A. Y. Iskhakov

Two-Factor Authentication System based on QR-Codes

Keywords: authentication, one-time passwords, tokens, Quick Response codes

The opportunity of two-factor authentication usage in the control systems and access management on the basis of Quick Response codes with one-time passwords is analyzed in the work. The mobile application is proposed to use as a software token.

А. Ю. Исхаков

СИСТЕМА ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ QR-КОДОВ

Введение

На сегодняшний день вектор развития рынка систем контроля и управления доступом (СКУД) [1] однозначно направлен на снижение влияния человеческого фактора на процесс обеспечения пропускного режима на объектах. Это обусловило и развитие систем, использующих многофакторную аутентификацию. Системы подобного рода традиционно применяются в пропускных пунктах режимных объектов, где вопрос удобства и времени аутентификации пользователей не является определяющим в построении системы защиты.

Между тем на многих объектах с большим количеством посетителей продолжительность процедуры аутентификации пользователей является важным критерием. Использование технологии бесконтактных карт доступа в совокупности с визуальной проверкой охранником-контролером обеспечивает максимально оперативное время проведения аутентификации.

Недостатком такого подхода является принцип передачи статичного идентификатора. Злоумышленник, скомпрометировав статичный идентификатор карты, может воспользоваться большим потоком посетителей и пройти через контрольно-пропускной пункт как легальный пользователь. Таким образом, возникает необходимость разработки системы аутентификации на основе современных признаков.

1. Предлагаемая схема аутентификации

Принцип рассматриваемого механизма двухфакторной аутентификации основан на использовании мобильного устройства связи (смартфон или коммуникатор) в качестве носителя пользовательского идентификатора.

Проблему защиты от копирования идентификатора предлагается решить посредством технологии одноразовых паролей [2], которые могут быть использованы лишь однократно и характеризуются ограниченным временем действия. Аппаратные возможности большинства современных телефонов позволяют реализовать программный генератор одноразовых паролей в качестве резидентной программы.

В качестве второго фактора аутентификации предлагается использовать метод графических паролей. Он позволяет защитить мобильное приложение от несанкционированного доступа в случае потери или кражи мобильного устройства. После проведенного анализа существующих технических решений в разрабатываемую систему аутентификации было решено внедрить модифицированный графический пароль типа «Лабиринт». Суть модернизации заключается в сокрытии следов на экране путем принудительного требования обвести одним касанием все точки обхода.

По сравнению с аппаратными реализациями системы аутентификации предлагаемый вариант обладает следующими преимуществами:

1) для организации не требуется оснащение пользователей смарт-картами [3] или аппаратными токенами. Снижение финансовых затрат;

2) пользователь избавляется от необходимости носить с собой дополнительный предмет-идентификатор (токен, смарт-карту). Мобильные устройства являются наиболее распространенным средством связи, которым пользуется подавляющее большинство людей;

3) частое использование телефона повышает вероятность быстрого обнаружения кражи или потери токена.

2. Коммуникация сервера и клиентских устройств

На рис. 1 в общем виде представлена схема аутентификации с использованием мобильного средства связи в качестве генератора одноразовых паролей.

