УДК *004.056*

ТЕХНОЛОГИЯ АВТОМАТИЗИРОВАННОГО ФОРМИРОВАНИЯ БАЗЫ ЛЕГИТИМНЫХ TLS-ОТПЕЧАТКОВ

Д.И. Неслуховский, Д.С. Горин
МИРЭА – Российский технологический университет, г. Москва, Россия

Аннотация. В работе рассматривается технология автоматизированного формирования базы легитимных клиентских TLS-отпечатков на основе контролируемого воспроизведения сетевых сессий в изолированном периметре. Описываются этапы

подготовки окружений, запуска клиентских приложений, захвата трафика и извлечения клиентских отпечатков из сообщений ClientHello для дальнейшего использования в системах мониторинга и защиты информации.
Ключевые слова: TLS fingerprinting; идентификация сетевого трафика; цифровые отпечатки; база отпечатков; мониторинг трафика; обнаружение аномалий.

TECHNOLOGY FOR AUTOMATED CONSTRUCTION OF A DATABASE OF LEGITIMATE CLIENT TLS FINGERPRINTS

D.I. Neslukhovskiy, D.S. Gorin
MIREA – Russian Technological University, Moscow, Russia

Abstract. The paper presents a technology for automated construction of a database of legitimate client TLS fingerprints based on controlled replay of network sessions in an isolated environment. The approach covers environment preparation, client application deployment, traffic capture, and extraction of client fingerprints from ClientHello messages for subsequent use in traffic monitoring and information security systems.
Keywords: TLS fingerprinting; network traffic identification; digital fingerprints; fingerprint database; traffic monitoring; anomaly detection.

Введение

Идентификация сетевого трафика является важным этапом защиты информации и организации пассивного мониторинга, поскольку позволяет устанавливать соответствие между наблюдаемыми соединениями и типами используемого клиентского программного обеспечения (ПО), включая веб-браузеры, мессенджеры, почтовые клиенты и иные сетевые приложения. Существенная доля трафика в современных сетях защищается с использованием протокола Transport Layer Security (TLS), что делает особенно востребованными методы, не требующие расшифрования содержимого сеанса и опирающиеся на анализ служебных параметров протокольного взаимодействия.

Одним из практичных подходов к идентификации зашифрованного трафика является набор методов, в совокупности именуемых «TLS fingerprinting», при которых цифровые отпечатки (ЦО, англ. fingerprints) формируются по совокупности параметров установления и ведения защищенного соединения, в первую очередь по структуре и содержимому сообщения ClientHello, и тем самым отражают устойчивые особенности конкретных реализаций клиентских приложений [1].

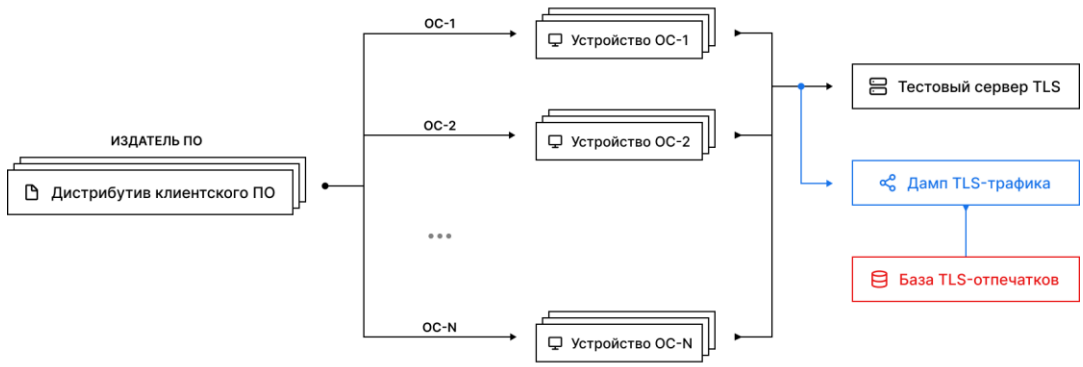
Как показано в работе [2], по мере выхода новых версий прикладного ПО пространство используемых протокольных признаков постоянно расширяется, в конфигурациях клиентов появляются ранее не встречавшиеся элементы, что приводит к быстрому устареванию статичных наборов эталонных профилей. Это обуславливает необходимость поддерживать базу легитимных клиентских отпечатков, формирующих набор эталонных профилей, как регулярно

и верифицируемо пополняемый ресурс, учитывающий эволюцию конфигураций реальных клиентов.

