УДК 004.7

Фетисов Максим Владимирович, магистрант, Российский технологический университет – Московский институт радиотехники, электроники и автоматики, г. Москва

Лукьянов Юрий Аркадьевич, доцент кафедры информационных технологий в системах управления, Российский технологический университет – Московский институт радиотехники, электроники и автоматики, г. Москва

ОБЗОР СОВРЕМЕННЫХ МЕТОДОВ И ПРОТОКОЛОВ ПЕРЕДАЧИ DNS ЗАПРОСОВ

Аннотация. В статье проведён обзор современных протоколов и методов передачи DNS запросов с целью выявления наиболее подходящих вариантов для практического применения в корпоративных и глобальных сетях. Проанализированы преимущества и недостатки протоколов с точки зрения безопасности, производительности и распространённости. Структурированы ключевые особенности следующих протоколов и методов передачи запросов: DNS over UDP/TCP, DNSSEC, DNS over TLS, DNS over HTTPS, DNS over QUIC, Oblivious DNS. На основе проведенного анализа сформулированы рекомендации по выбору оптимального протокола в зависимости от требований конкретной сетевой инфраструктуры и типа соответствующих угроз.

Annotation. The article provides an overview of modern protocols and methods for transmitting DNS queries in order to identify the most suitable options for practical use in corporate and global networks. The advantages and disadvantages of protocols are analyzed in terms of security, performance, and prevalence. The key features of the following protocols and methods for transmitting queries are structured: DNS over UDP/TCP, DNSSEC, DNS over TLS, DNS over HTTPS, DNS over QUIC, Oblivious DNS. Based on the analysis, recommendations

are formulated for choosing the optimal protocol depending on the requirements of a specific network infrastructure and the type of relevant threats.

Ключевые слова: DNS запросы, шифрование, протоколы передачи данных, безопасность, производительность, корпоративные сети, глобальные сети, Интернет, UDP, TCP, DNSSEC, DNS over TLS, DNS over HTTPS, DNS over QUIC, Oblivious DNS.

Keywords: DNS queries, encryption, data transfer protocols, security, performance, corporate networks, global networks, Internet, UDP, TCP, DNSSEC, DNS over TLS, DNS over HTTPS, DNS over QUIC, Oblivious DNS.

Введение

Система доменных имён (DNS) является неотъемлемой частью современной глобальной сетевой инфраструктуры. Проблемы и угрозы, связанные с ней, влияют на работоспособность всего Интернета и остаются актуальными по сей день. Разработанная в 1980-х годах система доменных имён создавалась с простой целью: преобразования удобочитаемых для человека доменных имён в IP-адреса для идентификации компьютеров в сети. По задумке создателей DNS должен был автоматизировать систему именования с возможностью её масштабирования, и в итоге была принята и реализована концепция иерархической организации системы доменных имён. Однако в то время вопросы безопасности передачи самих DNS запросов были вторичны, так как сами сети не были открыты широкой общественности и упор ставился на создание самой инфраструктуры системы доменных имён.

DNS over UDP/TCP

Традиционно DNS запросы передаются через протокол транспортного уровня UDP. Такое решение создателей DNS обусловлено простотой и скоростью передачи, так как данные в UDP передаются без шифрования и установления соединения. Протокол удовлетворял изначальным требованиям: запросы должны были быть быстрыми и состоять из одного пакета ответа. Стоит отметить, что в случаях, когда необходимо передать большие объёмы данных, такие как полные зоны DNS, используется TCP вместо UDP, который в дополнение ещё и гарантирует надёжность и целостность. Однако с распространением и популяризацией Интернета остро возникла необходимость обеспечения безопасности передачи DNS запросов. Появилось множество различных угроз, связанных с злоупотреблением открытостью передачи DNS запросов и ответов, что позволило перехватывать и подменять их. Таким образом, UDP уже не удовлетворял современным требованиям, подталкивая к разработке новых защищённых способов передачи данных. Далее разберём альтернативные варианты передачи DNS пакетов и обсудим, какие угрозы они предотвращают.

Атаки типа подмены, которым подвержены передачи данных через UDP, описаны в статье [1]. Также атаки других типов и их анализ подробно разобраны в статье [3, с. 924-925].

DNSSEC

Первым набором расширений безопасности для DNS является DNSSEC (Domain Name System Security Extensions), позволяющий с помощью цифровых подписей, добавляемых к DNS запросам, обеспечить аутентичность и целостность данных в системе доменных имён. Важно отметить, что DNSSEC не обеспечивает конфиденциальность запросов, всё ещё позволяя сторонним лицам анализировать запросы пользователей. Механизм работы аналогичен PKI (Public Key Infrastructures), в котором используется цифровая подпись и образуются цепочки доверия между узлами иерархической структуры. Стоит отметить, что за счёт использования цифровой подписи увеличивается и объём передаваемого трафика в среднем на 20%. Однако также DNSSEC требует поддержки криптографических ключей на всех уровнях инфраструктуры, что замедляет его массовое внедрение. Для достижения комплексной защиты лучшим вариантом является комбинирование DNSSEC с другими протоколами, которые обеспечивают шифрование трафика.

Подробнее об DNSSEC описано в статье [4]. Также комбинация DNSSEC с другими протоколами представлена в статье [5, с. 57].

