АНАЛИЗ РАСШИРЕНИЙ ПРОТОКОЛА TLS

А.С. Касьян

Основное назначение протокола TLS – организация защищенных соединений по незащищенной сети. Этот протокол характеризуется следующими свойствами, которые обуславливают его преимущества по сравнению с аналогом (протоколом SSL):

- совместимость (возможность разрабатывать программное обеспечение и библиотеки, которые могут взаимодействовать друг с другом с использованием общих криптографических параметров);

- расширяемость (возможность перехода от криптографических примитивов одного вида к криптографическим примитивам другого вида без необходимости создания новых протоколов);

- эффективность (возможность обеспечения использования протокола при приемлемых затратах на производительность информационной системы).

В настоящее время существуют следующие расширения протокола TLS, с помощью которых можно обеспечивать дополнительные его преимущества: Certificate Transparency, Server Name Indication, Session Ticket, Online Certificate Status Protocol (OCSP) stapling.

Использование расширения Certificate Transparency создает условия для совершенствования инфраструктуры открытых ключей в информационной системе путем ведения учета всех сертификатов общедоступных серверов. При использовании этого расширения центр сертификации при выпуске сертификата отправляет его на общедоступный сервер журналирования, а в ответ получает подписанное электронной цифровой подписью подтверждение внесения информации о сертификате в журнал, называемое Signed Certificate Timestamp.

Использование расширения Server Name Indication предоставляет клиенту возможность указать имя сервера, с которым он хочет установить соединение. Данное расширение обеспечивает поддержку виртуальных защищенных серверов в случае, когда одному IP-адресу соответствует несколько сайтов, каждый из которых имеет свой сертификат.

Использование расширения Session Ticket создает условия для сокращения продолжительности процесса «рукопожатия» между клиентом и сервером, что обусловлено исключением необходимости хранения на сервере информации, требуемой для возобновления ранее завершенного соединения за счет того, что сервер перенаправляет эту информацию клиенту, предварительно зашифровав ее. Такая информация называется «Session Ticket». При необходимости возобновления соединения клиент передает Session Ticket серверу, сервер расшифровывает эту информацию, проверяет ее на предмет целостности и далее использует ее для восстановления соединения.

Расширение OCSP представляет собой протокол, с использованием которого приложения определяют состояние отзыва запрашиваемых сертификатов. Сертификат может быть отозван в случаях нарушения его безопасности (например, компрометация приватного ключа сервера) или истечения его срока действия.

Исходя из результатов проведенного анализа расширений протокола TLS, можно заключить, что эти расширения представляются рациональными для использования в ходе реализации мероприятий по повышению эффективности процессов, направленных на защиту информации, циркулирующей в информационных системах.