ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Том 22
2016
№ 5

ТЕОРЕТИЧЕСКИЙ И ПРИКЛАДНОЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

Издается с ноября 1995 г.

УЧРЕДИТЕЛЬ
Издательство “Новые технологии”

СОДЕРЖАНИЕ

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

Саак А. Э. Диспетчеризация массивов заявок кругового и гиперболического типа в Grid-системах 323

Мохов А. С., Толчеев В. О. Способы учета структуры научных документов в задачах обработки и анализа текстовой информации 332

МОДЕЛИРОВАНИЕ И ОПТИМИЗАЦИЯ

Мухутдинов А. Р., Вахидова З. Р., Ефимов М. Г. Компьютерное моделирование бризантного действия взрыва 340

Инютин С. А. Метод вычисления количественной характеристики модулярной величины 343

ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ И СЕТИ

Богатырев В. А., Богатырев А. В. Модель резервированного обслуживания запросов реального времени в компьютерном кластере 348

Микова С. Ю., Оладько В. С. Сравнение алгоритмов выявления сетевых аномалий с помощью меры Ван Ризбергена 356

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

Авдошин С. М., Лазаренко А. В. Методы деанонимизации пользователей Tor . 362

БАЗЫ ДАННЫХ

Коровин А. С., Скирневский И. П. Система динамической визуализации больших массивов данных сложных физических экспериментов 373

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В БИОМЕДИЦИНСКИХ СИСТЕМАХ

Агеева У. О., Агеева В. Г., Барский А. Б. Бионическое интеллектуальное протезирование конечностей и логические нейронные сети 379

Прасолова А. Е. Коллективный нейросетевой алгоритм диагностики инфаркта миокарда 386

ПРИКЛАДНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Гриняк В. М., Иваненко Ю. С., Девятисильный А. С. Погрешность измерения координат компьютеризированными РЛС, обусловленная скоростью передачи данных в распределенных информационных системах 391

Скоробогатов Р. Ю. Расширение интерактивности компьютерной модели в телевизионной среде 396

Информация о журнале доступна по сети Internet по адресу **http://novtex.ru/IT.**
Журнал включен в систему Российского индекса научного цитирования.
Журнал входит в Перечень научных журналов, в которых по рекомендации ВАК РФ должны быть опубликованы научные результаты диссертаций на соискание ученой степени доктора и кандидата наук.

INFORMATION TECHNOLOGIES
INFORMACIONNYE TEHNOLOGII

Vol. 22
2016
No. 5

THEORETICAL AND APPLIED SCIENTIFIC AND TECHNICAL JOURNAL

Published since November 1995

ISSN 1684-6400

CONTENTS

INTELLIGENT SYSTEMS AND TECHNOLOGIES

Saak A. E. Scheduling of Sets of Hyperbolic-Type and Circular-Type Tasks in Grid-Systems 323

Mokhov A. S., Tolcheev V. O. Approaches to Considering Patterns of Scientific Documents in Processing and Analysis of Text Information 332

MODELING AND OPTIMIZATION

Mukhutdinov A. R., Vahidova Z. R., Efimov M. G. Computer Modelling of Brisant Action of Explosion 340

Inyutin S. A. Method Calculation Quantitative Characteristic Computer Modular Value 343

COMPUTING SYSTEMS AND NETWORKS

Bogatyrev V. A., Bogatyrev A. V. The Model of Redundant Service Requests Real-Time in a Computer Cluster 348

Mikova S. Yu., Oladko V. S. Comparison of Algorithms to Identify Network Anomalies Using Measures Van Rizbergena 356

CRYPTOSAFETY INFORMATION

Avdoshin S. M., Lazarenko A. V. Tor Users Deanonymization Methods 362

DATABASE

Korovin A. S., Skirnevskij I. P. Web-Application for Real-Time Big Data Visualization of Complex Physical Experiments 373

INFORMATION TECHNOLOGIES IN BIOMEDICAL SYSTEMS

Ageeva U. O., Ageeva V. G., Barskiy A. B. Bionic Intelligence Limbs Prosthetic and Logical Neural Networks 379

Prasolova A. E. Collective Newral Network Algorithm for the Diagnosis of Myocardial Infarction 386

APPLIED INFORMATION TECHNOLOGIES

Grinyak V. M., Ivanenko Yu. S., Devyatisilny A. S. Data Rate in Distributed Information System and its Effect on Digital Radar Measurement Error 391

Skorobogatov R. Yu. Introduction Virtual Characters in the Space of TV Studios . . 396

Complete Internet version of the journal at site: **http://novtex.ru/IT.**
According to the decision of the Higher Certifying Commission of the Ministry of Education of Russian Federation, the journal is inscribed in "The List of the Leading Scientific Journals and Editions wherein Main Scientific Results of Theses for Doctor's or Candidate's Degrees Should Be Published"

УДК 004.7

С. М. Авдошин, канд. техн. наук, проф., savdoshin@hse.ru,
А. В. Лазаренко, студент, avlazarenko@edu.hse.ru
Национальный исследовательский университет "Высшая школа экономики" (НИУ ВШЭ)

Методы деанонимизации пользователей Tor

Выполнен обзор методов деанонимизации пользователей Tor. Рассмотрены пассивные и активные методы деанонимизации, приведены их ключевые характеристики.

Ключевые слова: *DoS; Tor; анализ трафика; анонимная сеть; деанонимизация; тайминг-атаки*

Введение

На сегодняшний день сеть Tor [1] является самой большой в мире развернутой анонимной сетью. Ежемесячное число активных пользователей сети превышает 2 млн человек, а число волонтерских серверов, используемых в качестве узлов сети, превосходит 6 тыс. [2].

Поскольку помимо обычных пользователей преимуществами анонимизации трафика пользуются террористы, продавцы наркотиков и оружия, а также прочие нарушители закона, то деанонимизация пользователей является достаточно актуальной и важной задачей для специальных служб различных государств [3, 4]. Так, например, МВД РФ объявляло тендер на разработку способов деанонимизации пользователей сети Tor [5].

Прогресс, достигнутый в разработке методов деанонимизации, позволил американским специальным службам осуществить ряд успешных операций по борьбе с наркоторговлей. Так, например, был закрыт доступ к самому большому в теневом Интернете магазину наркотиков Silk Road [6].

Сеть Tor состоит из волонтерских серверов, являющихся ее узлами. Пользователи через луковый прокси (далее — ЛП) загружают список узлов из сервера каталогов и строят анонимные туннели (цепи), используя луковую маршрутизацию. ЛП строит цепь, как правило, состоящую из трех узлов: входного (*guard*), промежуточного (*middle*), выходного (*exit*). Время жизни цепи составляет 10 мин (по умолчанию). Входной узел обычно выбирается из фиксированного набора из трех узлов, уникального для каждого ЛП.

Более детальное описание Tor можно найти в работе [1].

Для организации атак необходимо обладать некоторыми ресурсами, например, коррумпированными узлами Tor, или серверами, доступ к которым пытается получить пользователь.

Поскольку сеть Tor является оверлейной сетью, она работает на основе транспортного слоя. Основными организациями, управляющими интернет-маршрутизацией, являются автономные системы (далее — АС). Атакующий может контролировать одну или несколько АС и предполагается, что он наблюдает трафик, проходящий через АС. Анализ влияния АС на деанонимизацию пользователей Tor можно найти в работе [7].

Как правило, атакующий преследует цель скомпрометировать как можно больше цепей, относящихся к конкретному пользователю или группе пользователей, поскольку компрометирование цепей влечет за собой деанонимизацию пользователей.

Ниже приведены термины и сокращения, использованные в работе.

Термины и сокращения

BGP (*Border Gateway Protocol*) — это основной протокол динамической маршрутизации, который используется в Интернете. Маршрутизаторы, использующие протокол BGP, обмениваются информацией о доступности сетей.

BGP Hijack (BGP-похищение) — незаконное поглощение группы IP-адресов.

BGP Interception (BGP-прослушивание) — незаконное прослушивание группы IP-адресов.

