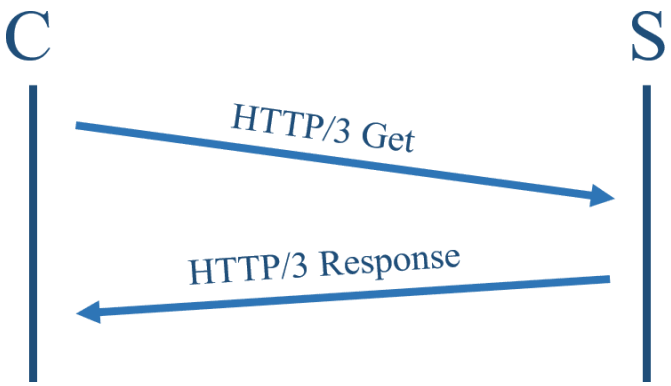

Рис. 3. Соединение QUIC 0-RTT

В данном случае считается, что сервер обладает необходимыми параметрами для расшифровки, получения и отправки пакетов HTTP/3.

2. Методы

Каждый скрытый канал имеет свои особенные признаки, отличающие его от легитимного трафика. Однако некоторые признаки делают это не так эффективно, как другие [5-7].

2.1 Оценка эффективности признаков скрытых каналов с использованием бита Fixed Bit

Для скрытого канала с использованием бита Fixed Bit свойственно наличие в данном поле значения, отличного от единицы. Пакеты, содержащие значение Fixed Bit равное нулю, считаются некорректными. Пакет со значением Fixed Bit, равным нулю, показан на рисунке 4.

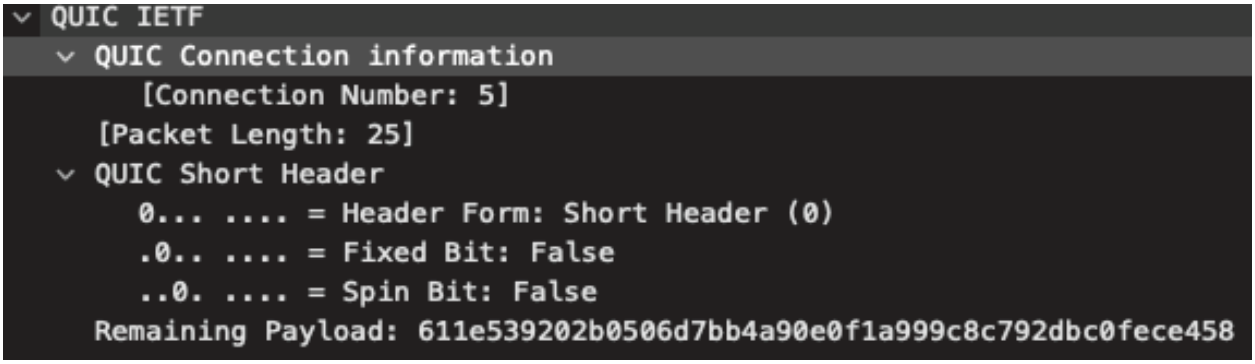

Рис. 4. СК с использованием Fixed Bit

При обучении нейронной сети наличие в данном поле иных значений будет являться признаком скрытого канала. Данный признак сильно повышает вероятность обнаружения скрытого канала.

2.2 Оценка эффективности признаков скрытых каналов с использованием кадра PADDING

Скрытый канал с использованием кадра PADDING имеет несколько признаков, подходящих для его обнаружения. Один из признаков — наличие последовательно идущих кадров PING и PADDING, кодирующих некоторое сообщение. При создании соединения кадр PING и PADDING используются часто, но кроме них также используется кадр CRYPTO, отвечающий за TLS рукопожатие. Последовательность этих кадров не определена, они могут идти в

любом порядке, однако наличие идущих один за другим кадров PING и PADDING может являться признаком скрытого канала. Вышеизложенный признак отображен на рисунке 5.

