МЕТОДЫ АНАЛИЗА ЗАШИФРОВАННОГО ТРАФИКА ДЛЯ ОБНАРУЖЕНИЯ СКРЫТЫХ УГРОЗ

Тамара Радивилова

***Аннотация**: Злоумышленники и вредоносное программное обеспечение используют зашифрованный протокол SSL/TLS для осуществления несанкционированной активности, что создает проблемы при обнаружении вторжений. Существует два подхода к обнаружению вторжений в зашифрованном трафике: без его дешифрования и после его дешифрования. В ходе работы проведен анализ основных методов дешифрования трафика протокола SSL/TLS. В работе представлены методы и технологии обнаружения вредоносной активности в зашифрованном трафике, которые используются ведущими компаниями. Также предложен метод перехвата и дешифровки трафика, передаваемого по протоколу SSL/TLS, который можно применять при удаленном прослушивании сети, что позволяет дешифровывать передаваемые данные в режиме приближенному к реальному времени.*

***Ключевые слова**: протокол SSL/TLS, угрозы, уязвимость, системы обнаружения сетевых вторжений, методы дешифрования.*

***ITHEA Keywords**: E.3 Data Encryption, C.2 Computer-communication networks - C.2.2 Network Protocols, I.5 Pattern recognition - I.5.4 Applications, K.6 Management of computing and information systems – K.6.5 Security and Protection.*

Введение

В последнее время наметился тренд увеличения доли шифрованного трафика. По оценкам компании Cisco на данный момент 60% трафика в Интернет зашифровано, а согласно прогнозам Gartner к 2019-му уже 80% трафика будет таковым [Cisco, 2014, Orans, 2016]. Шифрование необходимо для обеспечения приватности граждан, сохранения тайн в секрете, выполнения требований законодательства. Но злоумышленники также используют шифрование для обхода механизмов детектирования их несанкционированной активности, скрывая взаимодействие с командными серверами вредоносных программ и для других задач. [Cisco, 2014, Orans, 2016, Лукацкий, 2018]

С одной стороны средства защиты не могут видеть, что происходит в зашифрованном трафике (по данным Ponemon Institute 64% компаний не могут детектировать вредоносный код в зашифрованном трафике). Для проникновения в зашифрованные соединения организации часто используют атаку Man-in-the-Middle (MITM), которую они осуществляют в легальных целях, но это не является легальным (нарушение тайны переписки, требования законодательства по обеспечению конфиденцильности информации). Обычно на периметре корпоративной или ведомственной сети устанавливается шлюз или кластер из шлюзов, которые осуществляют “перехват” и дешифрование данных внутри сети компании, чтобы защититься от атак, использующих протокол SSL/TLS (SSL - Secure Sockets Layer, TLS - Transport Layer Security) для передачи вредоносного содержимого, а также для анализа передаваемых данных системами обнаружения вторжений (IDS). [Ponemon, 2016, D'Hoinne, 2013]. После дешифрования трафик проверяется на наличие вредоносных активностей, зашифровывается снова и отправляется на IP-адрес назначения. Обнаружение вредоносных активностей в SSL/TLS трафике является трудоемким и сложным, поскольку шифрование мешает эффективности классических методов обнаружения и является сложной проблемой для IDS.

Целью этой работы является обзор методов анализа трафика и разработка метода дешифрования трафика SSL/TLS для обнаружения скрытых угроз.

Основные механизмы проверки трафика SSL/TLS и разработки ведущих компаний

Разработчики ведущих компаний и ученые ведут активную работу по разработке методов обнаружения вредоносной активности в зашифрованном трафике.

Cisco Encrypted Traffic Analytics извлекает и анализирует четыре основных элемента данных: последовательность длин и времени пакета, распределение байтов, специфичные для TLS функции и исходный пакет данных. Уникальная архитектура специализированных интегральных схем Cisco (ASIC) обеспечивает возможность извлечения этих элементов данных без замедления работы сети передачи данных. [Cisco, 2014]

Cisco Stealthwatch Enterprise использует NetFlow, прокси-серверы, телеметрию конечных точек, механизмы политики и доступа, сегментацию трафика и многое другое, чтобы установить базовое «нормальное» поведение для хостов и пользователей на предприятии. Stealthwatch может коррелировать трафик с глобальными угрозами, чтобы автоматически идентифицировать зараженные хосты, командные и контрольные коммуникации и подозрительный трафик.

