УДК: 004.056.53

ОБЗОР И АНАЛИЗ МЕТОДОВ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМАХ ТЕСТИРОВАНИЯ

Усубакунова Гулжамал Муратбековна, магистрант группы ИТП(м)-1-19 Кыргызский государственный технический университет им. И. Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Ч.Айтматова 66, e-mail: guljamal.usubakunova@gmail.com

Шаршеева Кундуз Токтобековна, ст. преподаватель кафедры ИВТ,_Кыргызский государственный технический университет им. И. Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Ч.Айтматова 66, e-mail: kunduz2000@mail.ru

Аннотация. Аутентификация — это процесс предоставления пользователю доступа к информационной системе. Существует три основных метода аутентификации:

1. Пользователь знает некую унифицированную информацию (ввод пароля);

2. Пользователь имеет некий унифицированный носитель информации (смарт-карта, токен);
3. *Пользователь сам является неотъемлемой частью* аутентификации (биометрический).

Каждый метод работает по-своему и имеет свои преимущества и недостатки. В данной статье рассматриваются различные механизмы распознавания пользователя в системах тестирования для обеспечения безопасности данных, их уязвимости и рекомендации по использованию.

Ключевые слова: информационные технологии, аутентификация, система тестирования, биометрика, смарт-карта, информационная безопасность

OVERVIEW AND ANALYSIS OF USER AUTHENTICATION METHODS IN TESTING SYSTEMS

Usubakunova Gulzhamal Muratbekovna, undergraduate of ITP(m)-1-19, Kyrgyz State University named after Technical I. Razzakova, Kyrgyzstan, 720044, Bishkek, 66 Aitmatova Ave., e-mail: guljamal.usubakunova@gmail.com

Sharsheeva Kunduz Toktobekovna, senior lecturer at the Informatics and Computer Engineering Department, Kyrgyz State University named after Technical I. Razzakova, Kyrgyzstan, 720044, Bishkek, 66 Aitmatova Ave., e-mail:e-mail: kunduz2000@mail.ru

Abstract. Authentication is process of granting a user access to an information system. There are three main types of authentication mechanisms:

1. The user knows some unified information (password entry);
2. The user has a unified information storage (smart card, token);
3. The user himself is an integral part of the authentication (biometric).

Each authentication mechanism functions differently and has their strengths and weakness. In this paper we review different types of authentication mechanisms, their vulnerabilities, and recommend solutions to use.

Keywords*:* information technology, user authentication, testing system, biometrics, smart-card, information security

1. Введение

Пандемия COVID-19 существенно затронула все сферы общественной жизни, не стала исключением и усовершенствование системы образования. Так оценка полученных знаний становится основной задачей при дистанционном обучении. Создание автоматизированной системы тестирования решает данную задачу и позволяет не только получить объективные оценки уровня знаний, навыков обучающихся, проверить соответствие знаний необходимым требованиям, но и выявить пробелы в подготовке. С ростом необходимости внедрения таких систем стоит вопрос обеспечения безопасности, целостности системы от несанкционированного доступа и повышенной конфиденциальности к личной информации пользователей.

Аутентификация является ключевым элементом обеспечения сохранности пользовательских данных и регулирования доступа к информации.

В настоящее время получили распространение методы аутентификации, которые подразделяются в зависимости от типа информации на следующие виды:

1. «Something you know» (нечто, известное только пользователю – ПИН-коды, пароли, графические ключи, секретные слова);
2. «Something you have» (нечто, имеющееся у пользователя. Смарт-карта или токен выступает носителем информации);
3. «Something you are» (нечто, присущее только пользователю, например, сканеры лица, отпечатки пальцев или сетчатки глаза).

Все перечисленные виды позволяют пользователю одинаково получить доступ, однако они работают по-разному. В любом из этих случаев процедура аутентификации выполняется в четыре этапа - идентификация, аутентификация, авторизация и логирование.

Идентификация — процесс распознавания пользователя по его идентификатору.

Аутентификация — процедура проверки подлинности, доказательство что пользователь именно тот, за кого себя выдает.

Авторизация — предоставление определённых прав.

Логирование — это процесс ведения системных журналов. Системные журналы отслеживают все успешные и неудачные входы в систему.

Таким образом, аутентификация представляет собой процесс проверки подлинности пользователя. В системе безопасности процесс аутентификации проверяет информацию, предоставленную пользователем, сравнивая с базой данных. Если информация совпадает с базой данных, то пользователю предоставляется доступ к системе.

Чтобы понять, какой метод аутентификации применим к той или иной системе, следует разобраться в достоинствах и недостатках всех методов, а также иметь ясное представление о механизме их работы.