Основная часть

Постановка задачи. В работе рассматриваются организационные и технические вопросы получения исходных данных для методов идентификации клиентов по их ЦО в TLS-соединениях. Целью является проектирование поэтапного процесса автоматизированного формирования базы легитимных клиентских отпечатков, независимого от конкретных алгоритмов их последующего анализа. Предполагается, что процесс должен, используя только верифицированные экземпляры клиентского ПО и контролируемый тестовый периметр, автоматически собирать и разворачивать требуемые версии приложений, инициировать характерные для них сетевые сценарии, регистрировать результирующий трафик и извлекать из него клиентские ЦО в структурированном виде. Дополнительными требованиями являются масштабируемость по числу поддерживаемых клиентов и окружений, а также пригодность к регулярному повторному запуску по мере выхода новых версий программного обеспечения.

Методика формирования базы. Общая структура предлагаемого процесса формирования базы легитимных ЦО представлена на схеме и включает последовательные стадии от подготовки экземпляров клиентского ПО до аккумуляции результатов в базе данных.



Структура процесса формирования базы клиентских TLS-отпечатков
Structure of the client TLS fingerprint database generation process

На этапе подготовки окружений выполняется систематический сбор экземпляров клиентского ПО: с официальных ресурсов издателей ПО загружаются установочные пакеты, образы и другие дистрибутивные формы актуальных и архивных версий, после чего они разворачиваются на изолированных тестовых стендах с различными сочетаниями операционных систем и аппаратных платформ. Это обеспечивает

однозначную идентификацию исходной конфигурации и позволяет учитывать влияние программно-аппаратного окружения на формируемые клиентские TLS-отпечатки.

Далее развернутые экземпляры клиентского ПО в автоматизированном режиме выполняют заранее заданные сценарии взаимодействия с целевой (тестовой) серверной инфраструктурой в закрытом сетевом контуре, свободном от посторонних источников трафика; сценарии моделируют типичные для соответствующих классов приложений действия пользователя, что позволяет получать ЦО в условиях, приближенных к реальной эксплуатации.

Сетевая активность в пределах выделенного контура регистрируется на серверной стороне и сохраняется в виде дампов трафика в исходном виде для последующего анализа. В рамках автоматизированной обработки дампов выделяются соединения, инициированные тестируемыми клиентами, и извлекаются релевантные протокольные параметры, в первую очередь поля сообщения ClientHello (версии протокола, наборы шифров, расширения и связанные параметры), на основе которых формируются один или несколько клиентских ЦО на соединение. Полученные отпечатки вместе с метаданными (тип приложения, версия и конфигурация, операционная система, аппаратная платформа, дата и условия сбора и др.) заносятся в итоговую базу данных. Такая организация процесса упрощает его регулярный перезапуск и масштабирование при расширении перечня поддерживаемых приложений и платформ.

Практическое применение. Сформированная таким образом база легитимных клиентских ЦО может использоваться в системах мониторинга и обнаружения аномалий для сопоставления наблюдаемых клиентских отпечатков, вычисляемых по сообщениям ClientHello, с эталонными профилями и выделения соединений, инициируемых неизвестными либо подозрительными конфигурациями клиентского ПО. В системах фильтрации и контроля доступа такая база служит дополнительным источником признаков для проверки согласованности прикладных атрибутов (таких как заявленный тип или версия клиента) с фактической конфигурацией его TLS-стека [3]. Также, в задачах противодействия автоматизированным злоупотреблениям и вторжению в инфраструктуру наличие актуальных профилей легитимных клиентов облегчает выявление ClientHello, сформированных типовыми сетевыми стеками общего назначения (например, встроенными реализациями в средах выполнения JavaScript или Python), конфигурация которых заметно отличается от характерных для реальных пользовательских приложений.