CREATE-сообщение — сообщение управляющего типа, посылается для установления новой цепи через сеть.

DESTROY-сообщение — сообщение управляющего типа, посылается для разрыва существующей цепи.

DoS (*Denial of Service*) — хакерская атака на вычислительную систему с целью довести ее до отказа, т. е. создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам) либо этот доступ затруднен.

HTTP (*HyperText Transfer Protocol*) — протокол прикладного уровня передачи данных (изначально в виде гипертекстовых документов в формате HTML, в настоящий момент используется для передачи произвольных данных).

ID — уникальный идентификатор.

Iframe — html-контейнер, содержание которого игнорируется браузерами, не поддерживающими данный тег.

IP-адрес (*Internet Protocol Address*) — уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP.

ISP (*Internet Service Provider*) — организация, предоставляющая пользователям доступ к сети Интернет и связанные с этим услуги.

JavaScript — прототипно-ориентированный сценарный язык программирования.

RAPTOR (*Routing Attacks on Privacy in Tor*) — маршрутизационные атаки на приватность в Tor.

RELAY DATA-сообщение — сообщение управляющего типа, посылается для выполнения команды к ретранслированию данных.

Sybil-атака — атака на безопасность компьютерной системы, где репутационная система подрывается с помощью нелегитимных сущностей в пиринговых сетях.

Tagging attack — атака на приватность в сети Tor, при которой помечается какая-то ячейка и затем происходит ее поиск на другом конце соединения.

TCP (*Transmission Control Protocol*) — протокол управления передачей — один из основных протоколов передачи данных Интернета, предназначенный для управления передачей данных в сетях и подсетях TCP/IP.

Timing-атака — атака по сторонним каналам, в которой атакующий пытается скомпрометировать систему с помощью анализа времени, затрачиваемого на исполнение операций.

Tor (*The Onion Router*) — анонимная сеть и открытое программное обеспечение, позволяющее сохранять пользователям свою анонимность.

WF (*Website Fingerprinting*) — класс пассивных атак, позволяющий определить посещенный пользователем портал или скрытую службу.

Автономная система (АС) — это система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с Интернетом.

Конвейерная обработка HTTP — технология, которая позволяет передавать на сервер сразу несколько запросов в одном соединении, не ожидая соответствующих ответов.

Коррумпированная автономная система — автономная система, контролируемая наблюдателем.

Коррумпированный сервер — конечная точка назначения, контролируемая наблюдателем.

Коррумпированный узел — узел, трафик которого может модифицировать и просматривать атакующий.

ЛП — луковый прокси.

Метаданные сети — субканальная информация об используемых данных.

Микс Чаума — устройство для передачи и хранения, принимающее какое-то число сообщений фиксированной длины от нескольких источников, совершающее криптографическую трансформацию сообщений и затем передающее сообщение к следующему пункту назначения в случайном порядке.

Скрытая служба — портал/сайт, доступный только внутри сети Tor.

УМПС — узел с минимальной пропускной способностью.

ЦП — целевой поток.

1. Пассивные методы

Пассивные методы лежат в основе атак, при которых атакующий отслеживает сообщения внутри системы, не делая попыток изменения данных или вторжения в процесс взаимодействия.

1.1. Атаки анализа трафика

Анализ трафика — это извлечение информации из метаданных сети, включая объем и временные характеристики сетевых пакетов. Наблюдатель использует эти данные для выявления связи между инициатором сообщения и конечной точкой назначения. Ввиду того что внутренние механизмы Tor скрывают битовые шаблоны данных, передающихся через цепь, атакующий не может использовать информацию, содержащуюся в сообщении.

Традиционные атаки анализа трафика делятся на два класса.

В первом классе атак анонимная сеть представляется в виде черного ящика и рассматриваются временные связи между инициацией пользователем соединения и соединениями, установленными вне сети. Данный класс атак подробно не рассматривается в настоящей статье, поскольку он неприменим к глобальной сети ввиду ее размеров и огромного количества ресурсов, необходимых для проведения атаки. В работе [8] представлено подробное описание атак этого класса. Статистический вариант атак представлен в работе [9], в работе [10] подтвержден экспериментально. Такие атаки эффективны, если атакующий обозревает большую часть сети и есть возможность регистрировать пользова-

телей, заходящих в сеть и на внешние сервисы. Временной анализ атак рассмотрен в работах [10, 11].

Второй класс атак рассматривает трафик и нагрузку на каждом узле только внутри анонимной сети. В работе [12] представлено детальное описание данных атак. В действительности атакующий просматривает поток данных на каждом узле, например ответ сервера инициатору запроса. Поток в узле представляется в виде зависимости объема трафика от времени, затем проводится сглаживание этой функции за счет свертки ее с экспоненциально-убывающей функцией в целях получения шаблона, предсказывающего вид трафика в анонимной сети. Далее все фрагменты трафика в сети, преобразованные таким же образом, сравниваются с шаблоном. Степень сходства с шаблонами позволяет определить его принадлежность к конкретному узлу в цепочке соединения. Похожие атаки представлены в работах [13, 14].

Очевидная проблема таких атак заключается в том, что атакующий должен просматривать все узлы в сети и иметь возможность регистрировать метаданные трафика. В результате данные атаки используют модель пассивного глобального наблюдателя, который не рассматривается в модели угроз Tor. Заметим, что если наблюдатель обозревает не всю сеть, а какую-то ее часть, то он имеет возможность отследить случайные соединения. Исследование эффективности атак анализа трафика в зависимости от реальных моделей атакующего представлены в работе [15].

Малозатратная атака анализа трафика сети Tor [16] базируется на следующем наблюдении: высокая нагрузка на один из узлов в цепи влияет на задержку всех остальных узлов. Путем перенаправления соединения через специфические узлы и замера возникающих задержек наблюдатель может получить примерную нагрузку на узел. Эту нагрузку можно сравнить с известным шаблоном трафика с помощью традиционных техник анализа трафика [12].

Любой пользователь Tor может провести такие измерения и определить нагрузку на узел. Предполагается, что атакующий контролирует коррумпированный узел. Этот узел инициирует соединение, проходящее через другие узлы, нагрузка на которых должна быть измерена. Затем коррумпированный узел наполняет соединение пробным трафиком, который позволяет измерить задержки и вычислить нагрузку на узел, являющийся целью атакующего.

Просматривая соединение пользователя с сетью Tor или соединение сети Tor с конечной точкой назначения, наблюдатель может использовать эту технику для определения узлов, через которые ретранслировалось соединение. Существует более мощный вариант данной атаки: наблюдатель контролирует сервер, к которому подключается отслеживаемый пользователь. Сервер посылает пользователю через Tor данные, имеющие специфический шаблон трафика, что позволяет идентифицировать узлы пользователя.

Малозатратная атака на основе маршрутизации [17] предполагает, что анонимность может быть скомпрометирована с помощью локального набора коррумпированных узлов. Предполагается, что коррумпированные узлы этого набора имеют высокую пропускную способность.

Для применения атаки наблюдатель должен контролировать набор, состоящий из более чем одного узла из списка активных узлов Tor.

На первом шаге необходимо внедрить коррумпированные узлы в качестве входных и выходных узлов в цепи пользователя. Существенное сокращение необходимых ресурсов происходит за счет использования узлов с низкой пропускной способностью. Данное улучшение основывается на том, что узел может предоставить недостоверные данные о своих ресурсах службе каталогов, представляясь мощным узлом для всей системы. Однако вычислительных ресурсов узла должно хватать для установки новых соединений. Таким образом, все ресурсы узла направляются на прием новых соединений от ЛП.

Если коррумпированные узлы находятся в промежуточных позициях (между входным и выходным узлами), они могут разорвать цепь, поскольку такая конфигурация несовместима с атакой. Это вызовет перестройку цепи, и, возможно, после этого установится конфигурация, при которой коррумпированные узлы станут концевыми.

Наличие коррумпированных входного и выходного узлов является обязательным условием для успешного применения атаки, поскольку иная конфигурация не позволит проводить корреляцию трафика.