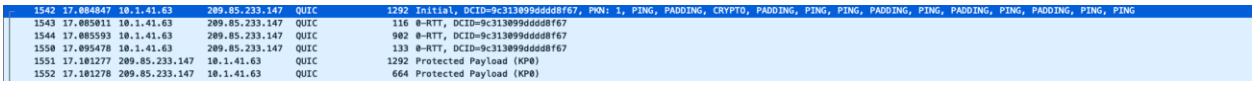

Рис. 5. СК с использованием кадра PADDING

Данный признак не дает однозначного ответа, является ли трафик легитимным, однако повышает вероятность обнаружения СК.

Второй признак — длина кадра PADDING состоящая только из единиц и нулей. Кадр PADDING может быть любым значением, что делает вероятность подряд идущих кадров PADDING с длиной, состоящей из единиц и нулей, крайне малой. Пример кадра со значением длины, состоящим из единиц и нулей, показан на рисунке 6.

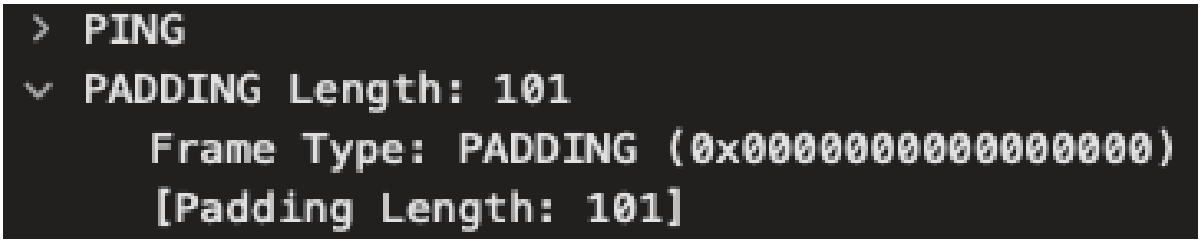

Рис. 6. Длина кадра PADDING из единиц и нулей

Данный признак повышает вероятность обнаружения СК.

Третий признак — увеличение общей длины пакета. Данный признак может быть менее эффективным, так как длина пакета может варьироваться от множества других параметров.

2.3 Оценка эффективности признаков скрытых каналов с использованием кадра PING

Скрытый канал с использованием кадра PING имеет один признак, отличающий его от легитимного трафика. Данным признаком является наличие или отсутствие единичного кадра PING в пакете инициализации соединения. Как правило, пакеты инициализации включают в себя от одного до трех кадров PING, что делает отсутствие данного кадра в пакете подозрительным ровно так же, как и наличие всего одного такого кадра. Данный признак может редко встречаться и в легитимном трафике.

3. Результаты

При создании датасета для машинного обучения были подобраны признаки каждого из известных скрытых каналов в протоколе HTTP/3 [8], описанные выше. В результате работы наивного Байевского классификатора были получены значения, по которым составлена таблица.

Таблица. Эффективность алгоритмов обнаружения скрытых каналов

Название СК	Признак СК	Вероятность обнаружения
GOAWAY	Четность или нечетность значения идентификатора соединения	99%
DATA	Количество кадров DATA на один пакет	59%
SETTINGS	Количество параметров настроек и четность или нечетность их значений	74%

В процессе обучения было выявлено, что вероятность обнаружения скрытого канала напрямую зависит от количества входных данных для тренировки [9]. Вместе с этим растет и время, затрачиваемое на обучение, как показано на рисунке 7.

