УДК 004.414.2

О. И. Семенюк[1]*

Исследование оверлейной сети Tor

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: semeniuk16@yandex.ru

Аннотация. В статье исследуется архитектура и принцип работы оверлейной сети Tor. В совокупности с анализом защищённости стека протоколов TCP/IP возможно получение более детального представления о существующих уязвимостях данной системы. В ходе исследования были определены основные проблемы использования систем анонимизации при одиночном и совместном использовании с другими средствами обеспечения сетевой безопасности. В рамках работы проведено моделирование предметной области, в результате которого предложено создание системы идентификации незадекларированных функций на выходных нодах сети Tor. Процесс работы системы описан при помощи BPMN-диаграммы, так как такой метод представления процессов помогает улучшить их понимание и выявляет возможности для их оптимизации и автоматизации. Область применения предлагаемого решения – обеспечение сетевой безопасности пользователей при использовании глобальной вычислительной сети Интернет.

Ключевые слова: анонимизация, оверлейная сеть, луковая маршрутизация, Tor, уязвимости, сетевая безопасность

O. I. Semeniuk[1]*

Tor overlay network research

[1] National Research Nuclear University (MEPhI), Moscow, Russian Federation
* e-mail: semeniuk16@yandex.ru

Abstract. The article explores the architecture and principle of operation of the Tor overlay network. In conjunction with the analysis of the security of the TCP/IP protocol stack it is possible to obtain a more detailed understanding of the existing vulnerabilities of this system. In the course of the study the main problems of using anonymization systems in single and joint use with other means of ensuring network security were identified. As part of the work a modeling of the subject area was carried out because of which it was proposed to create a system for identifying undeclared functions on the output nodes of the Tor network. The process of the system is described using a BPMN diagram as this method of representing processes helps to improve their understanding and identifies opportunities for their optimization and automation. The scope of the proposed solution is to ensure the network security of users when using the global computing network Internet.

Keywords: anonymization, overlay network, onion routing, Tor, vulnerabilities, network security

Введение

В современной цифровой эпохе выход в глобальную вычислительную сеть Интернет доступен практически каждому человеку. Стремительное развитие технологий и простота их эксплуатации предоставляет возможность беспрепятственного пользования интернет-ресурсами. Однако помимо положительных ас-

пектов существуют и негативные стороны. Большой объём открытой для каждого пользователя сети Интернет информации вынуждает всё чаще задумываться о сохранности персональных данных, оставляемых в сети.

Совершенствование процесса использования интернет-ресурсов влечёт за собой закономерное совершенствование действий и навыков злоумышленников. Итоговая статистика одного из крупнейший российских вендоров в сфере информационной безопасности Positive Technologies за 2022 год показывает общий рост кибератак на 20,8% в сравнении с 2021 годом. Также в 2022 году происходили массовые утечки – успешная кража конфиденциальной информации из организаций состоялась в 47% случаев. За год количество кибератак на государственные учреждения повысилось на 18% [1].

В рамках подержания конфиденциальности и увеличения степени сохранности персональных данных ведётся разработка и успешная эксплуатация программного обеспечения и решений, позволяющих достичь определённого уровня анонимности нахождения в сети. Но данные решения также применяются и злоумышленниками, которые реализуют с их помощью все виды преступной деятельности, начиная с добычи конфиденциальной информации определённой личности и заканчивая незаконной торговлей. Одной из самых популярных и широко используемых технологий является оверлейная сеть Tor (англ. – The Onion Router) [2].

Необходимо провести анализ архитектуры выбранной сети и принципа её работы для определения основных уязвимостей, блокировок и угроз информационной безопасности для определения мест, максимально подверженных атакам со стороны злоумышленников.

Исследование предметной области

Основой построения глобальной вычислительной сети Интернет является стек протоколов TCP/IP (англ. Transmission Control Protocol – протокол управления передачей, Internet Protocol – Интернет-протокол). Информация, передаваемая по TCP-протоколу, является исходно отправляемой информацией. В свою очередь, IP-протокол не гарантирует целостность доставляемой информации, поэтому TCP-протокол вложен в него.