Stealthwatch поддерживает глобальную карту рисков - очень широкий поведенческий профиль о серверах в Интернете, идентифицирующий серверы, связанные с атаками, может быть использован как часть атаки в будущем. Это не является черным списком, а представляет собой целостную картину с точки зрения безопасности. Stealthwatch анализирует новые зашифрованные элементы данных трафика в расширенном режиме NetFlow, применяя методы машинного обучения и статистическое моделирование, чтобы выявлять вредоносные шаблоны в зашифрованном трафике, для выявления угроз и улучшения реакции на инциденты.

The SANS Institute предлагает использовать четыре подхода к дешифрованию соединений SSL/TLS: 1) выполнение проверки на самом сервере; 2) прокси-сервер терминалов; 3) дешифрование самим IDS; 4) автономный инструмент для дешифрования соединения [Butler, 2013, Bakhdlaghi, 2017].

1. Выполнение проверки на самом сервере. Самый простой способ проверить зашифрованный трафик - использовать IDS на основе хоста (HIDS) на самом сервере, где дешифруется трафик, принадлежащий этому серверу. HIDS может отслеживать действия сервера и искать необычное поведение, изменения в базах данных, системных файлах или любых критически важных данных. Установка HIDS может добавить дополнительную нагрузку, которая может негативно повлиять на производительность, особенно для нагруженного сервера.

2. SSL/TLS терминальный прокси (обратный прокси). Обратный прокси - это сервер, который выступает в качестве посредника между серверами бекэнда и клиентами. Он принимает запросы клиентов и извлекает ресурсы, эффективно скрывающие бекэнд сервера от клиентов. Обратный прокси сервер может быть настроен для выполнения шифрования SSL/TLS, выступающего в качестве SSL/TLS терминального проски, который снимает нагрузку с дешифровки соединений SSL/TLS, передавая незашифрованный трафик на ассоциированные сервера. Однако использование прокси-сервера SSL / TLS позволяет использовать IDS внутри локальной сети серверов.

3. IDS выполняющий дешифрование. IDS предоставляется возможность выполнения процесса дешифрования при закрытом ключе. Это может быть предварительный процессор или плагин, который поддерживает дешифрование и нормализацию трафика перед тем, как перейти к механизму обнаружения. В настоящее время нет препроцессора для Snort для выполнения процесса дешифрования, хотя теоретически возможно разработать такой предварительный процессор или подключаемый модуль (Snort FAQ, n.d.). Однако функция дешифрования доступна в некоторых устройствах IDS, таких как Juniper IDP.

4. Автономный инструмент выполняющий дешифрование. Инструмент Viewssld использовался для дешифрования соединения SSL/TLS, использующего обмен ключами RSA. Viewssld - это бесплатный инструмент с открытым исходным кодом, который может дешифровывать трафик SSL / TLS для IDS. Он работает, прослушивая интерфейс на определенном IP-адресе, дешифруя зашифрованный трафик с помощью закрытого ключа сервера и выдает дешифрованный трафик на порт прослушивания IDS. Он не поддерживает обмен ключами Диффи-Хелмана, а поддерживает только обмен ключами RSA.

Компания Symantec использует решение Encrypted Traffic Management для устранения зашифрованного скрытого трафика [Symantec, 2017]. Ключевым компонентом этого набора решений SSL Visibility Appliance является высокопроизводительное средство проверки, дешифрования и управления SSL, масштабирование до 9 Гбит/с SSL-дешифрования и способное одновременно передавать дешифрованную информацию нескольким инструментам безопасности. Возможности проверки и дешифрования SSL, предоставляемые SSL Visibility Appliance, позволяют существующим средствам безопасности и сети (IDS/IPS - Intrusion Prevention Systems, DLP, анализаторам вредоносных программ, Next Gen Firewalls - NGFW, криминалистике, платформам аналитики безопасности), получать доступ к открытым текстам в потоках SSL, тем самым позволяя устройству безопасности эффективно выполнять свою работу, даже с SSL-зашифрованным трафиком.

Кампания Gigamon предлагает Security Delivery Platform GigaSECURE, в которой операциям безопасности разрешается использовать уникальный архитектурный подход «зоны дешифровки» для решения проблемы дешифрования SSL/TLS [Gigamon, 2017]. В «зоне дешифровки» трафик SSL/TLS дешифруется один раз и подается на несколько защищенных инструментов для дальнейшего анализа и проверки, тем самым устраняя ненужные и повторяющиеся циклы дешифрования и повторного шифрования в инфраструктуре. Благодаря расширенному дешифрованному решению дешифрования SSL/TLS, Gigamon обеспечивает полную видимость сети для выявления вредоносных угроз и предоставления дешифрованного трафика, представляющего интерес для соответствующих инструментов безопасности для немедленного анализа.

