Риск отправки поддельных данных может быть реализован с помощью атак на сетевой приложение на сервере, а также с помощью манипуляции данных передаваемых мобильному приложению для последующей отправки.

АУДИТ БЕЗОПАСНОСТИ ТРАФИКА В СИСТЕМЕ IP-ТЕЛЕФОНИИ

Д.В. Куприянова, Д.Н. Одинец

Протоколы SIP и RTP, используемы для передачи медиа данных, были разработаны без учета необходимости защищать передаваемую информацию, в следствии чего возможны следующие виды атак и уязвимостей: фрод звонков, вирус, попавший в сеть IP-телефонии может начать рассылать спам ее абонентам, нарушение звонков – атакующий рассылает пакеты клиентам звонка, DoS – за счет отправки большого количества сообщений «Invite» и «Registrer» нарушается работу компонентов SIP, атакующий прослушивает весь трафик в IP-телефонии, подбор паролей, Man-In-The-Middle – атакующий проникает в звонок между пользователями, и может не только прослушивать, но и изменять сообщения между клиентами.

Для защиты передаваемы данных, предлагается использовать протокол TLS – протокол защиты транспортного уровня. Данный протокол использует асимметричное шифрования для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений. Также для защиты данных может быть использован IPsec – набор протоколов для обеспечения защиты данных, передаваемых по протоколу IP, обеспечивающих аутентификацию, проверку целостности и/или шифрование IP-пакетов. В отличие от IPSec, TLS протокол реализуется на транспортном уровне и не требует поддержки на промежуточных устройствах.

Для улучшения защиты может быть использован VPN. В случае невозможности использования VPN, необходимо использовать VLAN. Данные решения создают виртуальную сеть, что позволяет передавать данные в надежных сетях.

В данном случае лучшим выбором будет использование VPN который позволяет шифровать данные, так как в этом случае нет необходимости реализации шифрования на клиентах, отсутствует риск ошибок в реализации шифрования, VPN может быть обновлен для использования более современных методов шифрования без необходимости обновления кода клиента [1–3].

Список литературы

1. Security in a SIP network: Identifying network attacks [Электронный ресурс]. URL: https://searchunifiedcommunications.techtarget.com/feature/Security-in-a-SIP-network-Identifying-network-attacks (дата обращения: 05.04.2019).

2. How to Address WoIP Security Challenges [Электронный ресурс]. URL: http://www.centurylinkbrightideas.com/how-to-address-voip-security-challenges/ (дата обращения: 05.04.2019).

3. SIP Server Security with TLS: RPE [Электронный ресурс]. URL: https://www.researchgate.net/publication/235601569_SIP_Server_Security_with_TLS_Relative_Performance_Evaluation (дата обращения: 05.04.2019).

СПОСОБЫ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Д.В. Куприянова, Д.Ю. Перцев

Анализ ситуации, проведенный BSA Global Software Survey [1], показывает, что рынок нелицензионного ПО уменьшается, однако по состоянию на 2018 г. составляет 37 % и оценивается более чем в 46 млрд. долларов. С учетом этого проблема защиты авторских прав по-прежнему является актуальной. К основным способам защиты ПО относится: лицензионный ключ, жесткая привязка к носителю информации, USB-ключ. Лицензионный ключ является самым простым способом защиты и предполагает генерацию ключа по некоторому шаблону с привязкой к имени пользователя или аппаратной конфигурации системы. Основным