

Федеральное государственное автономное образовательное учреждение высшего
образования

**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ»**

**Эссе по защите информации
«Атаки протокольного туннелирования»**

Выполнил: Дурнов Алексей Николаевич
студент Б01-009

Долгопрудный, 2023

1 Введение

2 Классификация систем обхода блокировок

В целях содействия свободе слова и беспрепятственному обмену информацией в Интернете, ученые предлагали различные решения для обхода блокировок и борьбы с цензурой на протяжении многих лет. Попробуем классифицировать их и перечислить их преимущества и недостатки.

1. **Системы на основе прокси-серверов:** К таким системам относятся прокси-сервера, VPN, Tor и т.д. В них клиенты передают свой трафик через промежуточные прокси-сервера, которые от имени клиентов подключаются к заблокированным сайтам. Подобный подход позволяет легко разворачивать такие системы, однако их также легко детектировать по публичным IP-адресам прокси-серверов. Таким образом, противнику не составляет труда блокировать их сразу же после обнаружения.
2. **Системы ложной маршрутизации:** Достаточно перспективный подход, при котором клиент, находящийся под цензурой, должен подключаться к незаблокированным веб-сайтам. Эти запросы содержат скрытую информацию, которая позволяет специальным промежуточным маршрутизаторам (маршрутизаторам-обманкам) на пути следования перехватывать их и расшифровывать истинное цензурируемое направление, к которому клиент хочет получить доступ. Затем эти маршрутизаторы-обманки передают запросы и ответы между клиентами и заблокированными сайтами, при этом делая вид, что клиент подключен к незаблокируемому веб-сайту. Примерами таких систем являются Telex, Cirripede, Slitheen, Tapdance, Waterfall of Liberty, SiegeBreaker и др. Чтобы заблокировать такие системы, может потребоваться принятие сложных мер: изменение политики маршрутизации на уровне всей страны. Такие изменения маршрутизации на практике оказываются непомерно дорогими. Таким образом, противникам становится очень сложно их блокировать. Однако для функционирования таких систем требуется сотрудничество с провайдерами и, следовательно, они представляют собой препятствие для развертывания.
3. **Системы, основанные на мимикрии:** Такие системы пытаются замаскировать и передать цензурируемое содержимое под сообщением обычного протокола приложений. Например, SkypeMorph помогает получить доступ к заблокированным сайтам, имитируя протокол общения Skype. Однако такие протоколы очень легко блокируются, так как тяжело передать все особенности базового протокола. Кроме того, их эффективность зависит от скорости протоколов прикрытия. Для Skype выделяется низкие скорости передачи данных, что приводит к низкому уровню QoS для просмотра веб-страниц.
4. **Системы, основанные на туннелировании:** Они полагаются на инкапсуляцию скрытого трафика в сообщениях стандартных прикладных протоколов – например, электронную почту, VoIP, видеопотоки, онлайн-игры и т.д. В качестве примеров можно привести SWEET, Covertcast, Delta Shaper, Freewave, CloudTransport, Rook и др. Такие системы являются улучшением по сравнению с системами, основанные на мимикрии, поскольку они не имитируют протокольные сообщения, а непосредственно используют их в качестве скрытых каналов.

Они используют все особенности прикрывающего протокола, в то время как цензурируемое содержимое инкапсулируется в полезную нагрузку. Это очень сильно затрудняет цензору к их дифференциации от обычных (базовых) протокольных сообщений. Таким образом, может потребоваться блокировка всех базовых приложений (таких как электронная почта, облачные сервисы и т.д.), что может привести к масштабным убыткам. Однако такие системы всё также плохо обеспечивают QoS.

5. **Прочие системы:** Существуют и другие системы для борьбы с блокировками, не относящихся ни к одному из выше перечисленных типов. Domain fronting используют различные популярные облачные сервисы, например, Google app engine, для доступа к цензурируемому контенту. Запрос к прокси-серверу (скрытому за облачным сервером), скрывается в протоколе HTTPS, который направляется на доменное имя безобидного внешнего интерфейса облачного сервера. Этот модуль расшифровывает HTTPS-запрос и направляет его на прокси-сервер. Для блокирования таких сервисов противнику может потребоваться заблокировать весь фасадный сервис (например, Google app engine), тем самым тем самым блокируя другие сторонние приложения, использующие эту платформу. Разворачивать такие системы не является экономически эффективным.

3 Tor

С тех пор как в 2002 году Тор стал общедоступным и начал завоевывать популярность среди пользователей во всем мире как система для анонимного общения и обхода цензуры, многие страны пытались заблокировать подключение к нему своих граждан. Эти попытки начинались с простых методов, таких как внесение сайта Тор в черный список, чтобы пользователи не могли попасть на него и скачать клиентское ПО Тор, и со временем становились все более изощренными: активно загружался список узлов Тор (также называемых ретрансляторами) с Tor Directory Servers и вносился в черный список, устанавливались DPI-системы для поиска характеристик связи Тор (например, набор шифров рукопожатия TLS в Тор), а также активное зондирование (выдача себя за Тор-клиента и подключение к подозрительным серверам для проверки наличия у них Тор-релея). Тор сообщество не стояло на месте и разрабатывали методы обхода попыток блокировок, главным образом внедряя Tor Bridges и Pluggable Transports (PTs).