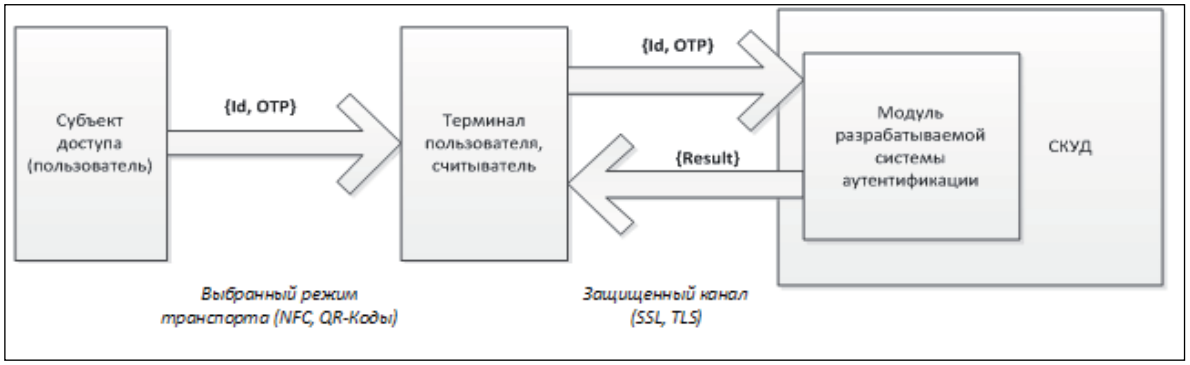

Рис. 1. Предложенная схема аутентификации

В качестве одного из вариантов реализации транспорта для аутентификационной информации между мобильным устройством и считывателем предлагается использовать технологию QR (quick response) кодов [4]. В данном случае система представляет собой программно-аппаратный комплекс, включающий персональный компьютер, видеокамеру (используется в качестве считывателя) и программное обеспечение для работы системы, включающее модули интеграции с распространенными СКУД.

Согласно спецификации ISO/IEC 18004 QR, в QR-коде может быть закодировано более 2 Кб текста, что является приемлемой длиной ключа для современных криптографических алгоритмов. Для коррекции ошибок QR-коды используют алгоритм Рида — Соломона (Reed — Solomon) [5]. Это позволяет применять мобильные устройства со значительными царапинами и сколами на дисплее. Предусмотрено 4 уровня коррекции ошибок, которые различаются количеством информации для восстановления и соответственно количеством полезной информации, которую можно восстановить при повреждении кода. Уровням коррекции соответствует следующий объем информации, которую можно восстановить: L — 7 %, M — 15 %, Q — 25 %, H — 30 %.

В качестве альтернативного способа передачи данных от мобильного устройства к считывателю предлагается использовать технологию беспроводной высокочастотной связи малого радиуса действия NFC [6]. При оценке применимости данной технологии в качестве транспорта аутентификационных данных выделяется важное преимущество в удобстве использования. В отличие от систем штрих-кодов или каналов передачи данных общего пользования (Wi-Fi, Bluetooth) в случае применения NFC система аутентификации характеризуется очень коротким временем для установки соединения. Вместо выполнения инструкций по согласованию для идентификации устройства связь между двумя устройствами NFC устанавливается моментально (менее чем за одну десятую секунды).

При реализации режима NFC с применением активного режима связи предпочтительнее использовать метод генерации одноразовых паролей «Запрос-ответ». В данном режиме динамической составляющей является случайный вопрос, который сервер генерирует на каждое обращение. Именно этот вопрос подвергается шифрованию аппаратом пользователя, в дальнейшем позволяя осуществить проверку аутентичности субъекта доступа. Данная схема позволяет избавиться от проблемы рассинхронизации, однако на практике требует наличия активных NFC-модулей в устройствах абонентов.

3. Алгоритм работы

Для использования мобильного устройства в качестве идентификатора его необходимо зарегистрировать в системе. Для этого требуется включить режим синхронизация времени и поднести смартфон к камере-считывателю. Клиентская программа отобразит на дисплее QR-код с текущим временем. Сервер вычислит и сохранит значение смещения времени мобильного устройства относительно эталонного в базе данных.

После этого необходимо провести процедуру согласования ключевой пары. Основу для секретного ключа k составляют следующие компоненты:

- численное значение графического пароля g для запуска приложения. В памяти смартфона хранится хэш-значение $g`$;
- ключевая пара n (набор из некоторых «заводских» параметров мобильного устройства, которые будут опрашиваться аппаратом при каждой генерации временного пароля). Привязка к физическим характеристикам является дополнительным рубежом защиты от полного копирования памяти мобильного устройства;
- случайный набор бит b, который сохраняется в скрытой области памяти мобильного устройства.

Далее вычисляется хэш-свертка от перечисленных компонентов. Из полученного значения в соответствии с выбранным асимметричным алгоритмом формируется закрытый ключ. Например, осуществляется выделение n символов из строки или преобразование к ближайшему простому числу. В соответствии с используемым алгоритмом вычисляется значение открытого ключа, которое передается на сервер аутентификации.