DNS over TLS

После разработки DNSSEC всё ещё остались угрозы конфиденциальности DNS запросов. Следующим шагом в обеспечении безопасности является DNS over TLS (DoT), применяющий шифрование TLS непосредственно к DNS пакетам. Основной принцип работы данного протокола заключается в установке защищённого TLS-соединения, через которое весь последующий трафик шифруется и аутентифицируется. DoT базируется поверх TCP на порту 853 и предоставляет соответственно меньшую скорость передачи по сравнению с UDP. Также стоит учитывать, что само использование DoT легко

обнаружить из-за статичного порта. С одной стороны, это позволяет улучшить безопасность корпоративных сетей с помощью фильтрации трафика, а с другой – DoT может быть легко заблокирован.

DNS over HTTPS

Альтернативой использования DoT является DNS over HTTPS (DoH). Как можно понять из названия, данный протокол инкапсулирует DNS сообщения в HTTPS поверх TLS с использованием стандартного порта TCP 443. Использование протокола HTTPS предоставляет несколько преимуществ по сравнению с DoT: маскировка под HTTPS трафик, которая защищает от блокировок по порту, возможность интеграции по веб-API. Также DoH имеет и некоторые недостатки: сложность контроля и фильтрации трафика в корпоративных сетях, увеличенный объём передаваемого трафика из-за инкапсуляции в HTTPS.

Практическое применение DoH и DoT описано в статье [2, с. 138-139].

Oblivious DNS over HTTPS

Стоит упомянуть недавно разработанный протокол Oblivious DNS over HTTPS (ODoH), являющийся усовершенствованной версией DoH. Концептуальная идея заключается в использовании дополнительного посредника – прокси-сервера, который принимает DNS запросы пользователя, но при этом не имеет возможности расшифровать сами данные DNS запроса. Далее прокси-сервер пересылает от своего IP адреса запрос к DNS серверу, который уже может расшифровать данные, но он видит только IP адрес прокси-сервера, что гарантирует приватность пользователя. Стоит отметить, что данный концепт работает только, если прокси и DNS сервера контролируются разными организациями.

DNS over QUIC

Среди других инновационных защищённых протоколов передачи остаётся обсудить DNS over QUIC (DoQ), который был официально стандартизирован в мае 2022 года рабочей группой IETF в документе RFC 9250. В отличие от DoT и DoH, которые инкапсулируют в TLS и TCP, DoQ

работает поверх изначального UDP. На своём уровне QUIC обеспечивает шифрование данных и аутентификацию, предоставляет восстановление потерь пакетов, компенсируя недостаток UDP. На данный момент QUIC слабо распространён и поддерживается немногими устройствами, однако его ключевые преимущества делают его перспективным протоколом будущего.

Выводы

На основе вышеизложенных принципов работы различных протоколов определим в каких ситуациях они наиболее применимы. Стандартная передача DNS over UDP/TCP поддерживается всеми техническими средствами и может использоваться в различных ЛВС, в которых требования к безопасности от внешних угроз носят вторичный характер.

В корпоративных сетях, в которых важна конфиденциальность и управляемость трафиком, рекомендуется использовать DNS over TLS, так как данный протокол обеспечивает шифрование, аутентификацию и является прозрачным для фильтрации. В отдельных ситуациях, в которых использование DoT недоступно, допустима интеграция DNS over HTTPS, однако данное решение усложнит контроль и фильтрацию трафика в корпоративной среде.

В пользовательском сегменте одним из наиболее подходящих вариантов является DNS over HTTPS. Протокол поддерживается многими браузерами и мобильными ОС и обеспечивает приватность пользовательских запросов.

В будущем DoT и DoH могут быть заменены протоколами DNS over QUIC или Oblivious DNS, однако на текущий момент они носят экспериментальный и приватный характер.

Список литературы

1. Асянова С.Р., Жигалова Я.И. Спуфинг как угроза кибербезопасности: понятие, виды, меры противодействия // Journal of Monetary Economics and Management. 2024. №11. С. 242-247.

2. Методы защиты трафика от вмешательства DPI-информационных систем вузов на базе использование DOH и DOT протоколов / В. В. Фигурчиков [и др.] // Управление образованием: теория и практика. 2022. №6/12. С. 133-142.
3. Полянская М.С. Анализ подходов к обнаружению атак в зашифрованном трафике // Современные информационные технологии и ИТ-образование. 2021. Т. 17, № 4. С. 922-931.
4. Радивилова Т. А., Бушманов В. С. Анализ основных атак на DNS-сервер и методы использования dnssec при защите DNS-сервера // Технологический аудит и резервы производства. 2013. № 2/1(10). С. 16-19.
5. Уралов Д., Каландарова Ф. К. Анализ протоколов безопасности, используемых для DDOS-АТАК. Типы и преимущества обновлённых протоколов безопасности // Universum: технические науки. 2025. № 4 (133). С. 55-58.

References

1. Asyanova S.R., Zhigalova Ya.I. Spoofing as a cybersecurity threat: concept, types, countermeasures // Journal of Monetary Economics and Management. 2024. No. 11. P. 242-247.
2. Methods of protecting traffic from interference by DPI systems of universities based on DoH and DoT protocols / V. V. Figurchikov [et al.] // Education Management: Theory and Practice. 2022. No. 6/12. P. 133-142.
3. Polyanskaya M.S. Analysis of approaches to attack detection in encrypted traffic // Modern Information Technologies and IT Education. 2021. Vol. 17, No. 4. P. 922-931.
4. Radivilova T. A., Bushmanov V. S. Analysis of main attacks on DNS servers and methods of using DNSSEC for DNS server protection // Technological Audit and Production Reserves. 2013. No. 2/1(10). P. 16-19.

5. Uralov D., Kalandarova F. K. Analysis of security protocols used for DDoS attacks. Types and advantages of updated security protocols // Universum: Technical Sciences. 2025. No. 4 (133). P. 55-58.