Основная проблема стека протоколов TCP/IP – отсутствие защиты передаваемой информации. При передаче информации не производится шифрование пакетов сообщений а также нет контроля подлинности передаваемых данных [3]. Эти проблемы позволяют злоумышленникам:

– получить несанкционированный доступ к сети;
– осуществить прослушивание сети;
– анализировать трафик;
– выдавать себя за другой узел цепи;
– произвести кражу конфиденциальной информации.

На основе описанных проблем существуют уязвимости данного стека протоколов, приводящие к отказу в обслуживании серверов, перенаправляющие пользователей на вредоносные сайты, позволяющие вести сканирование сети и

тому подобное [4]. Системы обнаружения вторжений или антивирусные программы, рекомендуемые для защиты от уязвимостей стека протоколов TCP/IP, не позволяют в полной мере защититься от злоумышленников [5, 6].

Под оверлейной сетью подразумевается виртуальная сеть, построенная поверх существующей сети, коей является рассматриваемая сеть Tor. Одно из преимуществ его использования – простота при установке и использовании из-за отсутствия необходимости в изменении ядра или применении специальных привилегий. Данный подход позволяет реализовать анонимность для сервисов и приложений, работающих на TCP-протоколах [7]. Также данный подход обеспечивает простую переносимость и развёртываемость сети.

Сеть Tor работает за счёт «луковой маршрутизации», суть которой заключается в послойном шифровании передаваемого пакета данных [8] (рис. 1).

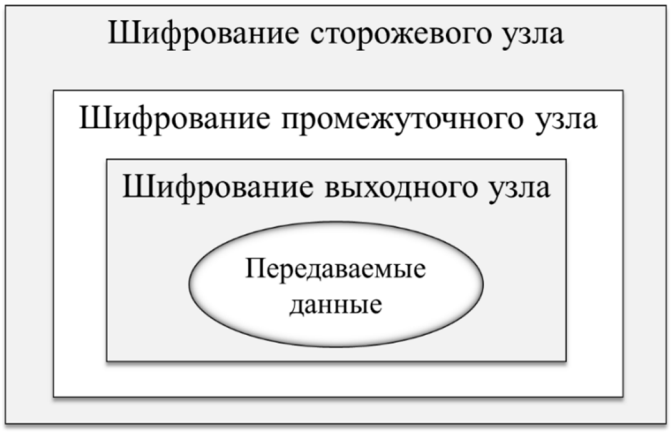

Рис. 1. Принцип шифрования данных при использовании луковой маршрутизации

Информация, передаваемая через сеть Tor, в среднем проходит последовательность из трёх узлов сети. Их роль выполняют компьютеры-посредники (ретрансляторы), расположенные по всему миру. Перечень ретрансляторов, используемых сетью Tor находится в публичном доступе.

Узлы (или ноды), составляющие цепочку в исследуемой сети:

– входной (или сторожевой) нод;
– промежуточный нод;
– выходной нод.

Благодаря луковой маршрутизации каждый последующий узел цепи «знает» лишь информацию об узле, с которого пришёл пакет данных, и об узле, на который следует оправить пакет далее. Данный подход повышает уровень анонимности пользователя, но снижает скорость передачи данных в сравнении с использованием обычной сети [9].

Однако, при расшифровании информации на выходном ноде становятся открытыми не только конечный адрес передачи данных, но и сама передаваемая информация [10]. Это даёт возможность злоумышленникам перехватывать необ-

ходимые им данные на этом узле цепи. Тем не менее, зная само содержание передаваемой информации и её отправителя, можно делать выводы о незаконном применении оверлейной сети, что позволит применять своевременные меры по усилению личной или корпоративной безопасности.

Совместное применение исследуемой сети с другими средствами обеспечения анонимности позволяет снизить количество возможных атак. Однако данный способ повышения безопасности не гарантирует их отсутствие.

Постановка задачи

Целью настоящей работы является выявление возможных уязвимостей и угроз информационной безопасности оверлейной сети Tor.

Для достижения цели была проведена её декомпозиция на следующие подзадачи:

1) систематизация проблематики предметной области посредством её анализа;
2) моделирование предметной области.