Если цепь полностью состоит из коррумпированных узлов, то компрометирование анонимности является тривиальной задачей. В наиболее вероятном варианте компрометированные узлы будут только входными и выходными для данного пользователя. Данный тип атаки позволяет компрометировать цепь до того, как пользователь начинает пересылать данные.

Для того чтобы собрать достаточно информации для корреляции клиентских запросов с ответами сервера через Tor, каждый коррумпированный узел регистрирует следующую информацию для каждой ячейки с данными: ее позицию в цепи (на входном, выходном узлах или в середине); местное время; ID прошлой цепи; прошлый IP-адрес; прошлый порт соединения; IP-адрес следующего промежуточного соединения; порт следующего промежуточного соединения; ID цепи следующего промежуточного соединения. Как только эти данные будут собраны, атакующий может связать пути,

в которых содержатся выходной и входной коррумпированные узлы, с ЛП, от которых идут запросы построения цепей. Обладая этой информацией, атакующий может связать адресанта с адресатом, компрометируя анонимность системы.

Для использования атаки данного типа коррумпированные узлы должны быть координированы. Самый простой способ координации — использовать централизованный сервер для сбора логов с узлов, что позволит наблюдателю выполнить алгоритм компрометирования цепи в реальном времени.

Алгоритм компрометирования цепи работает следующим образом: коррумпированный узел подтверждает, что запрос на создание цепи был отправлен ЛП, а не узлом. Затем проверяются хронологический порядок шагов создания цепи и совпадение промежуточного соединения для входного узла с промежуточным соединением выходного. После этого проверяется, получено ли для ответа от выходного узла сообщение, посланное от входного узла выходному. Если все проверки выполнены успешно, то цепь компрометирована.

В работе [17] приведены результаты экспериментов, которые проводили с использованием закрытой развернутой сети Tor. Она состояла из 60 легитимных и шести коррумпированных узлов. Атака успешно скомпрометировала 46 % цепей.

Атаки на основе пропускной способности канала [18] являются незаметными как для пользователя, так и для узла. Пропускная способность канала Tor может быть использована в качестве следа для обнаружения узла с минимальной пропускной способностью (УМПС). Через подробное рассмотрение динамики пропускной способности канала можно выявить, что два потока используют один и тот же набор узлов, это позволяет атакующему связать потоки с цепями и скомпрометировать приватность пользователя.

Фундаментальное наблюдение, используемое в атаке, — разнородность пропускных способностей узлов Tor [18]. Существуют три ключевых фактора, определяющих пропускную способность цепи: а) пропускная способность УМПС; б) число активных TCP-потоков между УМПС и следующим узлом; в) число других активных цепей, размноженных через TCP-соединение. То есть основная идея атаки — корреляционный анализ пропускных способностей цепей.

Первый вариант атаки позволяет определить, что две цепи используют общий набор узлов. На основе мониторинга пропускных способностей узлов проводится простой статистический тест для выявления корреляции между ними. Существуют три возможных варианта.

- Обе цепи используют одинаковый набор узлов. При таком варианте коэффициент корреляции пропускных способностей цепей будет высок. Это объясняется тем, что любые вариации потоков или пропускных способностей узлов будут влиять на пропускную способность цепей одинаково.
- Обе цепи не имеют общих узлов. В этом случае степень корреляции будет близка к нулю.
- Обе цепи имеют как минимум один общий узел. Если общий узел является УМПС в обеих цепях, тогда пропускные способности цепей будут иметь высокий коэффициент корреляции. Иначе изменения потоков или пропускных способностей узлов при пересылке данных не будут влиять на пропускную способность обеих цепей и их пропускные способности будут зависеть от их УМПС.

Второй вариант атаки — идентификация одного или нескольких узлов в качестве участника какого-либо целевого потока (ЦП) [18]. Этот поток может быть любым потоком, инициированным ЛП через сеть. Предполагается, что атакующий может сформировать пробный поток, просматривать трафик ЦП и имеет коррумпированный выходной узел. Кроме этого, у наблюдателя должен быть либо вебсервер, к которому пользователь пытается получить доступ, либо ISP, ретранслирующий данные. Атакующему не нужно модифицировать трафик. Он строит цепь с одним узлом, через эти узлы вычисляет корреляцию между ЦП и пробным потоком. Если пропускная способность имеет высокий коэффициент корреляции с пропускной способностью ЦП, тогда сервер может допустить, что оба потока проходят через общий узел.

Website fingerprinting (WF) — класс атак, получивший большую популярность среди исследователей [19—21]. Он демонстрирует, что наблюдатель, способный просматривать зашифрованный трафик какой-то части сети, имеет возможность, при некоторых условиях, скомпрометировать портал, посещенный пользователем в сети.

Атакующий должен иметь доступ к входному узлу пользователя, чтобы просматривать его трафик и видеть IP-адрес пользователя.

Стратегия атакующего следующая: он пытается смоделировать сетевые условия пользователей путем создания собственного ЛП, посещающего те порталы, связь пользователя с которыми необходимо подтвердить. Затем обучается классификатор с учителем и использованием большого количества сетевых свойств портала (цепочки пакетов, их размер и временные интервалы между ними). Используя построенную модель, атакующий классифицирует трафик пользователей в сети.

Атака начинается со сбора данных. В сети Tor есть несколько факторов, значительно усложняющих качество собранных данных: процесс конструирования цепей; пропускная способность; загруженность. Например, образцы трафика, собранные через одну цепь, могут отличаться от образцов, собранных через другую цепь. Контент порталов может со

временем меняться, что сильно влияет на образцы трафика.

WF-атаку можно представить в виде задачи классификации [19]. Каждый класс может быть группой сайтов, например "Специфический сайт", "Остальные сайты". Таким образом, после сбора данных нужно обучить классификатор. После тренировки на полученных образцах классификатор сможет идентифицировать неизвестные образцы.

Наиболее продвинутая модификация WF-атаки на Tor позволяет деанонимизировать пользователя с 95 %-ной вероятностью в закрытой сети Tor, и с 91 %-ной вероятностью в сети, открытой для узкой группы сайтов.

В ответ на успешную попытку применения WF-атаки [22] разработчики Tor сделали экспериментальную защиту [23]. Защита содержит три компонента: конвейерная обработка HTTP, размер конвейера и порядок запросов, задаваемые случайно. В работе [19] показали, что защита неэффективна. Более подробную техническую информацию о WF можно найти в работе [24].

1.2. Timing-атаки

Timing-атаки являются одними из самых ранних методов деанонимизации. Их наблюдали в самых старых анонимных сетях, включая ранние версии луковой маршрутизации [25]. Данные атаки очень похожи на атаки анализа трафика в сетях, основанных на миксах Чаума [26].

Классическая Timing-атака [27] использует метод, при котором атакующий наблюдает временные шаблоны в сетевом потоке и затем проводит корреляцию выявленных шаблонов с другими, найденными в трафике. Если атакующий имеет возможность наблюдать как пользовательский трафик, так и трафик в конечной точке соединения, то он может установить связь между ними.

Идея основывается на том, что в Tor задержка не может быть большой, т. е. временной шаблон пакетов данных должен сохраняться при продвижении через цепочку соединения.

Для применения данной атаки атакующему необходимо иметь коррумпированный узел.

Модель атаки следующая.

1. Коррумпированный узел устанавливает соединение с другими узлами Tor, чтобы измерить задержки соединений.

2. Коррумпированный узел продолжает проводить мониторинг задержек всех установленных соединений на протяжении определенного временного промежутка.

3. Значения задержек используют для расчета транспортной нагрузки тех узлов Tor, с которыми установил соединение злокачественный узел.

4. Вычисляют шаблоны трафика, зависящие от транспортной нагрузки.

5. Когда атакующий получит шаблоны трафика всех узлов, он может воспроизвести атаку по сценарию атаки анализа трафика.

