УДК 004.056.53

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ СТАНДАРТА EMV*

П.А. Вахрушев,
Пермский государственный национальный исследовательский университет;
ООО «Альтернатива»

Разработана компьютерная программа, предназначенная для реализации двухфакторной аутентификации пользователя при получении доступа к закрытой информации в СУБД. В качестве второго фактора аутентификации используется банковская карта стандарта EMV, описывающего инфраструктуру открытых ключей для банковских приложений.

Ключевые слова: *двухфакторная аутентификация, защита информации, EMV, банковские карты.*

1. Постановка проблемы

За довольно непродолжительный период времени информационная сфера совершила технологический рывок. Возросшая производительность персональной техники, возможность сохранять большие объемы данных, а также повсеместное подключение к высокоскоростной сети привели к распространению хранения важной информации в интернете.

Онлайн-приложения уязвимы к краже ценной информации, поскольку злоумышленники используют ошибки в механизме аутентификации пользователей для получения доступа к приватным данным [1].

Спектр данных, которые требуют защиты, довольно широк: сведения о сотрудниках и клиентах, номера банковских карт, информация о здоровье, финансовые документы, секреты производства [2].

В статье рассматриваются вопросы двухфакторной аутентификации пользователей с использованием смарт-карт формата EMV. Данный способ позволяет сократить затраты на стойкую аутентификацию, поскольку часть необходимого оборудования уже присутствует у сотрудников организаций. В то же время внедрение двухфакторной аутентификации существенно повышает защищенность информации.

2. Обзор существующих решений

Для проверки подлинности личности могут использоваться три различных типа информации:

– субъект знает;

– субъект имеет;

– часть субъекта.

Для надежной аутентификации эксперты рекомендуют использование более

* Исследование было проведено при содействии программы «УМНИК».

одного типа информации от субъекта. Например, таким сочетанием может быть секретная фраза и отпечаток пальца.

В настоящее время в организациях широко используются ключи iButton, eToken, смарт-карты и различные смс-сервисы. При этом стоимость внедрения готовых решений может оказаться довольно большой из-за необходимости разворачивания инфраструктуры публичных ключей и закупки необходимого оборудования.

3. Стандарт банковских карт с чипом EMV

EMV – Europay, MasterCard, Visa – международный стандарт для обеспечения инфраструктуры банковских карт с чипом [3, 4]. Стандарт определяет физическое, электронное и информационное взаимодействие между банковской картой и терминалом доступа. Существуют также стандарты для бесконтактных карт.

Стандарт полностью описывает инфраструктуру открытых ключей, применяемых для аутентификации держателя карты и проведения платежных транзакций. Инфраструктура гарантирует целостность, уникальность карты и подлинность личности владельца. Приведенные выше факторы позволяют использовать банковскую карту в качестве средства аутентификации в сторонних системах. Преимущества использования карт EMV для аутентификации пользователей [5]:

– каждый пользователь уже имеет такую карту, что снижает затраты на инфраструктуру;

– открытые стандарты;

– дешевизна считывателей смарт-карт;

– готовая инфраструктура публичных ключей.

4. Встроенные в EMV алгоритмы аутентификации [6]

SDA (Static Data Authentication) – алгоритм аутентификации по статичным данным. Он используется для проверки того, что данные, записанные на карте, действительны и никем не изменялись. Основан на вычислении цифровой подписи с помощью асимметричной криптографии. С помощью закрытого ключа эмитент подписывает важные данные на карте, а публичным ключом терминал проверяет эту подпись. Закрытый ключ эмитента сохраняется в секрете.

DDA (Dynamic Data Authentication) – алгоритм аутентификации по динамическим данным. При выполнении алгоритма карта подписывает изменяющиеся сессионные данные с помощью своего закрытого ключа. Сессионные данные генерируются терминалом и действуют только то время, пока карта находится внутри, что позволяет противостоять атакам копирования.

5. Упрощенный алгоритм аутентификации

Алгоритмы SDA и DDA являются надежными, но сложны в реализации, поскольку имеют различия для карт разных платежных систем.

Авторы предлагают упрощенный алгоритм аутентификации при помощи карты, в котором последняя используется как носитель ключевого материала. Схема основана на использовании HMAC для подписи сессионных данных и используется совместно с парольной защитой.

