МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт искусственного интеллекта
Базовая кафедра №252 – информационной безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема:
«Устройство и анализ алгоритмов по обходу DPI»

Студент группы ККСО-03-19	Николенко В.О.	_____ *(подпись)*
Научниый руководитель	Жанкевич А.О.	_____ *(подпись)*

Работа представлена к защите «__» _____ 2023 г.

Оценка: «__»

Москва – 2024

1. СОДЕРЖАНИЕ

2. ВВЕДЕНИЕ

В наше время информационные технологии развиваются уже далеко не семимильными шагами, с каждым годом появляется все больше методов передачи, шифрования, кодирования, анализа трафика, такие технологии как: TCP, UDP, TSL, SSL, HTTP, HTTPS, различные подписи с использованием эллиптических кривых, RSA, различные способы распределения ключей между клиентом и сервером.

Так как трафик это общение не только между машинами, но и между людьми...

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

3. ГЛОССАРИЙ

Давайте однозначно определим терминологию данной работы, с целью исключить недопонимания между её авторами и читателями.

DPI (англ. Deep Packet Inspection "глубокий анализ пакетов") - технология проверки сетевых пакетов по их содержимому с целью регулирования и фильтрации трафика, а также накопления статистических данных. В отличие от брандмауэров, DPI анализирует не только заголовки пакетов, но и полезную нагрузку, начиная со второго уровня модели OSI (канальный).

OSI (англ. Open Systems Interconnection "межсетевое взаимодействие открытых систем") - абстрактная модель представления одних и тех же данных, с которыми можно работать на разных уровнях, предлагаемых данной моделью: физическом, канальном, сетевом, транспортном, сеансовом, уровне представления, прикладном.

Физический Уровень - передача необработанных битов по физическим носителям (кабели, радиосигналы).
Примеры протоколов: Ethernet (физический аспект) USB, Bluetooth.

Канальный Уровень - организация надежной передачи данных между узлами одной сети; управление доступом к среде, обнаружение ошибок.
Примеры протоколов: Ethernet (кадры), Wi-Fi (IEEE 802.11), PPP (Point-to-Point Protocol).

Сетевой Уровень - маршрутизация и передача пакетов данных между различными сетями.
Примеры протоколов: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IPSec (для обеспечения безопасности).

Транспортный Уровень - обеспечение надежной передачи данных, контроль ошибок, восстановление соединений (TCP/UDP).
Примеры протоколов: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), SCTP (Stream Control Transmission Protocol).

Сеансовый Уровень - управление сессиями, установление, поддержание и завершение сеансов связи между приложениями.
Примеры протоколов: NetBIOS, PPTP (Point-to-Point Tunneling Protocol), RPC (Remote Procedure Call).

Уровень Представления - преобразование данных для представления их в удобном для приложений формате (шифрование, сжатие).
Примеры протоколов: SSL/TLS (для шифрования), JPEG, PNG (для изображения), ASCII, EBCDIC (кодировки данных).

Прикладной Уровень - взаимодействие с конечным пользователем через приложения (веб-браузеры, почтовые клиенты и т. д.).

Примеры протоколов: HTTP/HTTPS (веб-приложения), FTP (передача файлов), SMTP (электронная почта), DNS (система доменных имен).

Шифрование - процесс преобразования данных *(посредством таких операций как: линейных и нелинейных преобразований, наложения гаммы, и матричных преобразовний)* в форму, непонятную без ключа. Используется для обеспечения конфиденциальности информации (например, в коммуникациях).

Дешифрование - обратный процесс к шифрованию, преобразующий зашифрованные данные обратно в исходный вид с помощью ключа.

Кодирование - преобразование данных в другой формат для удобства передачи или хранения (например, Base64 для передачи бинарных данных через текстовые протоколы). Кодирование не является средством защиты.

Хеширование - одностороннее преобразование данных в уникальную фиксированную строку (хеш), которое невозможно обратным образом восстановить. Используется для проверки целостности данных, паролей и цифровых подписей.

4. ГЛУБОКИЙ АНАЛИЗ ПАКЕТОВ

Глубокий анализ пакетов/трафика - основообразующая система для контроля доступа к запрещённым ресурсам на территории конкретного государства. Таким образом

4.1. Применение

4.2. Виды

4.3. Виды обходов DPI

4.3.1. Shadowsocks

Shadowsocks - такой протокол который предполагает использование прокси-сервера. Сам же сервер использует шифрование для получения с клиента и отправки на него данных. Он был разработан для обхода интернет-цензуры и обеспечивает высокую скорость передачи данных.

Особенности данного алгоритма:

1) Шифрование: Shadowsocks использует различные алгоритмы шифрования (например, AES-256-GCM), что делает трафик менее заметным для DPI.
2) Прокси: Это SOCKS5-прокси, который позволяет передавать трафик через сервер, скрывая реальный IP-адрес пользователя.
3) Обфускация: Некоторые реализации Shadowsocks включают обфускацию трафика, чтобы он выглядел как обычный HTTPS-трафик.

4.3.2. VMess

VMess - протокол, разработанный для использования с V2Ray. Это более сложная и мощная система, чем Shadowsocks. Протокол предлагает больше функций для обхода цензуры.

Особенности данного алгоритма:

1) Шифрование: VMess использует шифрование как для данных, так и для заголовков, что делает его более защищенным от анализа.
2) Динамическое изменение портов: Протокол может динамически изменять порты и другие параметры для затруднения распознавания.
3) Мультиплексирование: VMess поддерживает мультиплексирование соединений, что позволяет экономить ресурсы и улучшать производительность.

4.3.3. VLESS

VLESS — новая и улучшенная версия VMess, которая была разработана с акцентом на производительность и безопасность. Протокол предлагает упрощенный подход к шифрованию и аутентификации.

Особенности данного алгоритма:

1) Безопасность: VLESS не использует шифрование заголовков, что делает его более легковесным и быстрым.
2) Поддержка различных транспортных протоколов: VLESS может работать через WebSocket, gRPC и другие транспортные протоколы, что помогает обойти блокировки.
3) Аутентификация: Использует различные методы аутентификации, включая UUID, что упрощает настройку.

5. ЗАКЛЮЧЕНИЕ

6. СПИСОК ЛИТЕРАТУРЫ