2. Методы аутентификации

2.1. Аутентификация по паролю

Этот тип аутентификации требует от пользователя ввода имени и секретной комбинации слов, чисел или символов.

Достоинства. Одна из сильных сторон данного метода заключается в том, что длинный пароль очень сложно взломать. Надежный секретный ключ состоит из заглавных и строчных букв, цифр и уникальных символов. В настоящее время рекомендуются пароли из 12–15 знаков. Для взлома пароля из 12 знаков с мощностью 94 и энтропией 78,7 бит потребуется 55 дней с помощью суперкомпьютеров, а с помощью ПК потребуется 3018 лет. Оценка 94 означает, что пароль выбран из набора 94 знаков, состоящего из букв верхнего и нижнего регистра, цифр и специальных символов. Энтропия – это показатель надежности пароля в битах и рассчитывается как $Entropy = \log_2 N$.

Недостатки. Взлом (подбор) пароля - самая большая проблема с момента ее ввода пользователем. Злоумышленник может перехватить пароль на разных этапах связи. Ключевая проблема пароля – человеческий фактор:

- использование примитивных паролей или паролей по умолчанию;
- применение одинаковых паролей для всех программ и сервисов или коротких паролей, схожие с именем пользователя;
- открыто записанные пароли или пароли, которые были установлены один раз и не изменены долгое время.

Рекомендации по использованию. Необходимо внедрить жесткую форму валидации на признаки описанные выше на этапе регистрации пользователя в системе. Другое решение для повышения надежности - графический пароль, который будет более безопасным по сравнению к текстовому паролю. Аутентификация выполняется путем выбора серии изображений. Для большей безопасности количество попыток ввода пароля должно быть ограничено.

2.2. Аутентификация с помощью смарт-карт

Смарт-карта — это некий носитель информации размером с кредитную карту со встроенным сертификатом, используемый для идентификации владельца. Пользователь может вставить карту в считыватель смарт-карт для проверки подлинности. Смарт-карты обычно используются с PIN-кодом обеспечивая многофакторную аутентификацию.

Достоинства. Определенный интерес для аутентификации представляет возможность смарт-карт проводить криптографические вычисления. Причем смарт-карты поддерживают одно- и многофакторную авторизацию. При однофакторной авторизации выполняется только одна операция - предъявление секретной информации, хранящейся на смарт-карте. Многофакторная авторизация вызывает необходимость от пользователя выполнения

нескольких дополнительных действий, например, ввод PIN-кода.

Многофакторные смарт-карты обеспечивают защиту от вероятной кражи злоумышленником, так как сама по себе смарт-карта не несет в себе никакой ценности.

Смарт-карты позволяют повысить надежность служб PKI (Public Key Infrastructure) путем использования для безопасного хранения закрытых ключей пользователя, а также путем выполнения криптографических преобразований и вычислений.

В основном многие разработчики применяют свои механизмы для хранения и применения закрытых ключей. Из них наиболее простым является использование смарт-карты в качестве носителя информации. При необходимости карта может экспортировать закрытый ключ, и шифрование данных будет производится на рабочей станции. По соображениям безопасности такой метод не является надежным, он применим при работе с низкоуровневой информацией.

Два других способа значительно безопаснее, так как шифрование информации происходит непосредственно внутри смарт-карты. В первом способе пользователь генерирует ключи на рабочей станции и переносит их на смарт-карту, а во втором случае генерация ключей происходит прямо на смарт-карте. И в первом, и во втором случае после сохранения закрытого ключа невозможно получить его обратно из смарт-карты. Если ключ генерируется с помощью смарты-карты, то он не доступен для публичного просмотра. Из этого следует, что вероятность резервного копирования закрытого ключа злоумышленником значительно снижается. Только владение смарт-картой позволяет использовать закрытые ключи. Если смарт-карта будет подвержена механическим воздействиям и выйдет из строя, то восстановление закрытого ключа представляется невозможным. Это необходимо учитывать в случае использования закрытого ключа для криптографических вычислений.

Недостатки. Недостаток заключается лишь в запоминании ПИН-кода, что приводит пользователей к выводу записать его на обратной стороне карты. Если карта будет украдена третьими лицами, то они легко могут использовать ее для идентификации.