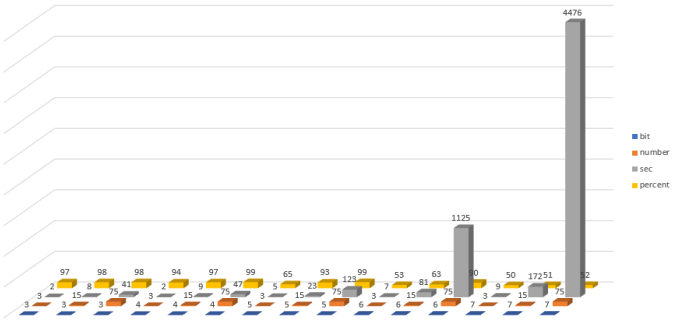

Рис. 7. Гистограмма зависимости времени тренировки и вероятности обнаружения канала от величины передаваемого сообщения и количества тренировочных данных

Наивный Байевский классификатор успешно обнаруживает СК с использованием GOAWAY, что отображено на рисунке 8.

При обучении обнаружения СК с использованием кадра SETTINGS классификатор успешно отличает легитимный трафик от нелегитимного по количеству полей в кадре настроек инициализации соединения. Консольный вывод программы отображен на рисунке 9.

Для СК с использованием кадра DATA классификатор успешно сигнализирует о наличии скрытого канала в 59 процентах случаев. Консольный вывод программы отображен на рисунке 10.

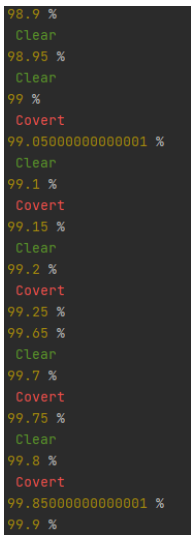

Рис. 8. Консольный вывод работы алгоритма обнаружения скрытого канала по кадру GOAWAY



Рис. 9. Консольный вывод работы алгоритма обнаружения скрытого канала по кадру SETTINGS

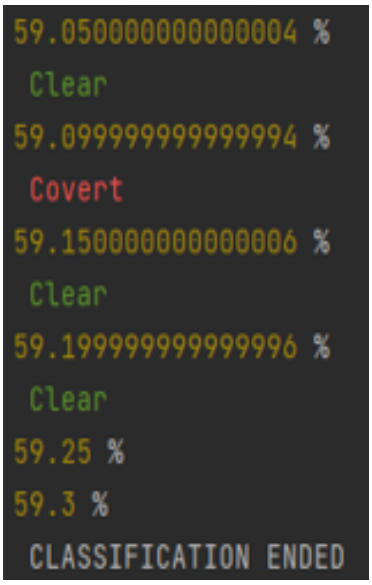

Рис. 10. Консольный вывод работы алгоритма обнаружения скрытого канала по кадру DATA

В связи с низкой вероятностью обнаружения скрытого канала с использованием кадра DATA было принято решение в дальнейшей работе использовать другой классификатор [10].

4. Заключение

В данной работе были изучены скрытые каналы в протоколе HTTP/3, а также проведена оценка их пропускной способности. Проанализированы признаки для формирования из полей трафика полезной информации для обучения классификатора. Для обучения был использован наивный Байевский классификатор для прогнозирования существования активного СК в системе. Дан сравнительный анализ пропускной способности каналов, сделан вывод об их опасности. Определено направление дальнейшей работы, включающее разработку и тестирование иных классификаторов для выявления наиболее точного, который может быть применен на практике

