УДК 004.021

РАЗРАБОТКА МЕТОДИКИ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ В СИСТЕМЕ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПА С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКОГО СКАНЕРА МОБИЛЬНОГО УСТРОЙСТВА

Алибутаев А.К. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Научный руководитель – к.т.н., доцент Левко И.В.

(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

В данной работе рассматривается способ снижения рисков получения несанкционированного доступа к прикладной системе администрирования системы контроля и управления доступом (СКУД). Предложенное решение направлено на повышение уровня доверия к результату аутентификации и идентификации путем увеличения количества факторов аутентификации и требований, предъявляемых к ним, в системе.

Введение. Актуальность проблемы обусловлена высоким значением СКУД в обеспечении безопасности и пропускного режима организации. Компрометация пароля одного из сотрудников или получение злоумышленником доступа к информационной системе с актуальным ключом сессии может привести к утечке информации, ослаблению существующих правил доступа или отключения отдельных модулей. Необходимость повышения уровня доверия к аутентификации и идентификации обусловлена возможностью создания нескольких ролей с различными правами доступа. Так, внутренний злоумышленник, являющийся оператором или сотрудником, производящим обслуживание помещений, может получить доступ к СКУД выше имеющихся у него прав. Популярные СКУД, используемые в России (“Castle”, “Sigur”, “RusGuard”) не предоставляют возможности настройки или добавления нескольких факторов для аутентификации оператора.

Основная часть. Для решения поставленной проблемы предлагается использовать разработанное мобильное приложение (мобильный клиент) для прохождения вторичной идентификации оператора. Для этого необходимо при регистрации сотрудника в качестве оператора СКУД ассоциировать аккаунт с идентификатором его смартфона, полученным при первой инициализации мобильного клиента. При этом к среде запуска приложения предъявляется требование наличия механизма разблокировки смартфона и подтверждения операций при помощи биометрического сканера, установленного в смартфон. Данное требование обусловлено необходимостью подтверждения владения устройством в момент прохождения второго этапа аутентификации.

После прохождения первичной идентификации на стационарном клиенте при помощи пары логин-пароль сервер генерирует уникальный секрет, после чего отправляет мобильному клиенту уведомление о необходимости прохождения вторичной идентификации. При запуске приложение запрашивает подтвердить вход отпечатком пальца, сохраненным в операционной системе мобильного устройства. После успешного подтверждения мобильным клиентом осуществляется запрос на получение ключа. Далее, на основании ключа и текущего Unix-времени вычисляется код аутентификации HMAC, который отправляется на сервер. Если HMAC, полученный с мобильного клиента совпадает с вычисленным на сервере, то процедура аутентификации считается успешно пройденной.

Выводы. Использование предложенной методики и программного решения за счет низкой стоимости реализации и быстроте внедрения может применяться организациями для повышения уровня доверия к результату аутентификации и идентификации в СКУД.

Алибутаев А.К. (автор)

Левко И.В. (научный руководитель)