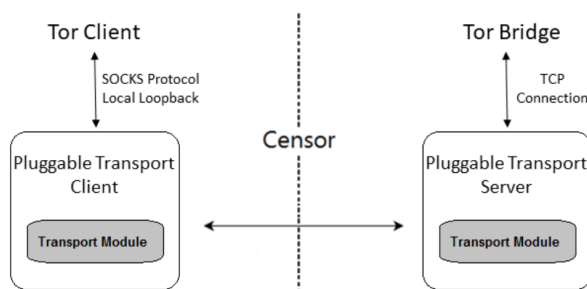


Рис. 1: Схема Pluggable Transports

PT представляют собой общую основу для разработки и развертывания технологий обхода блокировок. Их основная задача - обфусцировать соединение между клиентом Тог и мостом, служащим защитой входа в Тог, так, чтобы оно выглядело доброкачественным. PT состоит из двух частей, одна из которых устанавливается на стороне Тог-клиента, а другая - на стороне моста. PT открывает SOCKS-прокси для клиентского приложения Тог, обфусцирует или иным образом преобразует трафик, прежде чем направить его на мост. На стороне моста сервер PT выставляет обратный прокси, который принимает соединения от клиентов PT и декодирует обфускацию/трансформацию, примененную к трафику, перед передачей его реальному приложению моста. Данные, передаваемые между PT-клиентом и PT-сервером, могут быть зашифрованы, разрезаны на части общей длины или иным образом замаскированы, что делает их труднодоступными для цензора, который может обнаружить данные Тог и заблокировать их. Преобразование/обфускация данных и обратные операции выполняются транспортными модулями/протоколами обфускации, используемыми PT. По состоянию на сентябрь 2017 года, доступными и развернутыми протоколами обфускации в браузере Тог являются: obfs3, obfs4, ScrambleSuit, FTE и meek.

1. **Obfs3**: создает дополнительный уровень шифрования поверх TLS-соединения Тог, чтобы скрыть его уникальные характеристики. Для обмена ключами шифрования используется неаутентифицированный кастомизированное рукопожатие Диффи-Хеллмана. В результате этот протокол подвержен активным атакам на зондирование.
2. **ScrambleSuit**: защищает от активных зондирующих атак, используя для аутентификации внеканальный обмен секретами и номерами сеансов. ScrambleSuit также способен изменять свой сетевой отпечаток (распределение длины пакетов, время между приходами и т.д.). Этот протокол является предшественником Obfs4 и подвержен цензуре на основе белых списков.
3. **Obfs4**: имеет те же возможности, что и ScrambleSuit, но использует технику Elligator для обфускации открытых ключей и протокол ntor для односторонней аутентификации. В результате протокол работает быстрее, чем ScrambleSuit, и добавляет возможность мостовой аутентификации. Этот протокол также может быть заблокирован с помощью цензуры, основанной на белых списках.
4. **Meek**: использует технику, называемую Domain Fronting, для ретрансляции Тог-трафика на Тог-мост через сторонние серверы (т.е. CDN, такие как Amazon CloudFront и Microsoft Azure).
5. **Format-Transforming Encryption (FTE)**: преобразовывает трафик Тог в произвольные форматы стандартных протоколов, используя их языковые описания.

Эти протоколы обфускации можно разделить на две группы:

1. **Протоколы случайных потоков (obfs3, obfs4 и ScrambleSuit)**. Обмен данными в этих протоколах осуществляется в виде потоков случайных байтов, которые невозможно соотнести ни с одним известным протоколом. Эти протоколы состоят из двух фаз: фазы рукопожатия, на которой обе участвующие стороны надежно обмениваются ключами и/или номерами, и фазы коммуникации, состоящей в обмене зашифрованными сообщениями с использованием установленных ключей.

2. Структурированные потоковые протоколы (FTE и meek), которые пытаются имитировать известные протоколы из "белого списка", такие как HTTP.

Цензурирующие страны, обладающие возможностями активного зондирования, могут выявить мосты, взаимодействующие с использованием obfs3. Кроме того, протоколы случайных потоков относятся к категории "похожих на ничто", что означает, что они могут быть идентифицированы и заблокированы цензором с помощью стратегии "белого списка", поскольку их отпечаток (включая рукопожатие) не соответствует ни одному известному протоколу. С другой стороны, структурированные потоковые протоколы, имитирующие широко распространенные протоколы, устойчивы к блокированию на основе "белых списков". Однако они не защищают от активного зондирования.