Предлагаемое решение

Анализ принципа работы оверлейной сети Tor и её уязвимостей позволил определить основные угрозы информационной безопасности при её использовании. Таким образом, было принято решение начать разработку системы идентификации незадекларированных функций на выходных нодах сети Tor.

В качестве представления процесса работы системы идентификации был выбран язык моделирования BPMN (англ. Business Process Model and Notation – модель бизнес-процессов и нотация), так как он является промежуточным звеном между визуализацией и воплощением процесса.

На рис. 2 представлена BPMN-диаграмма процесса работы предлагаемой системы идентификации незадекларированных функций.

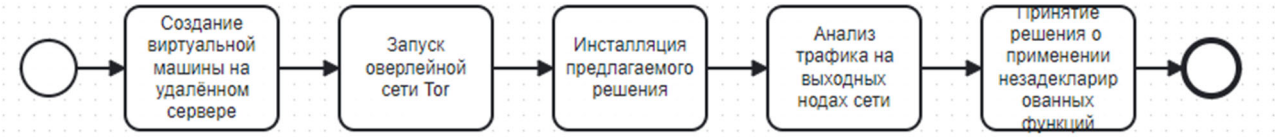

Рис. 2. BPMN-диаграмма процесса работы системы идентификации незадекларированных функций на выходных нодах сети Tor

Важно отметить, что приведённая диаграмма не является единственным способом описания результатов моделирования предметной области, поэтому в дальнейшем будут разработаны блок-схемы принципа работы системы и UML-диаграммы. Совокупность блок-схем и диаграмм упростит процесс проектирования и разработки программного решения.

Заключение

В данной работе был проведён анализ защищённости стека протокола TCP/IP и основных уязвимостей оверлейной сети Tor в рамках исследования предметной области. Итогом проведённого исследования является принятие решения по созданию системы идентификации незадекларированных функций на выходных нодах сети Tor.

Практическая значимость работы заключается в повышении безопасности эксплуатации оверлейной сети обычными пользователями.

В дальнейшем планируется проектирование и программная реализация предложенного решения, а также проведение ручного и автоматизированного тестирования разработанной системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Актуальные киберугрозы: итоги 2022 года [Электронный ресурс]. – 2023. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения 29.04.2023)

2. Басыня Е. А. Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации = Method to identify cybercriminals using network analysis of information systems with anonymization / Е. А. Басыня, В. Е. Хиценко, А. А. Рудковский // Доклады Томского государственного университета систем управления и радиоэлектроники. - 2019. – Т. 22, № 2. – С. 45–51.

3. Kantaeva A., Ussupona S. The features of the TCP/IP layers //Сборник статей Международной научно-практической конференции. — Петрозаводск, 2022. — Изд. «Международный центр научного партнёрства «Новая Наука» (ИП Ивановская И.И.)». — С. 55—58.

4. Терентьев А. М. Сетевой мониторинг. Методы и средства. Том 1 // Монография. — Чебоксары, 2019. — 117 с.

5. Bazanov V.V., Frolov A.A., Arzhskov A.V. Method for identifying dangerous forum posts on the onion network // Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2020. — 2020. — 229—232 p.

6. Нурмухамбетова С.А., Суслов К.В., Шагалов С.В. Анализ угроз сетевой безопасности // Сфера знаний: вопросы современного этапа развития научной мысли. — Казань. 2018. — С. 489—492.

7. Vincent O.N., Silvance O. Abeka, Prof. Anthony Rodrigues. Security evaluation of cellular networks handover Techniques // I. J. Computer Network and Information Security — 2018. — 45—59 p.

8. Белов Ю.С., Ткаченко А.В., Климушина Д.В. Технология луковой маршрутизации и сеть Tor // Высокие технологии и инновации в науке. Сборник избранных статей Международной научной конференции. — 2019. — С. 157—160.

9. Карпов Д.С., Ибрагимова З.А. Способы и средства обеспечения анонимности в глобальной сети Интернет // Правовая информатика. — 2021. — №3. — С. 60—67.

10. Новосельцева А.В., Клюев С.Г. Современные методы атак деанонимизации на сеть Tor // Прикаспийский журнал: управление и высокие технологии. — 2020. — № 1 (49). — С. 155—161.