Необходимо отметить, что системы дешифровки трафика, т.е. устройства, реализующие функции SSL–прокси SSL разгрузки, в дальнейшем будут все более востребованными, учитывая рост использования протокола шифрования SSL/TLS. Они позволяют не только дешифровать трафик для снижения нагрузки на конечные серверы, но и отправить его на дополнительный анализ с привлечением сторонних средств защиты информации.

Также, существует много ситуаций, когда администраторы ИТ должны использовать проверку пакетов, например Wireshark. Обычно самым простым способом дешифрования данных является использование закрытого ключа для соответствующего открытого ключа. Wireshark предоставляет еще одно средство для дешифрования данных, а также с использованием пре-мастер ключа.

В работах [McGrew, 2016; McGrew1, 2016; Strasák, 2017] рассмотрены методы обнаружения вредоносного трафика HTTPS без его дешифрования. Такие методы очень важны, так как в этом случае отпадает необходимость в каком-либо перехватчике трафика HTTPS, соблюдалась бы конфиденциальность и безопасность сообщений, и обнаружение вторжений происходило бы быстрее. Кроме того, эти методы могут использоваться совместно с некоторым перехватчиком трафика HTTPS в качестве первого уровня обнаружения вторжений в сетевом трафике, и если какой-либо трафик будет подозрительным, тогда для дешифрования будет использоваться перехватчик трафика HTTPS.

В работе [McGrew, 2016] авторы предлагают обнаружение вредоносной активности в HTTPS трафике без его дешифровки, однако их метод основан на сборе данных из незашифрованных сообщений TLS-рукопожатия. В отличие от них, в работе [Strasák, 2017] используются данные без дешифрования. Авторы работы [McGrew1, 2016] используют без дешифрования потоки TLS, потоки DNS, HTTP заголовки и незашифрованную информацию заголовка TLS для обнаружения вредоносного трафика HTTPS. Однако данные методы применимы только после детального статистического анализа трафика в сети и его дальнейшего анализа методами машинного обучения, так как трафик в каждой сети имеет свои характерные особенности.

Ponemon Institute попросил респондентов оценить вероятность возникновения конкретных атак и возможность противостояния этим атакам, которые показаны в таблице 1 [Ponemon, 2016].

Из таблицы 1 видно, что вероятность противодействия атаке достаточно мала, по сравнению с вероятностью ее появления.

Таблица 1. Вероятность возникновения конкретных атак и возможность противостояния этим атакам

Типы атак	Вероятность	
	атаки	Противостояния атаке
1. Злоумышленник делает фишинговые угрозы еще более законными, а даже осведомленые получатели считают, что использование TLS гарантирует им безопасность. Однако, нажав на ссылку, злоумышленник отправляет пользователей к серверу SSL, на который загружено злонамеренное программным обеспечением, которое заражает клиента, поскольку трафик вредоносных программ зашифрованный и не распознается системами обнаружения вторжений.	79%	17%
2. Злоумышленник отправляет зашифрованный поток защищенных, чувствительных и других критических данных, поступающих через брандмауэр через "обычные" порты (443,80 и др.), которые брандмауэр настроен принять, поскольку они являются утвержденными портами.	78%	30%
3. Ряд злоумышленников использует шифрование, чтобы скрыть информацию о сети, включая пароли и конфиденциальные данные, которые они присылают на серверы SSL. Шифрование ослепляет системы мониторинга/инспектирования для этой внутренней сети.	74%	16%
4. Злоумышленник мешает коммуникациям с вредоносным программным обеспечением, когда червь, вирус или ботнет «звонит домой», чтобы отправить украденные данные к главному компьютеру или загрузить инструкции или больше вредоносных кодов.	66%	26%
5. С помощью межсайтового скриптинга злоумышленники похищают файлы cookie, которые могут использоваться для захвата аккаунта или сеанса, изменения настроек, отравления cookie и / или ложной рекламы. Все это можно выполнить, прячась в SSL / TLS трафике.	62%	19%

Предлагаемый метод дешифрования трафика

Описанный в данной статье метод дешифровки TLS-трафика предполагает у злоумышленника наличие доступа к компьютеру или сети, либо же наличие закладки на компьютере жертвы, которая может собрать данные о сессиях. Такие условия нужны для формирования файла сессионных ключей, который будет использован вместе с соответствующим перехваченным трафиком [Волков, 2016]. Перехватить трафик жертвы можно, находясь в любом участке сети на промежутке между сервером и объектом нападения.