Литература

1. Lamshöft K., Dittmann J. Assessment of hidden channel attacks: Targetting modbus/tcp //IFAC-PapersOnLine. – 2020. – Т. 53. – №. 2. – С. 11100-11107.
2. Trevisan M. et al. Measuring HTTP/3: Adoption and performance //2021 19th Mediterranean Communication and Computer Networking Conference (MedComNet). – IEEE, 2021. – С. 1-8.
3. ZdNet [Электронный ресурс] // Cloudflare, Google Chrome, and Firefox add HTTP/3 support— Режим доступа: https://www.zdnet.com/article/cloudflare-google-chrome-and-firefox-add-http3-support/ — Свободный — (дата обращения: 13.02.2022)
4. Fathi-Kazerooni S., Rojas-Cessa R. Gan tunnel: Network traffic steganography by using gans to counter internet traffic classifiers //IEEE Access. – 2020. – Т. 8. – С. 125345-125359.
5. Алексеев В. М. Скрытые каналы передачи информации //Мир транспорта. – 2017. – Т. 15. – №. 4. – С. 50-56.
6. Когос К. Г., Финошин М. А. Перспективные подходы к обнаружению сетевых скрытых каналов //Безопасность информационных технологий. – 2021. – Т. 28. – №. 2. – С. 54-61.
7. Тимонина Е. Е. Анализ угроз скрытых каналов и методы построения гарантированно защищенных распределенных автоматизированных систем : дис. – М. : [Рос. НИИ информ. технологий и систем автоматизир. проектирования], 2004.
8. Devopedia [Электронный ресурс] // Naive Bayes Classifier — Режим доступа: https://devopedia.org/naive-bayes-classifier — Свободный — (дата обращения: 27.03.2022).
9. BigDataSchool [Электронный ресурс] // Dataset data preparation — Режим доступа: https://www.bigdataschool.ru/blog/dataset-data-preparation.html — Свободный — (дата обращения: 27.03.2022).
10. AnalyticSteps [Электронный ресурс] // 6 Types of Classifiers in Machine Learning — Режим доступа: https://www.analyticssteps.com/blogs/types-classifiers-machine-learning — Свободный — (дата обращения: 27.03.2022)

References

1. Lamshöft K., Dittmann J. Assessment of hidden channel attacks: Targetting modbus/tcp //IFAC-PapersOnLine. – 2020. – Т. 53. – №. 2. – С. 11100-11107.
2. Trevisan M. et al. Measuring HTTP/3: Adoption and performance //2021 19th Mediterranean Communication and Computer Networking Conference (MedComNet). – IEEE, 2021. – С. 1-8.
3. ZDNet [Electronic resource] // Cloudflare, Google Chrome, and Firefox add HTTP/3 support— Access mode: https://www.zdnet.com/article/cloudflare-google-chrome-and-firefox-add-http3-support / — Free — (accessed: 13.02.2022)
4. Fathi-Kazerooni S., Rojas-Cessa R. Gan tunnel: Network traffic steganography by using gans to counter internet traffic classifiers //IEEE Access. – 2020. – Т. 8. – С. 125345-125359.
5. Alekseev V. M. Hidden channels of information transmission //The world of transport. – 2017. – Vol. 15. – No. 4. – pp. 50-56.
6. Kogos K. G., Fioshin M. A. Promising approaches to the detection of network hidden channels //Information technology security. – 2021. – Vol. 28. – No. 2. – pp. 54-61.
7. Timonina E. E. Threat analysis of hidden channels and methods of constructing guaranteed protected distributed automated systems : dis. – M. : [Russian. Research Institute inform. technologies and automation systems. design], 2004.
8. Devopedia [Electronic resource] // Naive Bayes Classifier — Access mode: https://devopedia.org/naive-bayes-classifier — Free — (accessed: 03/27/2022).
9. BigDataSchool [Electronic resource] // Dataset data preparation — Access mode: https://www.bigdataschool.ru/blog/dataset-data-preparation.html — Free — (accessed: 03/27/2022).
10. AnalyticSteps [Electronic resource] // 6 Types of Classifiers in Machine Learning — Access mode: https://www.analyticssteps.com/blogs/types-classifiers-machine-learning — Free — (accessed: 03/27/2022)

© Симачев А. Ю. 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022.

Для цитирования: Симачев А. Ю. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ ОБНАРУЖЕНИЯ СКРЫТЫХ КАНАЛОВ В ПРОТОКОЛЕ HTTP/3// Научно-образовательный журнал для студентов и преподавателей «StudNet» 6/2022