УДК 004.056.53

ОБЗОР И АНАЛИЗ МЕХАНИЗМОВ АУТЕНТИФИКАЦИИ В ЭКСПЕРИМЕНТАЛЬНЫХ ВЕРСИЯХ ПРОТОКОЛА TLS

Голованов А. А. (Университет ИТМО)
Научный руководитель – д. т. н., доцент Беззатеев С. В.
(Университет ИТМО)

Введение. TLS (бывший SSL) – протокол безопасного клиент-серверного соединения, обеспечивающий конфиденциальность и целостность данных, а также аутентификацию сторон. Протокол имеет богатую историю версий от самого первого, SSL 1.0, до актуального, TLS 1.3, с каждым обновлением устранялись открываемые уязвимости. Тем не менее, в новейшей версии TLS 1.3 механизмы аутентификации и обмена ключом всё ещё уязвимы к атаке квантовым вычислителем, и необходим переход к использованию постквантовых криптографических алгоритмов. Этот переход связан с проблемами таких алгоритмов: относительная новизна; значительные длины ключей и шифртекстов и время исполнения. В связи с этим стоит задача разработки новой версии TLS, которая учитывает данные проблемы.

Основная часть. Данная работа состоит в обзоре и анализе механизмов аутентификации, использованных в существующих экспериментальных версиях протокола TLS. Среди рассмотренных протоколов:
1) реализация The Open Quantum Safe Project [1], включающая в себя несколько различных постквантовых алгоритмов и совмещающая их с классическими алгоритмами в гибридном режиме;
2) CECPQ2, разработанный компанией Google [2];
3) реализация KEMTLS [3], ставящая своей задачей кардинально пересмотреть механизм аутентификации протокола TLS.
Проведено сравнение по таким параметрам, как: вычислительная эффективность, гибкость и прочие. В сравнение включена также актуальная версия протокола TLS 1.3 [4].

Выводы. Проведён сравнительный анализ существующих решений. Результаты работы предполагается использовать в дальнейших разработках, а также при принятии решений по использованию протокола в зависимости от прикладной задачи.

Список использованных источников:

1. TLS | Open Quantum Safe // The Open Quantum Safe Project URL: https://www.imperialviolet.org/2018/12/12/cecpq2.html (дата обращения: 12.12.2022).
2. CECPQ2 // ImperialViolet URL: https://www.imperialviolet.org/2018/12/12/cecpq2.html (дата обращения: 10.01.2023).
3. P. Schwabe, D. Stebila, T. Wiggers Post-Quantum TLS Without Handshake Signatures // Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20). – New York, NY, USA: Association for Computing Machinery, 2020. – С. 1461–1480.
4. RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3 // Datatracker URL: https://datatracker.ietf.org/doc/html/rfc8446 (дата обращения: 10.12.2022).

Голованов А. А. (автор) Подпись

Беззатеев С. В. (научный руководитель) Подпись