Ниже приведено описание реализации предложенного метода к дешифровке TLS-трафика. В реализации использовался анализатор трафика Wireshark, который помогает провести анализ работы сети, диагностировать проблемы, а также имеет много других полезных возможностей.

Для проведения эксперимента была создана локальная сеть, состоящая из трех подсетей, веб-сервера и сервера доступа. Для подключения компьютеров из подсетей к веб-серверу использовался протокол HTTPS с использованием TLS-соединения. В одной из подсетей была добавлена дополнительная точка доступа, и закладка была сделана на одном из компьютеров, отправив ее по электронной почте. Затем, используя Wireshark, данные в сети были прочитаны дополнительной точкой доступа.

Для получения ключей включаем логгирование сессионных ключей, которые используются для зашифровки и дешифровки трафика. Получение таких логов не является трудоёмким. Их можно получить, например, из браузеров – браузеры Firefox и Chrome научились выводить в специально задаваемый файл данные, достаточные для деривации (получения) сессионных ключей, которыми шифруется передаваемый/принимаемый ими трафик, поскольку внутри TLS используется симметричное шифрование. Строго говоря, делают это не сами браузеры, а библиотека NSS в их составе; именно она задает формат записываемых файлов. Для дешифровки TLS необходимо иметь файл с логгированными записями сессионных ключей в NSS-формате и анализатор трафика Wireshark. Wireshark весьма чувствителен к формату NSS-файла, поэтому необходимо тщательно перепроверить сходимость числа байтов в каждом элементе строки и отсутствие лишних пробелов, что может сэкономить время.

Захватывать трафик нужно после того, как начнётся запись ключей в лог-файл, так как в противном случае нам не удастся завладеть сессионными ключами, которые соответствуют захваченным TLS-записям. Также необходимо помнить, что ключи являются временными, т.е. пригодны лишь для одной TLS-сессии. Также необходимо отслеживать обмен трафиком с определённым хостом и фильтрация по нужному протоколу, чтобы изначально отбросить

ненужные пакеты, проходящие через прослушиваемый интерфейс. После того, как удалось сформировать файл с сессионными ключами, нужно его привязать к Wireshark'у.

Теперь в содержимом пакета появилась вкладка «Decrypted SSL Data». Теперь, если перейти в эту вкладку можно увидеть текст запроса. Кроме того теперь можно выбрать любой пакет с протоколом SSL или TLS и в его контекстном меню выбрать функцию «Follow SSL Stream» – в результате получается содержимое пакетов. Как видно, несмотря на то, что общение проходит по HTTPS, мы видим передаваемый трафик и можем экспортировать его для дальнейшего анализа.

Описанный в данной работе метод обладает основным недостатком: он требует существенных затрат времени на составление файла с сессионными ключами. Однако предложенный метод можно формализовать, а в последующем и автоматизировать, что сократит временные затраты на реализацию данной атаки и, возможно, откроет новые возможности для проведения таких атак.

Особенностью описанного метода является то, что не обязательно перехватывать трафик на компьютере, который генерирует TLS-трафик, его можно перехватывать находясь в сети и прослушивая её. А добыть файл с сессионными ключами можно, поставив на компьютер жертвы закладку или просто скопировать его, имея доступ к компьютеру

Выводы

SSL/TLS стал универсальным стандартом для аутентификации и шифрования сообщений между клиентами и серверами. Он широко распространен в организациях и предприятиях и быстро растет из-за быстрого увеличения облачных, мобильных и веб-приложений. Однако SSL создает угрозу безопасности, вводя «слепое пятно», что увеличивает риск проникновения вредоносного ПО в организацию. Проверка SSL/TLS является важной и желательной функцией для аналитиков безопасности, но она имеет свою стоимость.

Для дешифрования трафика желательно выбрать способ дешифрования трафика, основанный на потребностях и структуре сети: на самом сервере, SSL/TLS терминальный прокси или использование автономного инструмента или возможностей, добавленных в IDS. Если HIDS установлен на самом сервере, он может добавить дополнительную нагрузку, которая может негативно повлиять на производительность, особенно для загруженного сервера.