Для того чтобы сделать атаку более эффективной, необходимо сделать коррумпированный сервер, к которому будет подключаться пользователь. Благодаря этому нет необходимости просматривать соединение для извлечения шаблона трафика. Наблюдатель может выбрать шаблон трафика, который легко обнаруживается и посылает свои потоки через коррумпированный сервер. Цель такого улучшения — найти цепь между узлом пользователя и коррумпированным сервером. С таким улучшением анонимность системы падает до уровня простого прокси.

1.3. Circuit fingerprinting-атака [28]

Данная атака является одной из самых современных комбинированных атак.

Атака спроектирована для компрометирования приватности пользователя, контактирующего со скрытыми службами Tor, что позволяет с высокой степенью точности определить взаимосвязь пользователя со скрытой службой. Как только активность пользователя и скрытой службы идентифицирована, используется WF-атака. Предполагается, что атакующий наблюдает трафик между пользователем и сетью Tor.

Трафик, участвующий во взаимодействии со скрытой службой, оставляет четкий след, поэтому легко выявить соответствующий шаблон трафика.

Первый шаг атакующего — найти цепи, участвующие во взаимодействии со скрытой службой. Для классификации таких цепей используют следующие характеристики: длительность активности; число входящих и исходящих сообщений; последовательность первых 10 сообщений. При этом для классификации цепочки используется дерево решения.

Определив цепочку, атакующий должен получить доступ к входному узлу пользователя, которого он пытается деанонимизировать. Для того чтобы понять, пытается ли пользователь получить доступ к анонимной скрытой службе или к обычному порталу, используется классификатор. Второй классификатор используется, чтобы определить, какую скрытую службу пользователь посетил.

Результаты эксперимента, представленные в работе [28], показали, что данный метод позволяет выявить связь пользователя со скрытым сервисом в 98 % случаев при первой атаке, в 99 % случаев при второй атаке. Кроме того, в 88 % случаев корректно определяется, какую из 50 страниц, за которыми ведется наблюдение, пользователь посетил.

2. Активные методы

Активные методы лежат в основе атак, во время которых атакующий пытается изменить данные или каким-либо другим образом вторгнуться в процессы системы.

2.1. Timing-атака

Timing-атака с использованием браузера [29] позволяет наблюдателю выявить часть пользователей Tor, использующих коррумпированный узел и оставивших открытым окно браузера не менее чем на час. Для реализации атаки необходим коррумпированный сервер, входной и выходной коррумпированные узлы.

Выходной узел модифицирует HTTP-трафик, проходящий через него, вставляя невидимый контейнер *iframe*, содержащий JavaScript-код, в запрашиваемые веб-странички. JavaScript-код итеративно контактирует с сервером, посылая уникальный идентификатор, и продолжает работать до тех пор, пока человек оставляет открытой вкладку с зараженной страничкой в браузере. Полная атака работает следующим образом.

1. Атакующий разворачивает необходимые ресурсы: а) вставляет два коррумпированных узла в сеть Tor (входной и выходной); б) разворачивает веб-сервер, который получает и записывает данные, посылаемые JavaScript-кодом.

2. Коррумпированный выходной узел модифицирует весь HTTP-трафик, вставляя туда невидимый JavaScript-код — генератор сигнала, который генерирует уникальный сигнал для каждого клиента Tor.

3. Веб-браузер клиента запускает JavaScript-код, посылая сигнал на сервер.

Этот трафик поступает через клиента Tor, но клиент все еще остается анонимным.

4. Каждые 10 мин ЛП строит новую цепь. ЛП выбирает коррумпированный входной узел (случайно).

5. Атакующий проводит анализ трафика для того, чтобы сравнить сигналы на каждой цепи, поступающие через его входной узел, с разными сигналами, которые принимает веб-сервер. Совпадение сопоставляет клиент Tor с его историей трафика, записанной во время использования коррумпированного выходного узла.

Входному узлу нужно только регистрировать проходящий шаблон трафика на каждой цепи, выходной узел нужен только для вставок JavaScript-кода. Существует модификация атаки, использующая только HTML, описание можно найти в работе [29].

Timing-атаки с использованием BGP на уровне АС [30] бывают двух типов.

Анализ трафика через BGP-похищение. Для деанонимизации пользователя наблюдатель может, в первую очередь, применить известные атаки для компрометирования входного узла [18]. Далее наблюдатель может начать атаку префиксного перехвата против префикса, соответствующего найденному входному узлу. Атака позволяет коррумпированной АС увидеть трафик, предназначающийся входному узлу, за счет поглощения всего трафика входного узла. Поэтому соединение будет активным только какое-то время, а потом оно будет сброшено. Коррумпированная АС может узнать набор клиентов, ассоциированных с входным узлом для продолжительности времени соединения, через инспекцию IP-заголовков.

Анализ трафика через BGP-прослушивание. Для того чтобы совершить точную деанонимизацию пользователя через анализ трафика, коррумпированная АС может запустить атаку BGP-подслушивания [31]. Эта атака позволяет АС стать промежуточной на пути по направлению к входному узлу, т. е. после перехвата трафик возвращается обратно к нужной точке назначения. Атака позволяет сохранить соединения, оставляя возможность АС точно деанонимизировать клиента через тайминг-анализ.

2.2. Атаки анализа трафика

Атака с пометкой ячеек (подтверждающая атака) [32] заключается в том, что атакующий имеет контроль над входным и выходным узлами пользователя. Атака начинается с коррумпированного входного узла. Входной узел выбирает сообщение в TCP-потоке данных и дублирует это сообщение. Исходный IP-адрес сообщения и момент времени дублирования регистрируются. Дублированное сообщение проходит весь путь через цепь и прибывает в выходной узел. Атакующий, управляя выходным узлом, должен засечь дублированное сообщение и записать время, IP-адрес назначения сообщения и порт. Тем самым он подтверждает, что ячейка использует коррумпированные узлы. Таким образом, атакующий устанавливает входные и выходные узлы.

В оригинальной статье про Tor [1] такой класс атак называют *"tagging attack"* (помечающие атаки). Суть в том, что помечается какое-то сообщение, которое потом ищется в потоке данных.

RAPTOR-атака [33] является совершенно новой техникой деанонимизации пользователя с помощью анализа трафика. В качестве наблюдателя здесь используется АС. RAPTOR-атака использует динамические аспекты протокола BGP.

Атака состоит из трех компонент, совместное применение которых дает синергетический эффект. RAPTOR использует асимметричную природу маршрутизации Интернета (BGP-путь от посылающего к приемнику может отличаться от BGP-пути от приемника к посылающему). Эта асимметрия повышает шансы атакующего, обладающего коррумпированной АС, просмотреть хотя бы одно из направлений.

Первый компонент — асимметричный анализ трафика. Данная форма является новой формой ана-

лиза трафика, позволяющей коррумпированной АС деанонимизировать пользователей. Традиционный анализ трафика рассматривает только один сценарий: наблюдатели обозревают трафик от клиента к входному узлу и от выходного узла к веб-серверу. Как правило, пути через Интернет асимметричны, так что путь от выходного узла к веб-серверу может отличаться от пути от веб-сервера к выходному узлу. Возможен и такой вариант: наблюдатель не имеет возможности просматривать трафик на пути от выходного узла к серверу, но может просматривать трафик TCP-подтверждения доставки на пути от сервера к выходному узлу.

Асимметричный анализ трафика позволяет наблюдателю деанонимизировать пользователей до тех пор, пока наблюдатель может просматривать любое направление трафика на обоих концах соединения. Анализ работает для четырех сценариев: а) трафик данных от клиента к входному узлу и трафик от выходного узла к серверу; б) трафик данных от клиента к входному узлу, трафик TCP-подтверждения доставки от сервера к выходному узлу; в) трафик TCP-подтверждения доставки от входного узла к клиенту и трафик данных от выходного узла к серверу; г) трафик TCP-подтверждения доставки от входного узла к клиенту, трафик TCP-подтверждения доставки от сервера к выходному узлу. При анализе исследуются поля TCP-заголовков в наблюдаемом трафике для выявления номера TCP-последовательности и номер TCP-подтверждения доставки. Далее вычисляется корреляция между этими полями.