Заключение

Идентификация клиентов по их ЦО представляет собой важный инструмент анализа зашифрованного трафика. Для надежного применения этого инструмента недостаточно одних алгоритмов вычисления ЦО, также критически важен и конвейер, который в контролируемых условиях формирует достоверные клиентские профили и обеспечивает их регулярное обновление с учетом дрейфа признаков и появления новых конфигураций. Описанный процесс автоматического формирования базы легитимных клиентских отпечатков, основанный на воспроизведении типичных сетевых сценариев и последующей обработке трафика в контролируемом периметре, решает эту задачу и создает основу для интеграции методов TLS fingerprinting в прикладные системы мониторинга и защиты информации.

Список использованных источников

1. Husak M., Cermak M., Jirsik T., Celeda P. (2015) Network-Based HTTPS Client Identification Using SSL/TLS Fingerprinting. *10th International Conference on Availability, Reliability and Security (ARES), Toulouse, France, 24-27 August, 2015*. 389–396. DOI 10.1109/ARES.2015.35.

2. Неслуховский Д.И., Нефедов В.С. (2025) Оценка расширения пространства признаков TLS-отпечатков веб-браузеров во времени. *Кибернетика и информационная безопасность «КИБ-2025» : Сборник научных трудов Третьей Всероссийской научно-технической конференции: в 2-х томах, Москва, 3-4 декабря 2025 года.* Москва, НИЯУ МИФИ. 2. 70–71. EDN RVUAYZ.

3. Heino J., Hakkala A., Virtanen S. (2023) Categorizing TLS traffic based on JA3 pre-hash values. *Procedia Computer Science*. 220 (2023). 94–101. DOI 10.1016/j.procs.2023.03.015.

References

1. Husak M., Cermak M., Jirsik T., Celeda P. (2015) Network-Based HTTPS Client Identification Using SSL/TLS Fingerprinting. *10th International Conference on Availability, Reliability and Security (ARES), Toulouse, France, 24-27 August, 2015*. 389–396. DOI 10.1109/ARES.2015.35.

2. Neslukhowskiy D.I., Nefedov V.S. (2025) Evaluation of the Expansion of the Feature Space of TLS Fingerprints of Web Browsers Over Time. *Cybernetics and Information Security «KIB-2025» : Proceedings of the Third All-Russian Scientific and Technical Conference, in 2 Volumes, Moscow, December 3–4, 2025.* Moscow, MEPhI. 2. 70–71. EDN RVUAYZ.

3. Heino J., Hakkala A., Virtanen S. (2023) Categorizing TLS traffic based on JA3 pre-hash values. *Procedia Computer Science*. 220 (2023). 94–101. DOI 10.1016/j.procs.2023.03.015.

Сведения об авторах

Неслуховский Д.И., студент каф. КБ-2 «Информационно-аналитические системы кибербезопасности», Институт кибербезопасности и цифровых технологий,

федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет», neslukhovskiy.d@yandex.ru.

Горин Д.С., канд. экон. наук., доцент, зав. каф. КБ-3 «Разработка программных решений и системное программирование», Институт кибербезопасности и цифровых технологий, федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет», gorin@mirea.ru.

Information about the authors

Neslukhovskiy D.I., Student of Department KB-2 «Informational and Analytical Cybersecurity», Institute of Cybersecurity and Digital Technologies, Federal State-Funded Educational Institution of Higher Education «MIREA – Russian Technological University», neslukhovskiy.d@yandex.ru.

Gorin D.S., Cand. Econ. Sci., Associate Professor, Head of the Department KB-3 «Software Development and Systems Programming», Institute of Cybersecurity and Digital Technologies, Federal State-Funded Educational Institution of Higher Education «MIREA – Russian Technological University», gorin@mirea.ru.