Как и в случае с синхронизацией времени, процедура согласования ключа происходит путем считывания с дисплея QR-кода. Этот этап занимает несколько секунд и не требует дополнительных устройств и доступа к сетям передачи данных.

Получение QR-кода для аутентификации описывается функцией F:

$$F(u, p, t) = Q[u * E_{R[H(p)\ l]}(u \oplus t)],$$

где u — идентификатор пользователя;

ρ — набор из компонентов секретного ключа;

t — текущая временная метка;

$Q(x)$ — операция преобразования сообщения x в QR-код;

$*, \oplus$ — операции конкатенации с некоторыми разделителями;

$Ek(x)$ — операция шифрования сообщения x на ключе k;

$R(x,y)$ — операция формирования секретного ключа из входной строки x в соответствии с набором требований y, предъявляемых к секретному ключу в используемом режиме шифрования;

$H(x)$ — операция хэширования строки x;

l — набор требований, предъявляемых к секретному ключу в используемом режиме шифрования.

После считывания пользовательского QR-кода (сообщение M) осуществляется его декодирование Q` и дальнейшее разбиение Array на массив из двух элементов (идентификатор пользователя и значение пароля):

$$F`(M) = Array[Q`(M)].$$

Далее происходит операция проверки подлинности, описываемая функцией P:

$$P[t, D_{S(array[0])}(array[1])] \rightarrow \{0,1\},$$

где t — время жизни одноразового пароля;

$Dk(x)$ — операция расшифровывания сообщения x на ключе k;

$array[0]$ — идентификатор пользователя;

$array[1]$ — значение пароля;

$S(x)$ — операция получения открытого ключа $k2$ по пользовательскому идентификатору x из базы данных.

В случае успешного расшифрования значения одноразового пароля система сверяет текущее время с временным штампом пароля. Если разница не превышает установленный интервал t, то в СКУД передается управляющее воздействие на пропуск субъекта доступа.

Компоненты системы, реализующие основной функционал процедуры аутентификации, представлены на рис. 2.

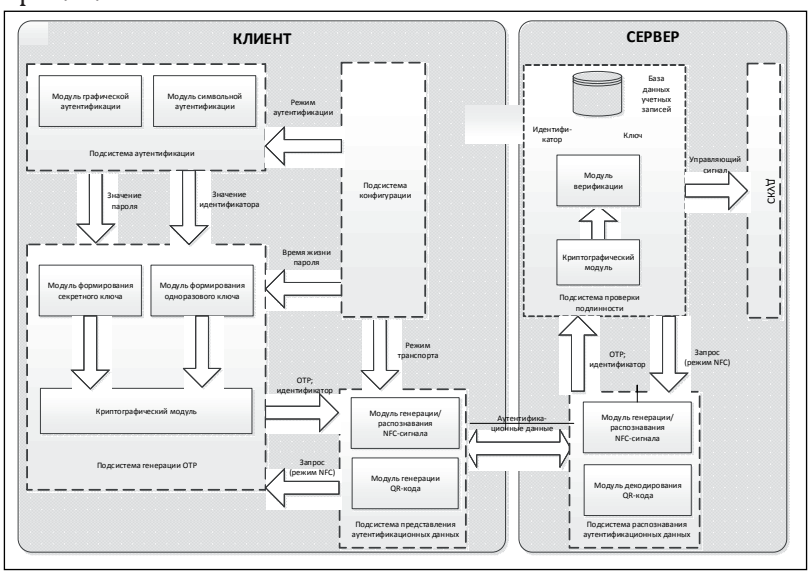

Рис. 2. Предложенная схема аутентификации

Заключение

В рамках разработки системы аутентификации был предложен подход, заключающийся в использовании в качестве транспорта аутентификатора субъекта доступа технологии QR-кодов или беспроводной высокочастотной связи малого радиуса NFC. Обе технологии позволяют построить защищенную модель процесса передачи аутентификатора и реализовать ее без внедрения дополнительных физических устройств-идентификаторов.

Отличительной особенностью подхода является отсутствие ограничений на выбор устройства в рамках одной категории мобильных средств. Для повышения степени унификации и расширения круга потенциальных потребителей было принято решение реализовать оба режима транспорта данных. Таким образом, ограничения на используемые средства мобильной связи сводятся к минимуму.