Второй компонент — анализ натуральных перебоев. Путь между клиентом и входным узлом изменяется во времени вследствие физической топологии и политик АС. Такие изменения увеличивают со временем вероятность попадания пользовательских цепей в коррумпированные АС.

Третий компонент — атаки BGP-похищения и BGP-прослушивания. Подробно данные атаки были описаны в работе [31]. Атака BGP-прослушивания позволяет коррумпированной АС стать на пути перед входным узлом, т. е. после перехвата трафик будет возвращаться обратно через входной узел. Такой перехват сохранит соединение и позволит АС провести асимметричный анализ трафика. Кроме того, такая атака позволяет коррумпированной АС деанонимизировать пользователя, посещающего какой-то конкретный сайт. АС видит трафик на клиенте и может запустить атаку BGP-прослушивания против выходного узла.

Результаты экспериментов, приведенные в работе [33] показывают, что атака успешна в 90 % случаев.

2.3. DoS-атаки

Обычные DoS-атаки не требуют глубокого знания Tor и могут быть осуществлены с использованием простых, известных техник [34]. Кроме того, детальный анализ обычных DoS-атак на Tor можно найти в работе [35]. В 2014 г. вышла работа [36], посвященная атаке, позволяющей израсходовать всю доступную память узла, однако вследствие кооперации авторов с разработчиками Tor атака более не работоспособна, поэтому в настоящей статье не рассматривается.

Атака packet spinning [37] заставляет пользователя выбирать коррумпированные узлы через вывод из строя легитимных узлов. Атакующий строит циклические цепи через сеть Tor и посылает большой объем данных через этот путь, чтобы легитимные узлы были максимально загружены. Атакующий запускает другой набор коррумпированных узлов, которые когда-нибудь будут выбраны пользователями, потому что атакующий перегрузил все легитимные. Атака будет успешной, если инициатор выбирает только коррумпированные узлы для своих цепей, в результате чего деанонимизация становится тривиальной.

Атака перегрузки с использованием длинных путей [38] основана на следующих свойствах Tor: а) маршрутизаторы Tor не вставляют искусственные задержки между запросами; б) IP-адреса всех узлов Tor публично известны и доступны.

Атака предполагает, что атакующий контролирует выходной узел. Узел используется для вставки JavaScript-кода в HTML-ответ на запрос. Код заставляет браузер посылать HTTP-запросы каждую секунду и в ответ на каждый запрос выходной узел посылает пустой ответ, который отвергается браузером. Атакующий записывает интервалы времени периодических запросов, производимых браузером. Так как запросы маленькие, возникает задержка, равная примерно разнице во времени доставки сигнала кодом.

У владельца коррумпированного выходного узла теперь стоит задача вызвать перегрузку узлов, подозреваемых в участии в цепи. Предполагаем, что все узлы являются подозреваемыми, и в самом простом случае атакующий будет итеративно через все узлы проверять, является ли данный узел входным узлом цепи.

Для каждого узла X атакующий конструирует длинную цепь, которая с повторениями включает X в цепь. Вследствие того что Tor сбрасывает цепь при попытке расширения цепи через предыдущий узел, нужно использовать два или более промежуточных узлов для замыкания цепи на X.

Как только цепь становится достаточно длинной (авторы статьи [38] предлагают 24 узла), атакующий использует цепь для передачи данных. Цепь длины m позволит атакующему с пропускной способностью p уменьшить пропускную способность сети Tor на значение $m \cdot p$. Узлу X придется участвовать в $m/3$ дополнительных цепях, что позволит атакующему встраивать большие задержки в конкретный узел.

Если узел X не относится к компрометирующей цепи, измеримые задержки не вызовут заметных изменений во время выполнения атаки. Если X — входной узел, атакующий будет просматривать внедренный шаблон задержки и выявит искомую цель.

CellFlood DoS-атака [39] вместо создания большого числа запросов, на обработку которых требуется мало вычислительных ресурсов, как в обычной DoS-атаке, использует несколько тяжелых запросов создания цепи, которые быстро генерируются атакующим с минимальным количеством ресурсов, однако будут требовать большое количество вычислительных ресурсов от узла, на который идет атака.

Обработка CREATE сообщения занимает в 4 раза больше времени, чем его генерация [40], вследствие криптографических операций, основанных на паре открытый-закрытый ключ, совершаемых во время расширения цепи. Это может быть использовано для всех доступных ресурсов атакуемого узла.

Благодаря архитектуре Tor, узел, на который приходит огромное число CREATE-сообщений, не теряет возможности пересылать сообщения типа RELAY_DATA. Узел, получающий CREATE-сообщения быстрее, чем его процессор может обработать, отвечает на них, посылая DESTROY-сообщения в ответ. Следовательно, узел, находящийся под атакой, будет отклонять запросы от легитимных узлов. Если атака выполняется стратегически, возможна перегрузка большой части сети и выявление цепи, проходящей через конкретные узлы.

Если атакующий заинтересован в том, чтобы исключить узел или набор узлов из сети Tor, ему выгоднее использовать поток CREATE-сообщений, чем обычную и более дорогую DoS-атаку.

Описание некоторых методов не вошло в настоящую работу ввиду большой степени схожести с уже рассмотренными. Другие методы в рамках тематики Tor описывать не имеет особого смысла. К числу таких атак относятся Sybil-атаки [41], которые возможны при внедрении в Tor большого числа коррумпированных узлов, составляющих ощутимую долю узлов Tor. В работе [42] описана комбинированная атака, основанная на анализе трафика, использующаяся совместно с Sybil-атакой. В работах [42, 43] можно найти атаки на основе анализа трафика с использованием исторических данных о TCP. Ресурс [44] содержит исчерпывающую библиографическую подборку по атакам и защите анонимных систем.

Заключение

В работе были рассмотрены методы, позволяющие успешно провести деанонимизацию пользователей сети Tor. Из рассмотрения методов можно сделать однозначный вывод: атакующему, имеющему большой запас ресурсов, например государственным службам, частным корпорациям и т. д., не составит большого труда деанонимизировать большое число пользователей сети Tor. Различные комбинации рассмотренных атак можно применить и к деанонимизации пользователей анонимных сетей другого типа, описанных, например, в работе [45].

