6. Цели, предмет и критерии оценки управляющих организаций для формирования потребительского рейтинга / Институт экономики города [Электронный ресурс] – Режим доступа: http://www.urbanecomomics.ru/sites/default/files/4072_import.pdf (дата обращения 20.06.2020).
7. Рейтинговое агентство RAEX (Эксперт РА) [Электронный ресурс] – Режим доступа: <http://www.raexpert.ru/> (дата обращения 15.05.2020).
8. Справочно-новостной сайт «ДОМ-и-ДВОР.рф» [Электронный ресурс] – Режим доступа: <http://dom-i-dvor.info/> (дата обращения 15.05.2020).
9. Государственная корпорация — Фонд содействия реформированию жилищно-коммунального хозяйства «Реформа ЖКХ» [Электронный ресурс] – Режим доступа: <https://www.reformagkh.ru/> (дата обращения 15.05.2020).
10. Методика оценки управляющих организаций для построения потребительского рейтинга/ Институт экономики города [Электронный ресурс] – Режим доступа: <http://www.urbanecomomics.ru/node/4293/> (дата обращения 12.06.2020).
11. Методические рекомендации по оценке эффективности работы организаций, управляющих многоквартирными домами /Методические рекомендации комитета по жилищно-коммунальному хозяйству г. Саратова от 19.08.2008
12. Патудин В.М., Стерлягов С.П. Комплексный рейтинг управляющих организаций в сфере управления многоквартирными домами как инструмент контроля качества жилищно-коммунальных услуг / Сборник научных статей международной конференции «Ломоносовские чтения на Алтае: фундаментальные проблемы науки и образования», Барнаул, 20-24 октября, 2015. – Барнаул : Изд-во Алт. ун-та, 2015. – С. 3562-3564

Хомутецкая М.А., Воробьева В.А., Омельченко Т.А.
Исследование механизмов обеспечения безопасности tor-сети

*ФГАОУ ВО «Волгоградский государственный университет»
(Россия, Волгоград)*

doi: 10.18411/lj-08-2020-09

idsp: ljjournal-08-2020-09

Аннотация

Статья посвящена исследованию механизмов обеспечения безопасности сети Tor с целью определения лучшего набора средств, обеспечивающих безопасность пользователя в сети Tor. Выделены компоненты сети tor, угрозы и механизмы защиты для каждого компонента. Разработана программа для автоматизации выбора наилучшего набора механизмов обеспечения безопасности сети Tor.

Ключевые слова: Сеть Tor, обеспечение информационной безопасности сети, анонимность в сети, шифрование.

Abstract

The article is devoted to the study of security mechanisms of the Tor network in order to determine the best set of tools that ensure user security in the Tor network. The components of the tor network, threats, and protection mechanisms for each component are highlighted. A program has been developed to automate the selection of the best set of security mechanisms for the Tor network.

Keywords: Tor, network's information security, network anonymity, encryption.

Tor-сеть – это система прокси-серверов, предназначенных для сетевого соединения в анонимном режиме, защищенном от прослушивания и без возможности отслеживания действий пользователя [1]. Среди основных функций и возможностей Tor выделяют запрет на отслеживание поведения пользователя в браузере, защиту клиентов при обмене мгновенными сообщениями, бесплатное распространение и открытый исходный код для операционных систем Mac OS X, Windows и Linux[4]. На рисунке представлено сравнение маршрутов передвижения трафика в обычной и tor-сети.

Рисунок 1 – Путь передвижения трафика по сети

Маршрут передвижения трафика по tor-сети от его начала до конечного пункта проходит по следующим основным элементам: Абонент А (Пользователь 1/клиент 1 сети tor) — Канал связи от Абонента А до входного узла — Входной узел — Промежуточные узлы и каналы связи — Выходной узел — Канал связи от выходного узла до Абонента Б — Абонент Б (Пользователь 2/клиент 2 сети tor/Конечный ресурс).

Tor работает на основе метода «луковичной маршрутизации». Пользовательские данные сначала шифруются так, чтобы их могли расшифровать только на выходном узле, который отправляет трафик в конечную точку назначения [5]. После этого эти данные снова шифруются и их расшифровка может быть возможна только на промежуточном узле, а затем их переносят через различные ретрансляторы, присутствующие в сети Tor. На каждом ретрансляторе один слой расшифровывается, а оставшиеся данные передаются на любой случайные ретранслятор до тех пор, пока не будет достигнут конечный сервер. Для сервера назначения, выходной узел является исходными данными. В результате каждый узел содержит только нужную ему информацию, а именно: откуда пришли зашифрованные данные, и куда их надо отправить [2]. Таким образом, очень трудно проследить личность пользователя или сервер с помощью любых систем наблюдения, действующих в середине пути.