HMAC (Hash-based Message Authentication Code) – алгоритм генерации хешкода аутентификации сообщений. Алгоритм используется для проверки подлинности информации, передаваемой между двумя сторонами.

В качестве закрытого ключа используется значение криптографической хешфункции от всей публичной области памяти карты. Публичная область памяти уникальна для каждой карты.

Перед началом использования в базу данных сервера для определенного пользователя заносится закрытый ключ его карты.

Каждый сеанс сервер генерирует случайное число – сессионный ключ. Для прохождения аутентификации пользователю необходимо сгенерировать валидную HMAC-подпись для этих данных и переслать обратно серверу (рисунок).

Если подпись, принятая от клиента,

совпадает с подписью, сгенерированной сервером, то пользователь считается валидным.

6. Заключение

Механизм аутентификации был апробирован для СУБД Redis. Двухфакторная аутентификация осуществляется в два шага. Первый шаг – обычная аутентификация пользователя с получением сессионного ключа. Второй шаг – клиентское ПО зашифровывает его закрытым ключом и отправляет серверу результат. В качестве хранилища закрытого ключа выступает банковская карта стандарта EMV.

Технология была успешно применена и доказала свою жизнеспособность.

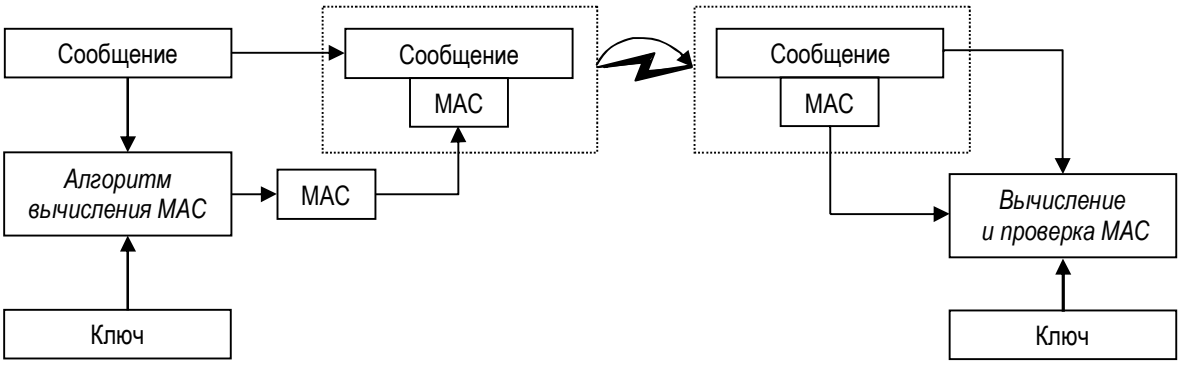

Рис. Схема алгоритма HMAC

Библиографический список

1. Application Security, Inc. Доклад «Безопасность баз данных». http://www.slideshare.net/ngsec/application-security-14372318.
2. Software Application Solutions. Доклад «Protecting Sensitive Data Using Encryption and Key Management». https://www.owasp.org/images/c/c1/Database_Encryption.ppt.
3. Официальный сайт EMV. http://www.emvco.com/.
4. Стандарт «ISO/IEC 7816-3:2006». https://www.iso.org/obp/ui/#!iso:std:iso-iec:7816:-3:ed-3:v1:en.
5. Статья «Fraud and EMV». http://www.gemalto.com/emv/fraud_emv.html.
6. Документация «EMV». http://www.openscdp.org/scripts/tutorial/emv/index.html

TWO-FACTOR AUTHENTICATION USING A EMV CHP CARD

P.A. Vakhrushev

Perm State National Research University, LLC «Alternativa»

A computer program has been designed to implement two-factor user authentication when accessing sensitive information in the database. A bank card of EMV standard describing public keys infrastructure is used as the second authentication factor.

Keywords: two-factor authentication, data protection, EMV, bank cards.

Сведения об авторе

Вахрушев Павел Андреевич, студент, Пермский государственный национальный исследовательский университет (ПГНИУ), 614990, г. Пермь, ул. Букирева, 15; ведущий программист, ООО «Альтернатива», 614000, г. Пермь, ул. Голева, 9А; e-mail: webartifex@gmail.com

Материал поступил в редакцию 25.05.2015 г.