АНАЛИЗ ПРОЦЕДУР И МЕХАНИЗМОВ БЕЗОПАСНОСТИ ПРОТОКОЛА SIP

В.Ю. ШЕВЦОВ, М.Ю. ХОМЕНОК

SIP-сети подвержены различного рода угрозам, обусловленным особенностями взаимодействия элементов сети по протоколу SIP, такими как использование посредников, сложность или отсутствие доверительных отношений между узлами, работа в режиме пользователь-пользователь. Для обеспечения безопасности с учетом всех особенностей SIP, требуются отдельные механизмы, применимые к различным аспектам протокола. Исходя из типов угроз, которым подвержен протокол SIP, и решения задач по сохранению конфиденциальности и целостности сообщений, предотвращению атак воспроизведения или получения доступа к сообщению путём фальсификации, обеспечению аутентификации и анонимности участников сессии, тела SIP-сообщений требуют применения служб безопасности, обеспечивающих конфиденциальность, целостность и аутентификацию.

SIP-безопасность можно улучшить на основе возможностей, поддерживаемых протоколами TCP/IP, используя протокол защиты транспортного уровня TLS (Transport Layer Security) или набор протоколов (IPSec-IP Security) для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяющих осуществлять подтверждение подлинности и/или шифрование IP-пакетов путем обмена ключами для обеспечения аутентификации и шифрования между SIP компонентами.

Защищенный вариант протокола SIP — SIPs основан на обеспечении безопасности средствами транспортного уровня, работающего поверх протоколов, ориентированных на соединение (TCP). TLS предоставляет возможности аутентификации и безопасной передачи данных через IP-сеть с использованием криптографических средств. При этом часто происходит лишь аутентификация сервера, в то время как клиент остается неаутентифицированным. Для взаимной аутентификации каждая из сторон должна поддерживать инфраструктуру открытого ключа, которая позволяет защитить клиент-серверные приложения от перехвата сообщений, редактирования существующих сообщений и создания поддельных.

Не менее важной проблемой является так же защита от атак на компоненты сети SIP, при которых создаются условия, что легитимные пользователи не могут получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ становится затруднённым. В докладе

рассматриваются особенности от защиты от DoS-атак (Denial-of-Service — отказ в обслуживании) с учетом возможностей анализа характеристик SIP- и медиа-трафика.