Список литературы

1. **Dingledine R., Mathewson N., Syyerson P.** Tor: The Second-Generation Onion Router [Electronic resource] // Tor project [Official website]. URL: https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf (accessed: 8.09.2015).
2. **TorMetrics** [Electronic resource] // Tor project [Official website]. URL: https://metrics.torproject.org (accessed: 28.09.2015).
3. **The Russian** government hired people to hack the Tor browser, but they failed and now they're quitting [Electronic resource] // Meduza [Official website]. URL: https://ineduza.io/en/news/2015/09/09/the-russian-government-hired-people-hack-the-tor-browser-but-they-failed-and-now-they-re-quitting (accessed: 28.09.2015).
4. **The NSA's** Been Trying to Hack into Tor's Anonymous Internet For Years [Electronic resource] // Gizmodo [Official website]. URL: http://gizmodo.com/the-nsas-been-trying-to-hack-into-tors-anonymous-inte-1441153819 (accessed: 28.09.2015).
5. **Закупка** № 0373100088714000008 [Электронный ресурс] // Государственные закупки [Официальный сайт]. URL: http://zakupki.gov.ru/epz/order/notice/zkk44/view/comrnon-intb.html?regNumber=0373100088714000008 (дата обращения: 2.10.2015).
6. **The Rise** & Fall of Silk Road [Electronic resource] // Wired [Official website]. URL: http://www.wired.com/2015/04/silk-road-1/ (accessed: 28.09.2015).
7. **Danezis G.** Statistical disclosure attacks [Electronic resource] // Freehaven [Official website]. URL: http://freehaven.net/anonbib/cache/statistical-disclosure.pdf (accessed: 1.10.2015).
8. **Kedogan D., Agrawal D., Penz S.** Limits Of Anonymity in Open Environment [Electronic resource] // Springer Link [Official website]. URL: http://link.springer.com/chapter/10.1007 %2F3-540-36415-3_4 (accessed: 1.10.2015).
9. **Danezis G.** Statistical disclosure attacks [Electronic resource] // Freehaven [Official website]. URL: http://freehaven.net/anonbib/cache/statistical-disclosure.pdf (accessed: 1.10.2015).
10. **Mathewson N., Dingledine R.** Practical traffic analysis: Extending and resisting statistical disclosure [Electronic resource] // Freehaven [Official website]. URL: http://freehaven.net/doc/e2e-traffic/e2e-traffic.pdf (accessed: 1.10.2015).
11. **Agrawal D., Kesdogan D., Penz S.** Probabilistic Treatment of Mixes to Hamper Traffic Analysis [Electronic resource] // Freehaven [Official website]. URL: http://freehaven.net/anonbib/cache/agrawal03.pdf (accessed: 1.10.2015).
12. **Danezis G.** The Traffic Analysis of Continuous-Time Mixes [Electronic resource] // Freehaven [Official website]. URL: http://freehaven.net/anonbib/cache/danezis:pet2004.pdf (accessed: 1.10.2015).
13. **Zhu Y., Fu X., Graham B., Bettati R., Zhao W.** On flow correlation attacks and countermeasures in mix networks [Electronic resource] // Freehaven [Official website]. URL: http://freehaven.net/anonbib/cache/flow-correlation04.pdf (accessed: 1.10.2015).
14. **Levine B. N., Reiter M. K., Wang C., Wright M. K.** Timing attacks in low-latency mix-based systems [Electronic resource] // Freehaven [Official website]. URL: http://freehaven.net/anonbib/cache/flow-correlation04.pdf (accessed: 1.10.2015).
15. **Johnson A., Wacek C., Jansen R., Sherr M., Syverson P.** Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries [Electronic resource] // Aaron Michael Johnson [Official website]. URL: http://www.ohmygodel.com/publications/usersrouted-ccs13.pdf (accessed: 2.10.2015).
16. **Murdoch S. J., Danezis G.** Low-Cost Traffic Analysis of Tor [Electronic resource] // UCL-CS [Official website]. URL: http://sec.cs.ucl.ac.uk/users/smurdoch/papers/oakland05torta.pdf (accessed: 1.10.2015).

17. **Bauer K., McCoy D., Grunwald D., Kohno T., Sicker D.** Low-Resource Routing Attacks Against Tor [Electronic resource] // University of Washington [Official website]. URL: https://homes.cs.washington.edu/~yoshi/papers/Tor/wpes25-bauer.pdf (accessed: 1.10.2015).

18. **Mittal P., Khurshid A., Juen J., Caesar M., Borisov M.** Stealthy Traffic Analysis of Low-Latency Anonymous Communication Using Throughput Fingerprinting [Electronic resource] // Princeton University [Official website]. URL: http://www.princeton.edu/~pmittal/publications/throughput-fingerprinting-ccs11.pdf (accessed: 1.10.2015).

19. **Cai X., Zhang X., Joshi B., Johnson R.** Touching from a Distance: Website Fingerprinting Attacks and Defenses [Electronic resource] // Stony Brook University [Official website]. URL: http://www3.cs.stonybrook.edu/~xcai/fp.pdf (accessed: 1.10.2015).

20. **Wang T., Cai X., Nithyanand R., Johnson R., Goldberg I.** Effective Attacks and Provable Defenses for Website Fingerprinting [Electronic resource] // Centre for Applied Cryptographic Research The University of Waterloo [Official website]. URL: http://cacr.uwaterloo.ca/techreports/2014/cacr2014-05.pdf (accessed: 1.10.2015).

21. **Cai X., Nithyanand R., Wang T., Johnson R., Goldberg I.** A Systematic Approach to Developing and Evaluating Website Fingerprinting Defences [Electronic resource] // Freehaven [Official website]. URL: http://freehaven.net/anonbib/cache/ccs2014-fingerprinting.pdf (accessed: 1.10.2015).

22. **Panchenko A., Niessen L., Zinnen A., Engel A.** Website fingerprinting in onion routing based anonymization networks [Electronic resource] // Freehaven [Official website]. URL: http://freehaven.net/anonbib/cache/wpes11-panchenko.pdf (accessed: 1.10.2015).

23. **Experimental** Defense for Website Traffic Fingerprinting [Electronic resource] // Tor project [Official website]. URL: https://blog.torproject.org/blog/experimental-defense-website-traffic-fingerprinting (accessed: 1.10.2015).

24. **Wang T., Goldberg I.** Improved Website Fingerprinting on Tor [Electronic resource] // Freehaven [Official website]. URL: http://freehaven.net/anonbib/cache/wpesl3-fingerprinting.pdf (accessed: 1.10.2015).

25. **Goldschlag D., Reed M., Syverson P.** Onion Routing for Anonymous and Private Internet Connections. January 28, 1999 [Electronic resource] // Onion Routing [Official website]. URL: http://www.onion-router.net/Publications/CACM-1999.pdf (accessed: 8.09.2015).

26. **Chaum D.** Untraceable Electronic Mail, Return Addressed, and Pigital Pseudonyms [Electronic resource] // Free Haven [Official website]. URL: http://www.freehaven.net/anonbib/cache/chaum-mix.pdf (accessed: 28.09.2015).

27. **Wiangsripanawan R., Susilo W., Safavi-Naini R.** Pesign principles for low latency anonymous network systems secure against timing attacks [Electronic resource] // ACM Pigital Library [Official website]. URL: http://dl.acm.org/citation.cfm?icH1274553 (accessed: 28.09.2015)

28. **Kwon A., AlSabah M., Lazar D., Dacler M., Devadas S.** Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services [Electronic resource] // USENIX [Official website]. URL: http://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/kwon (accessed: 2.10.2015).

29. **Abbot T., Lai K., Lieberman M., Price E.** Browser-Based Attacks on Tor [Electronic resource] // Privacy Enhancing Technologies [Official website]. URL: https://www.petsymposium.org/2007/papers/PET2007_preproc_Browser_based.pdf (accessed: 1.10.2015).

30. **Vanbever L., Li O., Rexford J., Mittal P.** Anonymity on QuickSand: Using BGP to Compromise Tor [Electronic resource] // ACM SIGCOMM [Official website]. URL: http://conferences.sigcomm.org/hotnets/2014/papers/hotnets-XIII-final80.pdf (accessed: 1.10.2015).

31. **Ballani H., Francis P., Zhang X.** A study of prefix hijacking and interception in the Internet [Electronic resource] // ACM Pigital Library [Official website]. URL: http://dl.acm.org/citation.cfm?id=1282411 (accessed: 1.10.2015).

32. **Pries R., Yu W., Fu X., Zhao W.** A New Replay Attack Against Anonymous Communication Networks [Electronic resource] // IEEE Xplore [Official website]. URL: http://ieeexplore.ieee.org/xpl/login.isp?tp=&arnumber=4533341&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabsall.isp%3Farnumber%3D4533341 (accessed: 2.10.2015).

33. **Sun Y., Edmundson A., Vanbever L., Li O., Rexford J., Chiang M., Mittal P.** RAPTOR: Routing Attack on Privacy in Tor [Electronic resource] // USENIX [Official website]. URL: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-sun.pdf (accessed: 5.10.2015).

34. **Low** orbit ion cannon. [Electronic resource] // Wikipedia [Official website]. URL: http://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon (accessed: 1.10.2015).

35. **Borisov N., Mittal P., Danezis G., Tabriz P.** Denial of Service or Denial of Security? How Attacks on Reliability can Compromise Anonymity [Electronic resource] // Princeton University [Official website]. URL: http://wfww.princeton.edu/~pmittal/publications/dos-ccs07.pdf (accessed: 1.10.2015).

36. **Jansen R., Tschorsch F., Johnson A., Scheuermann B.** The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network [Electronic resource] // Center for High Assurance Computer Systems [Official website]. URL: http://www.nrl.navy.mil/itd/chacs/biblio/sniper-attack-anonymously-deanonymizing-and-disabling-tor-network (accessed: 1.10.2015).

