УДК 004.056.55

ПОДСИСТЕМА ЗАЩИТЫ ДАННЫХ ОНЛАЙН-КОНСУЛЬТАНТА ПРИ ИХ ПЕРЕДАЧЕ В СЕТЯХ ДОСТАВКИ КОНТЕНТА

И.Е. Пехов (Университет ИТМО, Санкт-Петербург)
С.В. Савков (Университет ИТМО, Санкт-Петербург)
Научный руководитель - И.Б. Бондаренко (Университет ИТМО, Санкт-Петербург)

Достаточно большое количество задач современный человек решает с помощью Интернета: развлекается, совершает покупки, управляет финансами. В процессе того или иного дела он может столкнуться со сложностями в работе с системой, либо выбора наиболее подходящего товара или услуги, с чем ему могут помочь владельцы или администраторы этих Интернет-сервисов. Но такой стандартный способ связи как электронная почта не удовлетворяет требованиям к скорости решения проблем посетителей ресурса. Именно эту задачу, задачу оперативного контакта между компанией и клиентом, и решают системы Онлайн-консультирования. По данным исследования агентства Oneupweb [1], для целой трети посетителей Интернет-магазинов и других веб-сервисов важно наличие подобной системы на используемом ресурсе. При этом в большинстве случаев нагрузка на сервис консультирования пропорциональна нагрузке на основной ресурс, а значит, сервис онлайн-консультирования является высоконагруженным на популярном ресурсе.

Одним из решений проблемы высоких нагрузок на сервер является применение систем CDN (сетей доставки контента) [2], которые позволяют оптимизировать доставку и содержимого конечным пользователям. Но полная интеграция со сторонней инфраструктурой, предполагающая передачу информации этому сервису, поднимает новые вопросы о сохранении конфиденциальности информации. Безусловно, на путях «сервер-CDN» и «CDN-клиент» ее можно обеспечить с помощью криптографического протокола TLS. Но насколько мы можем доверять самим подобным системам в вопросах конфиденциальности и целостности информации?

В рамках нашей работы мы предлагаем решение этой проблемы с помощью применения ассиметричного шифрования между сервером сервиса онлайн-консультирования и клиентом. Используются ключи RSA длиной 2048-бит. Для обмена открытыми ключами применяется защищенный TLS [3] канал, минуя сервис CDN - напрямую между сервером и клиентом. Закрытые ключи сервера и посетителя хранятся в базах данных онлайн-консультанта и Интернет-сервиса соответственно. Поскольку для Интернет-ресурса, на котором установлен онлайн-консультант, общение между консультантом и посетителем должно происходить наиболее прозрачно, то на стороне клиента шифрование будет производиться силами веб-браузера. Со стороны консультанта шифрование будет осуществляться на стороне сервиса. Конфиденциальность достигается за счет шифрования с помощью открытого ключа собеседника, а целостность – за счет подписи с помощью своего закрытого ключа.

Таким образом, наряду с повышением доступности сервиса с помощью CDN, передаваемая информация обладает конфиденциальностью и целостностью за счет применения ассиметричного шифрования.

Список литературы

1. Российская газета // Ответят на все вопросы [Электронный ресурс] – Режим доступа: https://rg.ru/2013/02/05/konsultacii.html, свободный (27.02.2019).
2. Как сделать CDN для своего сайта и почему это полезно для высоконагруженных проектов // Хабр [Электронный ресурс] – Режим доступа: https://habr.com/ru/company/sports_ru/blog/198598/, свободный (27.02.2019).
3. World Wide Web Consortium (W3C) // WebID-TLS [Электронный ресурс] – Режим доступа: https://www.w3.org/2005/Incubator/webid/spec/tls/, свободный (27.02.2019).