

С новой спецификацией TLS 1.3 шифрование в Интернете станет надежнее

Организация Internet Engineering Task Force (IETF), которая отвечает за создание стандартов и правил, регулирующих Интернет, [одобрила](#) спецификацию TLS 1.3. Новая версия протокола Transport Layer Security позволит повысить безопасность передачи данных.

За четыре года обсуждения спецификации был принят только 28-й вариант документа. Согласно заключению IETF, версия TLS 1.3 позволит клиентским и серверным приложениям "общаться через Интернет таким образом, чтобы предотвратить вмешательство с целью прослушивания и фальсификации сообщений".

В спецификации приводится механизм взаимодействия в рамках соединений по протоколу HTTPS, посредством которого клиент и сервер взаимодействуют друг с другом в Интернете. Наиболее заметным изменением стал отказ от устаревших алгоритмов шифрования и хэширования SHA-224 и MD5. Они были заменены более сложными альтернативами, включая ChaCha20, Poly1305, Ed25519, x448 и x25519.

Кроме того, TLS 1.3 предусматривает снижение времени взаимодействия между клиентом и сервером за счет уменьшения задержки соединения. В прошлом для HTTPS-запросов это было проблематичным. Также TLS 1.3 вводит режимы TLS False Start и Zero Round Trip Time (0-RTT), предназначенные для ускорения работы хост-серверов при обращении клиентов, с которыми в прошлом уже были совершены взаимодействия.

В целом, TLS 1.3 должен стать радикальным шагом для повышения безопасности интернета по сравнению с предыдущей спецификацией десятилетней давности. В отличие от предыдущих версий она обеспечивает лучшую защиту, например, при использовании злоумышленниками так называемой "Downgrade Attack" (атаки, цель которой перевод системы на использование более уязвимых протоколов, поддержка которых осуществляется для совместимости со старыми решениями).

Именно последнее обстоятельство стало причиной давления на IETF со стороны финансовых компаний, которые просили оставить возможность использовать предыдущие протоколы для внутренних сетей. Однако члены группы отклонили это предложение, сообщив, что любые исключения поставят под удар всю систему безопасности.

"Область, вокруг которой [зафиксировано](#) наибольшее количество споров, касалась включения режима 0-RTT, который имеет другие свойства безопасности, нежели остальная TLS".

Основные веб-браузеры, включая Chrome, Edge, Firefox, Safari, Opera и Vivaldi, скорее всего, поддержат стандарт, представив соответствующие обновления в ближайшие недели.