Как и в обычной сети, на сегодняшний день существует ряд угроз информационной безопасности, реализация которых способна скомпрометировать элементы tor-сети. Абонент А, входной узел, промежуточные узлы и каналы связи, Абонент Б подвержены риску вычисления IP-адреса пользователя посредством подключенных и используемых скриптовых языков в Тор браузере на его (пользователя) устройстве. Каналы связи «от Абонента А до входного узла» и «от выходного узла до Абонента Б» подвержен риску глобального наблюдения. Выходной узел подвержен риску кражи или модификации данных, переданных пользователем, посредством «подставного» выходного узла, который может использовать свои привилегии и воспользоваться расшифрованным пакетом пользователя [3]; а также выявления IP-адреса пользователя посредством подключенных и используемых скриптовых языков в Тор браузере на его (пользователя) устройстве.

Для анализа механизмов обеспечения безопасности сети Tor определены критерии и их возможные значения:

- 1) Уровень анонимности субъекта tor-сети: высокий; средний; низкий.
- 2) Возможность обеспечения целостности данных: да; нет.
- 3) Возможность обеспечения доступности данных: да; нет.
- 4) Возможность обеспечения конфиденциальности данных: да; нет.
- 5) Сложность настройки механизма обеспечения безопасности tor-сети: высокая; средняя; низкая.

Таблица 1

Сравнительный анализ механизмов обеспечения безопасности Tor-сети по выделенным критериям.

Критерии	Механизмы обеспечения безопасности						
	Пользователь			Сервис Tor			
	Отключени е в Tor браузере скриптовых языков	Использование сайтов, которые поддерживают HTTPS- протокол	Знание пользовате ля о рисках	Шифрован ие	Вычислени е «подставн ых узлов»	Мосты	Секретн ые узлы
1	Высокий	Средний	Низкий	Высокий	Средний	Высокий	Низкий
2	Нет	Да	Нет	Да	Да	Да	Нет
3	Да	Да	Да	Да	Да	Да	Да
4	Да	Да	Да	Да	Да	Да	Нет
5	Высокая	Средняя	Низкая	Средняя	Высокая	Средняя	Низкая

Для автоматизации выбора наилучшего набора механизмов обеспечения безопасности tor-сетей разработано программное средство.

Интерфейс разработанного программного средства.

Проведена серия экспериментов с участием группы экспертов, которым было предложено выбрать один из трех предложенных средств обеспечения безопасности тор-сети на уровне пользователя (область 1), и одно из трех предложенных средств обеспечения безопасности тор-сети на уровне сервиса Тор (область 2). А также, расставить значения критериев для выбранного средства обеспечения безопасности (область 3).

Каждому из значений критериев программно присвоено числовое значение. После выбора экспертом средства обеспечения безопасности, программа автоматически выставляет соответствующие данному средству значения критериев и рассчитывает расстояние Хэмминга, определяющее степень безопасности выбранного средства: чем меньше расстояние Хэмминга, тем лучше обеспечивает безопасность анализируемое средство.

Таблица 2

Результаты экспериментальных исследований

№	Название эксперимента	Входные данные	Полученный результат
1	Определение лучшего средства реализации механизма обеспечения безопасности сети Тор на уровне пользователя	Отключение в Тор браузере скриптовых языков	1
		Использование сайтов, которые поддерживают HTTPS-протокол	1
		Знание пользователя о рисках	3
2	Определение лучшего средства реализации механизма обеспечения безопасности сети Тор на уровне сервиса Тор	Шифрование	0,5
		Вычисление «подставных узлов»	0,5
		Мосты	0,5
		Секретные узлы	3,5

Лучшими средствами реализации механизмов обеспечения безопасности тор сети на уровне пользователя являются: отключение в Тор браузере скриптовых языков; использование сайтов, которые поддерживают HTTPS-протокол. Оба этих средства имеют одинаковое значение расстояния Хэмминга, равное единице, и это наименьшее значение в группе средств обеспечения безопасности сети Тор на уровне пользователя.

Лучшими средствами реализации механизмов обеспечения безопасности тор сети на уровне сервиса Тор являются: шифрование; вычисление «подставных узлов»; мосты. Данные средства имеют одинаковые значения расстояния Хэмминга, равное 0,5, которое является наименьшим значением в группе средств обеспечения безопасности сети Тор на уровне сервиса Тор.

1. Кузьменко, Н.Г. Компьютерные сети и сетевые технологии / Н.Г. Кузьменко. - СПб.: Наука и техника, 2013. - 368 с.
2. Луганцев, Л.Д. Компьютерные сети / Л.Д. Луганцев. - М.: МГУИЭ, 2001. - 452 с.
3. Fossbytes. Everything about Tor: What is Tor? How Tor Works? <https://fossbytes.com/everything-tor-tor-works/> By Aditya Tiwari May 22, 2017
4. Fossbytes. TOR Anonymity: Things Not To Do While Using TOR. <https://fossbytes.com/tor-anonymity-things-not-using-tor/> By Aditya Tiwari May 23, 2018
5. Луковая_маршрутизация [Электронный ресурс] – Режим доступа: http://poli-grafi.ru/Луковая_маршрутизация – 27.05.2016.