37. **Pappas V., Athanasopoulos E., Ioannidis S., Markatos E. P.** Compromising Anonymity Using Packet Spinning [Electronic resource] // FORTH-ICS [Official website]. URL: http://www.ics.forth.gr/dcs/Activities/papers/torspin.isc08.pdf (accessed: 2.10.2015).

38. **Evans N. S., Dingledine R., Grothoff C.** A practical congestion attack on tor using long paths [Electronic resource] // ACM Digital Library [Official website]. URL: http://dl.acm.org/citation.cfm?id=1855771 (accessed: 2.10.2015).

39. **Barbera M. V., Kemerlis V. P., Pappas V., Keromytis A. D.** CellFlood: Attacking Tor Onion Routers on the Cheap [Electronic resource] // Springer Link [Official website]. URL: http://link.springer.com/chapter/10.1007%2F978-3-642-40203-6_37 (accessed: 1.10.2015).

40. **How** fast is the RSA algorithm [Electronic resource] // RSA Laboratories [Official website]. URL: http://www.rsa.com/rsalabs/node.asp?id=2212 (accessed: 1.10.2015).

41. **Douceur J. R.** The Sybil Attack [Electronic resource] // Freehaven [Official website]. URL: http://freehaven.net/anonbib/cache/sybil.pdf (accessed: 2.10.2015).

42. **Chakravarty S., Barbera M. V., Portokalidis G., Polychronakis M., Keromytis A. D.** On the Effectiveness of Traffic Analysis Against Anonymity Nerworks Using Flow Records [Electronic resource] // Columbia University [Official website]. URL: https://mice.cs.columbia.edu/getTechreport.php?techreportID=1545 (accessed: 2.10.2015).

43. **Gilad Y., Herzberg A.** Spying in the Dark: TCP and Tor Traffic Analysis [Electronic resource] // Freenet [Official website]. URL: http://freehaven.net/anonbib/cache/tcp-tor-pets12.pdf (accessed: 2.10.2015).

44. **Selected** Papers in Anonimity [Electronic resource] // Freehaven [Official website]. URL: http://freehaven.net/anonbib/ (accessed: 2.10.2015).

45. **Авдошин С. М., Лазаренко А. В.** Технология анонимных сетей // Информационные технологии. 2016. Т. 22, № 4. С. 284—291.

S. M. Avdoshin, Ph. D., professor, Head of Software Engineering School,
Faculty of Computer Science, HSE, e-mail: savdoshin@hse.ru
A. V. Lazarenko, Undergraduate Student, Software Engineering School,
Faculty of Computer Science, HSE, e-mail: avlazarenko@edu.hse.ru
National Research University Higher School of Economics (HSE)

Tor Users Deanonymization Methods

Tor currently is the biggest anonymous network in the world, which is not only the biggest but the safest one. That is why it is widely used by different criminals such as: killers, drug dillers, carders, etc.. The problem of users deanonimizaiton is considered as a very hard and sophisticated task, because of Tors' design and anonymity-features. However, it is possible to solve this problem. This paper is an overview of Tor users deanonimization methods. It describes passive and active methods, their key features. Passive methods are methods, where an adversary can only analyze traffic in the network, but modifications of it are restricted. Active methods actively use traffic modification for its own purposes. The majority of attacks uses Tor vulnerability, related to end-to-end traffic eavesdropping. In the modern Tor network such an attacks could be successful with a very small probability, because an attacker must control both entry and exit tor nodes of a victim. The probability of such combination is very small. On the other hand, there is a class of attacks, known as website fingerprinting attacks. This attacks are very powerful, if an attacker is smart enough in the field of data science. Moreover, WF attacks requires a particularly small amount of resources for successful usage in the real network. But if an attacker is a global adversary of the network, simple statistical tests will help him to successfully deanonimize all users in the network.

Keywords: *anonymous network; deanonymization; PoS; timing attacks; Tor; traffic analysis*

References

1. **Pingledine R., Mathewson N., Syverson P.** Tor: The Second-Generation Onion Router [Electronic rescource], *Tor project* [Official website], URL: https://svn.torproject.org/svn/proiects/design-paper/tor-design.pdf (accessed: 8.09.2015).
2. **TorMetrics** [Electronic resource], *Tor project* [Official website], URL: https://metrics.torproject.org (accessed: 28.09.2015).
3. **The Russian** government hired people to hack the Tor browser, but they failed and now they're quitting [Electronic resource], *Meduza* [Official website]. URL: https://meduza.io/en/news/2015/09/09/the-russian-government-hirecl-people-hack-the-tor-browser-but-they-failed-and-now-they-re-quitting (accessed: 28.09.2015).
4. **The NSA's** Been Trying to Hack into Tor's Anonymous Internet For Years [Electronic resource], *Gizmodo* [Official website], URL: httpv/gizmodo.com/the-nsas-been-trying-to-hack-into-tors-anonymous-inte-1441153819 (accessed: 28.09.2015).
5. **Zakupka** № 0373100088714000008 [Electronic resource], *Gosudarstvennie zakupky* [Official website], URL: http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber=0373100088714000008 (accessed: 2.10.2015).
6. **The Rise** & Fall of Silk Road [Electronic resource], *Wired* [Official website]. URL: http://www.wired.com/2015/04/silk-road-1/ (accessed: 28.09.2015).
7. **Panezis G.** Statistical disclosure attacks [Electronic resource], *Freehaven* [Official website]. URL: http://freehaven.net/anonbib/cache/statistical-disclosure.pdf (accessed: 1.10.2015).
8. **Kedogan D., Agrawal D., Penz S.** Limits Of Anonymity in Open Environment [Electronic resource], *Springer Link* [Official website], URL: http://link.springer.com/chapter/10.1007%2F3-540-36415-3_4 (accessed: 1.10.2015).
9. **Danezis G.** Statistical disclosure attacks [Electronic resource], *Freehaven* [Official website], URL: http://freehaven.net/anonbib/cache/statistical-disclosure.pdf (accessed: 1.10.2015).
10. **Mathewson N., Pingledine R.** Practical traffic analysis: Extending and resisting statistical disclosure [Electronic resource], *Freehaven* [Official website], URL: http://freehaven.net/doc/e2e-traffic/e2e-traffic.pdf (accessed: 1.10.2015).
11. **Agrawal D., Kedogan D., Penz S.** Probabilistic Treatment of Mixes to Hamper Traffic Analysis [Electronic resource], *Freehaven* [Official website], URL: http://freehaven.net/anonbib/cache/agrawa103.pdf (accessed: 1.10.2015).
12. **Panezis G.** The Traffic Analysis of Continuous-Time Mixes [Electronic resource], *Freehaven* [Official website], URL: http://freehaven.net/anonbib/cache/danezis:pet2004.pdf (accessed: 1.10.2015).
13. **Zhu Y., Fu X., Graham B., Bettati R., Zhao W.** On flow correlation attacks and countermeasures in mix networks [Electronic resource], *Freehaven* [Official website]. URL: http://freehaven.net/anonbib/cache/flow-correliation04.pdf (accessed: 1.10.2015).
14. **Levine B. N., Reiter M. K., Wang C., Wright M. K.** Timing attacks in low-latency mix-based systems [Electronic resource], *Freehaven* [Official website], URL: http://freehaven.net/anonbib/cache/flow-correlation04.pdf (accessed: 1.10.2015).
15. **Johnson A., Wacek C., Jansen R., Sherr M., Syverson P.** Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries [Electronic resource], *Aaron Michael Johnson* [Official website], URL: http://www.ohmygodel.com/publications/usersrouted-ccs13.pdf (accessed: 2.10.2015).
16. **Murdoch S. J., Panezis G.** Low-Cost Traffic Analysis of Tor [Electronic resource], *UCL-CS* [Official website], URL: http://sec.cs.ucl.ac.uk/users/smurdoch/papers/oakland05torta.pdf (accessed: 1.10.2015).
17. **Bauer K., McCoy D., Grunwald D., Kohno T., Sicker D.** Low-Resource Routing Attacks Against Tor [Electronic resource], *University of Washington* [Official website], URL: https://homes.cs.washington.edu/-yoshi/papers/Tor/wpes25-bauer.pdf (accessed: 1.10.2015).
18. **Mittal P., Khurshid A., Juen J., Caesar M., Borisov M.** Stealthy Traffic Analysis of Low-Latency Anonymous Communication Using Throughput Fingerprinting [Electronic resource], *Princeton University* [Official website]. URL: http://www.princeton.edu/-pmittal/publications/throughput-fingerprinting-ccs11.pdf (accessed: 1.10.2015).
19. **Cai X., Zhang X., Joshi B., Johnson R.** Touching from a Pistance: Website Fingerprinting Attacks and Pefenses [Electronic resource], *Stony Brook University* [Official website], URL: http://www3.cs.stonybrook.edu/~xcai/fp.pdf (accessed: 1.10.2015).
20. **Wang T., Cai X., Nithyanand R., Johnson R., Goldberg I.** Effective Attacks and Provable Defenses for Website Fingerprinting [Electronic resource], *Centre for Applied Cryptographic Research The Umyersity of Waterloo* [Official website], URL: http://cacr.uwaterloo.ca/techreports/2014/cacr2014-05.pdf (accessed: 1.10.2015).
21. **Cai X., Nithyanand R., Wang T., Johnson R., Goldberg I.** A Systematic Approach to Developing and Evaluating Website Fingerprinting Defences [Electronic resource], *Freehaven* [Official website]. URL: http://freehaven.net/anonbiD/cache/ccs2014-fingerpnnting.pdf (accessed: 1.10.2015).