В работе предложен метод дешифровки трафика SSL/TLS, который можно применять даже при удаленном прослушивании сети. Данный метод был автоматизирован и позволяет дешифровывать данные практически в режиме онлайн.

В работе [Anderson, 2017] проведен анализ использования TLS вредоносными и корпоративными приложениями, в ходе которого взяты миллионы зашифрованных потоков TLS и целевое исследование по 18 семействам вредоносных программ, которые состоят из тысяч уникальных образцов вредоносных программ и десяти тысяч вредоносных потоков TLS. Сделан вывод, что использование TLS вредоносными программами отличается от доброкачественного использования в настройках предприятия и что эти различия эффективно используются в правилах и классификаторах машинного обучения. В своей дальнейшей работе мы планируем провести анализ зашифрованного SSL/TLS трафика методами data science на обнаружение несанкционированной деятельности.

Bibliography

[Anderson, 2017] Blake Anderson, Subharthi Paul and David McGrew. Deciphering Malware's use of TLS (without Decryption). Journal of Computer Virology and Hacking Techniques, pp 1–17, 2017. https://doi.org/10.1007/s11416-017-0306-6

[Bakhdlaghi, 2017] Yousef Bakhdlaghi. Snort and SSL/TLS Inspection. SANS Institute. InfoSec Reading Room. P.24. 2017.

[Butler, 2013] J. Michael Butler. Finding Hidden Threats by Decrypting SSL. A SANS Analyst Whitepaper. 2013.

[Cisco, 2014] White paper. Encrypted Traffic Analytics. Cisco public, 2018.

[D'Hoinne, 2013] Jeremy D'Hoinne and Adam Hils. Security Leaders Must Address Threats From Rising SSL Traffic. Gartner, 2013.

[Gigamon, 2017] Whitepaper: Prevent Encrypted Threats and Data Loss with Inline SSL Decryption.

[McGrew, 2016] David McGrew, Blake Anderson, Subharthi Paul. Deciphering Malware's use of TLS (without Decryption). 6 Jul 2016.

[McGrew1, 2016] David McGrew, Blake Anderson. Identifying Encrypted Malware Traffic with Contextual Flow Data. 2016.

[Orans, 2016] Lawrence Orans, Adam Hils, Jeremy D'Hoinne, Eric Ahlm. Gartner Predicts 2017: Network and Gateway Security, 2016.

[Ponemon, 2016] Hidden Threats in Encrypted Traffic: A Study of North America & EMEA. Independently conducted by Ponemon Institute LLC, 2016.

[Strasák, 2017] František Strasák. Detection of HTTPS Malware Traffic. Bachelor project assignment. Czech Technical University in Prague. 2017. P.49.

[Symantec, 2017] A Technology Brief on SSL/TLS Traffic. Symantec Corporation World Headquarters.

[Волков, 2016] В.А. Волков. Об одном из методов атаки на протокол TLS «Young Scientist» • № 5 (32) • may, 2016, с.213-217.

[Лукацкий, 2018] Алексей Лукацкий. Как Cisco анализирует зашифрованный трафик без его расшифрования и дешифрования. January 15, 2018 [онлайн] Gblogs.cisco.com, Доступно: https://gblogs.cisco.com/ru/eta/

Информация об авторах

Тамара Радивилова *– к.т.н., доцент Харьковского национального университета радиоэлектроники; пр. Науки 14, 61166, Харьков, Украина; e-mail:: tamara.radivilova@gmail.com.*

Основные области научных исследований: самоподобные и мультифрактальные временные ряды, телекоммуникационные системы, управление трафиком, информационная безопасность

Annex for papers written in Russian

Methods of analysis encrypted traffic for hidden threats detection

Tamara Radivilova

Abstract*: Attackers and malicious software uses encrypted protocol SSL/TLS to perform unauthorized activity, which creates problems for intrusion detection. There are two approaches to intrusion detection in encrypted traffic: without decrypting it and after decrypting it. The analysis of the main methods of SSL/TLS protocol traffic decryption was carried out. The work presents methods and technologies for detecting malicious activity in encrypted traffic, which are used by leading companies. Also, a method for intercepting and decrypting traffic transmitted over SSL/TLS, which can be used for listening to the network remotely, offers a way to decrypt the transmitted data in almost real-time mode.*

Keywords*: protocol SSL/TLS, threats, vulnerability, Intrusion Detection Systems, decryption methods.*