Применение модернизированного пароля типа «Лабиринт» позволяет внедрить в систему второй фактор аутентификации. Были учтены основные условия и ограничения, накладываемые на парольную систему для приложений подобного рода. Однако для исключения ограничений в виде наличия сенсорного экрана у мобильных устройств сотрудников организации должен быть реализован альтернативный способ аутентификации по текстовому паролю.

Предлагаемый подход позволяет не только повысить степень защищенности системы аутентификации [7], но и решить проблему эргономичности использования традиционных электронных пропусков без необходимости применения многочисленных организационных мер. На данном этапе реализован прототип системы аутентификации, включающий:

- методику аутентификации для использования в электронных проходных;
- алгоритмы аутентификации в зависимости от выбранного режима транспорта данных;
- опытный образец клиентской и серверной части системы, основанный на передаче QR-кодов.

СПИСОК ЛИТЕРАТУРЫ:

1. Электронные проходные [Электронный ресурс] // SOTOPS. M., 2013. URL: http://sotops.ru/catalog/elektronnye-prohodnye-Perco (дата обращения: 30.04.2013).
2. Аутентификация. Теория и практика обеспечения доступа к информационным ресурсам: учеб. пособие для вузов / Под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. М.: Горячая линия–Телеком, 2009. – 552 с.
3. *Сабанов А. Г.* Основные процессы аутентификации // Вопросы защиты информации. 2012. № 3. С. 54–57.
4. QR код [Электронный ресурс] // Next Generation Codes. M., 2008–2013. URL: http://www.qrcc.ru/qrcode.html (дата обращения: 30.04.2013).
5. QRP: An improved secure authentication method using QR codes 2013. URL: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/14761/6/dpintorTFM0612memoria.pdf (дата обращения: 15.04.2013).
6. *Громов Д., Кузнецов И.* Технология NFC и перспективы ее использования на транспорте [Электронный ресурс] // Нова Кард. Н. Новгород, 2013. URL: http://www.novacard.ru/ru/actual/?id=850 (дата обращения: 01.04.2013).
7. *Ходашинский И. А., Савчук М. В., Горбунов И. В., Мещеряков Р. В.* Технология усиленной аутентификации пользователей информационных процессов // Доклады ТУСУР. 2011. № 2 (24). С. 236–248.

REFERENCES:

1. Elektronnie proxodnie [Elektronniy resurs] / SOTOPS. – Elektron. dan. – M., 2013. – URL: http://sotops.ru/catalog/elektronnye-prohodnye-Perco (data obrasheniay: 30.04.2013).
2. Autentifikatsiya. Teoriay I praktika obespecheniay dostupa k informatsionnim resursam : ucheb. Posobie dlay vuzov / pod red. A. A. Shelupanova, S. L.Gruzdeva, Y. S. Nahaeva, M.: Goraychay liniay – Telekom, 2009. – 552 p.
3. *Sobanov A. G.* Osnovnie protsessi autentifikatsii / A.G. Sabanov // Voprosi zashiti informatsii – 2012. № 3. P. 54–57.
4. QR code [Elektronniy resurs] // Next Generation Codes. Elektron. dan. [M.], 2008–2013. – URL: http://www.qrcc.ru/qrcode.html (data obrasheniay: 30.04.2013).

5. QRP: An improved secure authentication method using QR codes [Electronic resource] — Electron data. [S. l.], 2013. URL: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/14761/6/dpintorTFM0612memoria.pdf (access date: 15.04.2013).
6. *Gromov D.* Tekhnologiay NFC b perspektivi ee ispolzovaniay na transporte [Electronic resource] / D.Gromov< I. Kuznetsov // Nova Kard. Elektron. dan. N.Novgorod, 2013. URL: http://www.novacard.ru/ru/actual/?id=850 (data obrasheniay: 01.04.2013).
7. *Shkodashinskiy I. A., Savchuk M. V., Gorbunov I. V., Meshayrikov R. V.* Teshknologiay usilennoy autentifikatsii polzovateley informatsionnishk protsessov // Dokladi TUSURa. 2011. № 2 (24). P. 236–248.