22. **Panchenko A., Niessen L., Zinnen A., Enggl A.** Website fingerprinting in onion routing based anonymization networks [Electronic resource], *Freehaven* [Official website], URL: http://freehaven.net/anonbib/cache/wpes11-panchenko.pdf (accessed: 1.10.2015).

23. **Experimental** Defense for Website Traffic Fingerprinting [Electronic resource], *Tor project* [Official website], URL: https://blog.torproject.org/blog/experimental-defense-vvebsite-traffic-fingerprinting (accessed: 1.10.2015).

24. **Wang T., Goldberg I.** Improved Website Fingerprinting on Tor [Electronic resource], *Freehaven* [Official website], URL: http://freehaven.net/anonbib/cache/wpes13-fingerprinting.pdf (accessed: 1.10.2015).

25. **Goldschlag D., Reed M., Syverson P.** Onion Routing for Anonymous and Private Internet Connections. January 28, 1999 [Electronic resource], *Onion Routing* [Official website], URL: http://www.omon-router.net/Publications/CACM-1999.pdf (accessed: 8.09.2015).

26. **Chaum D.** Untraceable Electronic Mail, Return Addressed, and Digital Pseudonyms [Electronic resource], *Free Haven* [Official website], URL: http://www.treehaven.net/anonbib/caclie/chaum-mix.pdf (accessed: 28.09.2015).

27. **Wiangsripanawan R., Susilo W., Safavi-Naini R.** Design principles for low latency anonymous network systems secure against timing attacks [Electronic resource], *ACM Digital Library* [Official website], URL: http://dl.acm.org/citation.cfm?ig=1274553 (accessed: 28.09.2015).

28. **Kwon A., AlSabah M., Lazar D., Dacler M., Devadas S.** Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services [Electronic resource], *USENIX* [Official website]. URL: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/kwon (accessed: 2.10.2015).

29. **Abbot T., Lai K., Lieberman M., Price E.** Browser-Based Attacks on Tor [Electronic resource], *Privacy Enhancing Technologies* [Official website]. URL: https://www.petsymposium.org/2007/papers/PET2007_preproc_Browser_based.pdf (accessed: 1.10.2015).

30. **Vanbever L., Li P., Rexford J., Mittal P.** Anonymity on QuickSand: Using BGP to Compromise Tor [Electronic resource], *ACM SIGCOMM* [Official website]. URL: http://conferences.sigcomm.org/hotnets/2014/papers/hotnets-XIII-final80.pdf (accessed: 1.10.2015).

31. **Ballani H., Francis P., Zhang X.** A study of prefix hijacking and interception in the Internet [Electronic resource], *ACM Digital Library* [Official website]. URL: http://dl.acni.org/citation.cfm?id-1282411 (accessed: 1.10.2015).

32. **Pries R., Yu W., Fu X., Zhao W.** A New Replay Attack Against Anonymous Communication Networks [Electronic resource], *IEEE Xplore* [Official website], URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4533341&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D453334 1 (accessed: 2.10.2015).

33. **Sun Y., Edmundson A., Vanbever L., Li O., Rexford J., Chiang M., Mittal P.** RAPTOR: Routing Attack on Privacy in Tor [Electronic resource], *USENIX* [Official website]. URL: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-sun.pdf (accessed: 5.10.2015).

34. **Low orbit** ion cannon. [Electronic resource], *Wikipedia* [Official website]. URL: http://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon (accessed: 1.10.2015).

35. **Borisov N., Mittal P., Danezis G., Tabriz P.** Denial of Service or Denial of Security? How Attacks on Reliability can Compromise Anonymity [Electronic resource], *Princeton University* [Official website], URL: http://www.princeton.edu/~pmittal/publications/dos-ccs07.pdf (accessed: 1.10.2015).

36. **Jansen R., Tschorsch F., Johnson A., Scheuermann B.** The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network [Electronic resource], *Center for High Assurance Computer Systems* [Official website], URL: http://www.nrl.navy.mil/itd/chacs/biblio/sniper-attak-anonymously-deanonymizing-and-disabling-tor-network (accessed: 1.10.2015).

37. **Pappas V., Athanasopoulos E., Ioannidis S., Markatos E. P.** Compromising Anonymity Using Packet Spinning [Electronic resource], *FORTH-ICS* [Official website], URL: http://www.ics.forth.gr/dcs/Activities/papers/torspin.isc08.pdf (accessed: 2.10.2015).

38. **Evans N. S., Dingledine R., Grothoff C.** A practical congestion attack on tor using long paths [Electronic resource], *ACM Digital Library* [Official website], URL: http://dl.acm.org/citation.cfm?id-1855771 (accessed: 2.10.2015).

39. **Barbera M. V., Kemerlis V. P., Pappas V., Keromytis A. D.** CellFlood: Attacking Tor Onion Routers on the Cheap [Electronic resource], *Springer Link* [Official website], URL: http://link.springer.com/chapter/10.1007%2F978-3-642-40203-637 (accessed: 1.10.2015).

40. **How** fast is the RSA algorithm [Electronic resource], *RSA Laboratories* [Official website]. URL: http://www.rsa.com/rsalabs/node.asp?id=2212 (accessed: 1.10.2015).

41. **Douceur J. R.** The Sybil Attack [Electronic resource], *Freehaven* [Official website]. URL: http://freehaven.net/anonbib/cache/sybil.pdf (accessed: 2.10.2015).

42. **Chakravarty S., Barbera M. V., Portokalidis G., Polychronakis M., Keromytis A. D.** On the Effectiveness of Traffic Analysis Against Anonymity Nerworks Using Flow Records [Electronic resource], *Columbia University* [Official website], URL: https://mice.cs.columbia.edu/getTechreport.php?techreportID=1545 (accessed: 2.10.2015).

43. **Gilad Y., Herzberg A.** Spying in the Dark: TCP and Tor Traffic Analysis [Electronic resource], *Freenet* [Official website]. URL: http://freehaven.net/anonbib/cache/tcp-tor-pets12.pdf (accessed: 2.10.2015).

44. **Selected** Papers in Anonimity [Electronic resource], *Freehaven* [Official website], URL: http://freehaven.net/anonbib/ (accessed: 2.10.2015).

45. **Avdoshin S., Lazarenko A.** Technology of Anonymous Networks, *Informational Technologies*, 2016, vol. 22, no. 4, pp. 284—291.