УДК 004.75

МЕТОДЫ АУТЕНТИФИКАЦИИ ДЛЯ СИСТЕМЫ ГОРИЗОНТАЛЬНОГО МАСШТАБИРОВАНИЯ НА УСТРОЙСТВАХ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ

Антонов М.А. (Университет ИТМО),
Кореньков Ю.Д. (Университет ИТМО)
Научный руководитель – к.т.н., Кореньков Ю.Д.
(Университет ИТМО)

Вопрос безопасности пользовательских данных - неотъемлемая часть проектирования любой современной системы. Особенно важно уделить ей достаточное внимание при разработке инфраструктурного программного обеспечения, выступающего фундаментом для многопользовательских систем. Так, при реализации системы горизонтального масштабирования, функционирующей на устройствах конечного пользователя, необходимо обеспечить безопасное подключение и идентификацию этих устройств, а также аутентификацию самого пользователя.

Взаимодействие прикладных приложений, выполняющихся на пользовательских устройствах под управлением разрабатываемой системы горизонтального масштабирования, осуществляется посредством специальной службы-супервизора, обеспечивающей возможность удалённого вызова процедур между различными устройствами. Безопасность каналов передачи данных при этом достигается за счёт использования TLS-соединений между службами-супервизорами, выступающими в роли узлов распределённой системы. Управление сертификатами осуществляется автоматически на основе профилей, ассоциированных либо с конечным устройством, либо с пользователем, использующим несколько устройств.

Автоматизация управления пользовательскими профилями требует возможности осуществления безопасной аутентификации и идентификации устройств в двух ситуациях: при первичном подключении нового устройства к распределённой системе, что спряжено с передачей на новое устройство информации о известных профилях, и при вторичных подключениях ранее задействованных устройств, в отсутствии пользовательского доступа к таким устройствам.

Устройства, подключённые к создаваемой системе горизонтального масштабирования, разделяющие владение информацией о профиле некоторого пользователя, рассматриваются как члены приватной вычислительной сети данного пользователя. При этом они могут быть подключены к одной локальной сети, к различным локальным сетям, а также быть подключёнными к разным сетям в разные моменты времени. Глобальная доступность обеспечивается за счёт автоматического выбора предпочтительного маршрута и абстракции логического канала передачи данных между узлами системы от транспортного соединения, осуществляемого посредством прямых соединений в локальных сетях, или посредством подобного чесночному шифрованию механизма с использованием глобальной p2p-сети.

При проектировании разрабатываемой системы были выделены два принципиально разных сценария аутентификации: при наличии возможности прямой передачи между доступными пользователю устройствами информации, необходимой для установления безопасного соединения, и при отсутствии такой возможности. В состав блока информации, называемого файлом-приглашением, необходимого для установления безопасного соединения, входят идентификатор узла в распределённой системе, список конечных точек для подключения и токен запроса аутентификации с цифровой подписью, являющийся обязательным реквизитом для первичного подключения.

В данных условиях были разработаны два метода аутентификации:
С передачей файла-приглашения между известным и подключаемым к системе устройством посредством QR-кода, Bluetooth, NFC или вручную пользователем в виде зашифрованного файла.

Посредством DHT (распределённой хэш-таблицы), встроенной в p2p-сеть, узлами которой являются службы-супервизоры. Если первый метод недоступен в силу физической удалённости или ограничений связи между устройствами, задействуется второй способ, при котором зашифрованный файл-приглашение помещается в DHT, а в качестве основы для одноразовых ключа доступа и ключа шифрования применяется пара из пользовательского пароля и числа, сгенерированного криптографически стойким генератором. Кроме этого, во всех случаях после установления безопасного логического соединения с впервые подключаемым к системе устройством, процедура аутентификации дополнительно включает подтверждение с помощью динамического одноразового пин-кода. Только после этого на подключаемое устройство передаётся информация о соответствующем пользовательском профиле, существующем в системе, после чего оно становится участником соответствующей приватной вычислительной сети, используемой для горизонтального масштабирования.

Таким образом, в результате работы были разработаны два различных метода аутентификации для системы горизонтального масштабирования, функционирующей на устройствах конечного пользователя. При этом модульность системы позволяет использовать и другие методы аутентификации, например, на основе внешних служб двухфакторной аутентификации, таких как Google Authenticator или Microsoft Authenticator.

Список использованных источников:

1. Telegram Open Network / Dr. Nikolai Durov. https://ton.org/ton.pdf (23.11.2022).
2. Hook, David. Beginning Cryptography with Java. Германия: Wiley, 2005.
3. Oppliger R. SSL and TLS: Theory and Practice. – Artech House, 2023.

Антонов М.А. (автор) Подпись

Кореньков Ю.Д. (научный руководитель) Подпись