4 FTE

Часть DPI систем используют явно или неявно регулярные выражения для классификации протоколов на прикладном уровне, поэтому рассмотрим механизмы, позволяющие злоумышленнику принудительно идентифицировать протокол, против любого DPI, основанного на проверке регулярных выражений. Основная идея заключается в том, чтобы встроить защиту от DPI в схемы шифрования. Добавим к обычному интерфейсу шифрования возможность принимать на вход регулярное выражение. Задача этого регулярного выражения определять формат шифротекстов: это означает, что шифротексты, взятые в виде строк соответствующего алфавита, гарантированно будут соответствовать заданному регулярному выражению. Такой криптографический примитив называется форматно-преобразующим шифрованием. Благодаря правильному выбору регулярного выражения, шифротексты, которые на самом деле несут исходный протокол, будут классифицироваться DPI как сообщения от другого протокола, по нашему выбору.

Схема FTE состоит из трех алгоритмов: генерация ключа, шифрования и дешифрования. Генерация ключа работает, как и в обычном шифровании, с выдачей случайно выбранного симметричного ключа K . Шифрование Enc принимает ключ, формат и сообщение. Оно может быть случайным, полным или детерминированным и всегда выдаёт шифротекст C или символ ошибки \perp . Расшифрование Dec принимает ключ K , формат F и шифротекст C . Его выходом является сообщение или символ ошибки \perp . Формат F задаёт множество $L(F)$, называемое языком F . Требование заключается в том, что любой шифротекст, выводимый Enc , должен быть элементом $L(F)$.

FTE является схожим с шифрованием сохраняющий формат (FPE), впервые формализованного Bellare, Ristenpart, Rogaway и Stegers (BRRS). В нём также используются форматы, но при этом требуется, чтобы и открытый текст, и шифротекст были элементами одного и того языка, определенного формата.

Хочется, чтобы FTE могло поддерживать форматы, описываемые регулярными выражениями. Это легко позволит "программировать" форматы и наделит FTE теми выразительными возможностями, что и DPI системы, основанные на регулярных выражениях.

Реализация $Enc(K, F, M)$ для регулярного выражения F :

1. Шифруем сообщение M с помощью стандартной схемы аутентифицированного шифрования, получая промежуточный шифротекст Y .

2. Рассматриваем Y как число в $\mathbb{Z}_{|L(F)|}$ (в кольце класса вычетов по модулю размера языка).

Применяем кодирующую функцию $\text{unrank}: \mathbb{Z}_{|L(F)|} \rightarrow L(F)$. Для возможности шифровки требуем, чтобы unrank была биективной функцией с эффективно вычислимой обратной функцией $\text{rank}: L(F) \rightarrow \mathbb{Z}_{|L(F)|}$. Ключевой алгоритмической проблемой является реализация функций rank и unrank эффективно. Они связывают с каждой строкой языка её ранг, т.е. позицию в общем упорядоченном языке. Goldberg и Sipser предложили эффективный способ ранжирования регулярного языка, когда этот язык представлен детерминированным конечным автоматом (DFA). BRRS использовали его для нереализованной схемы FPE для произвольных регулярных языков, закодированных как DFA, но они также подчеркивают, что, асимптотически говоря, доказательно не существует способа дать эффективные функции rank и unrank , начиная с регулярных выражений. Существуют стандартные средства для преобразования регулярного выражения в недетерминированный конечный автомат (NFA), а затем в DFA, но второй шаг приводит к экспоненциальному раздуванию размера состояния. Такое поведение в худшем случае не является проблемой для FTE, отчасти потому, что типы регулярных выражений, используемых в DPI, сами по себе явно разработаны для того, чтобы избежать раздувания в худшем случае. Предложенная реализация использует компромисс между временем и памятью, предложенный Goldberg и Sipser, для поддержки более эффективной работы во время выполнения программы путем предварительного вычисления таблиц, позволяющих (не) ранжировать все строки $x \in L$, где $|x| \leq n$. Сложность такой предварительной обработки составляет $O(n \cdot |\Sigma| \cdot |Q|)$, где Σ - базовый алфавит, а Q - множество состояний DFA, реализующего регулярное выражение FTE. С учетом этих таблиц, сложность функций rank_L и unrank_L составляет $\Omega(n)$ и $O(n|\Sigma|)$, где n - длина выхода rank_L и входа unrank_L соответственно. Подход "Encrypt-then-Unrank" сохраняет конфиденциальность сообщений и аутентичность базовой схемы аутентифицированного шифрования.

5 DNS-Morph

6 Заключение

Список литературы

- [1] Mihir Bellare, Thomas Ristenpart, Phillip Rogaway, Till Stegers. Format-Preserving Encryption.
- [2] Kevin P. Dyer, Scott E. Coull, Thomas Ristenpart, Thomas Shrimpton. Protocol Misidentification Made Easy.
- [3] Rami Ailabouni, Orr Dunkelman, Sara Bitan. DNS-Morph UDP-Based Bootstrapping Protocol For Tor.
- [4] Piyush Sharma, Devashish Gosain. Camoufler Accessing The Censored Web By Utilizing Instant Messaging.
- [5] Zhonghang Sui, Hui Shu, Fei Kang, Yuyao Huang, Guoyu Huo. A Comprehensive Review of Tunnel Detection on Multilayer Protocols.