Рекомендации по использованию. Предлагается внедрить в систему тестирования аутентификацию с использованием *паспорта* гражданина Кыргызской Республики образца *2017* года (ID-карта), которая выступает смарт-картой и хранит в себе всю необходимую информацию (рис.1) для идентификации пользователя, а так же имеет электронную цифровую подпись, которую можно использовать для подписания тестовых работ, например, при переводе ОРТ(*Общереспубликанское тестирование) на онлайн-формат.*

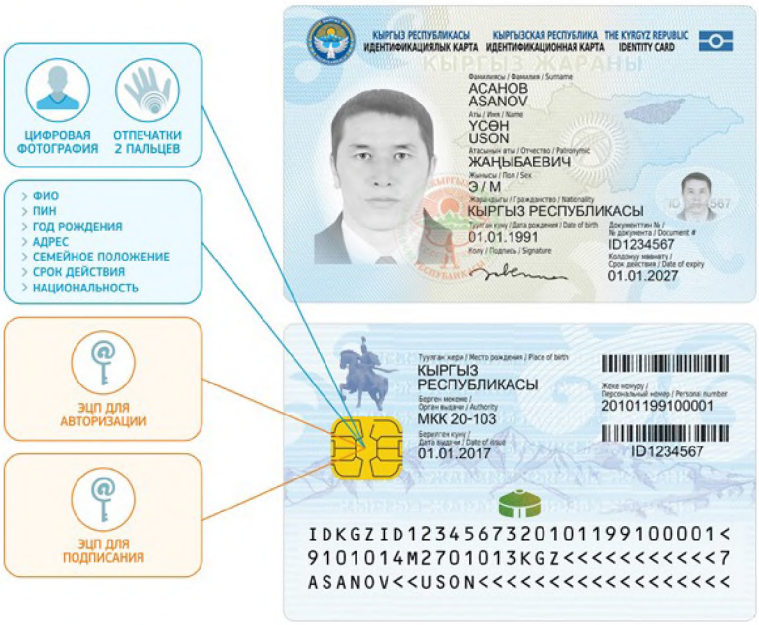

Рис.1 П*аспорт* гражданина Кыргызской Республики образца *2017* года

2.3. Биометрическая аутентификация

Биометрическая аутентификация пользователя – это метод, который идентифицирует пользователя проверяя его личность на основе измерения его уникальных физиологических особенностей или поведенческих характеристик. К физиологическим особенностям относятся отпечаток пальца, распознавание лица, сканирование радужной оболочки глаза, геометрия руки, сканирование сетчатки. Поведенческая биометрия — это распознавание голоса, походки, сканирование нажатия клавиш и сканирование подписи.

Аутентификация через сканирование отпечатков пальцев является наиболее широко используемым на сегодняшний день. Большинство мобильных телефонов и ноутбуков нового поколения оснащены цифровым считывателем отпечатков пальцев, а на старых поколениях имеется возможность ее подключения. Сканер отпечатков пальцев в качестве проверки использует изображения для определения контуров рисунка папиллярного узора.

Достоинства:

- Биометрическая аутентификация позволяет пользователю избежать сложной задачи по восстановлению паролей.
- Биометрические данные уникальны. Очень сложно воспроизвести биометрические характеристики.
- Биометрические характеристики не могут быть потеряны.
- Устройства биометрической аутентификации удобны в пользовании и экономичны в эксплуатации.

Недостатки:

- Биометрические характеристики нельзя изменить в текущей базе данных - в отличие от паролей, они связаны с конкретной личностью на протяжении всей ее жизни;
- Из-за возрастных изменений, травм, ампутаций и прочего, требуется постоянное обновление эталонных моделей сравнения, которые вносятся в память электронно-вычислительных устройств;
- Для создания образцов биометрии требуются специальные считывающие устройства;
- Биометрические характеристики невозможно сохранить в секрете, поэтому опытные злоумышленники могут подделать образцы отпечатков пальцев или ладоней.

Рекомендации по использованию. Биометрическая аутентификация снижает человеческий фактор при определении подлинности пользователя. Но она вызывает ошибки типа 1 и 2. Ошибка первого рода — ситуация, когда отвергнута правильная нулевая гипотеза (англ. type I errors, α errors, false positive, ошибочное отвержение) и ошибка второго рода — ситуация, когда принята неправильная нулевая гипотеза (англ. type II errors, β errors, false negative, ошибочное принятие). Лучшее решение может быть объединение различных биометрических характеристик.

2.4. Аутентификация на основе сертификата

Аутентификация личности на основе цифровых сертификатов аналогично прохождению в закрытую организацию. Охрана пропускает сотрудников на территорию учреждения по предъявлению пропуска, который содержит фотографию и личные данные, заверенные печатью предприятия и подписью руководителя. Сертификат выступает своего рода пропуском и выдается по запросам специальными сертифицирующими центрами при выполнении определенных условий.

Сертификат представляет собой электронную форму, в которой обычно содержится стандартные данные:

- открытый ключ владельца данного сертификата;
- сведения о владельце сертификата, такие, например, как имя, адрес электронной почты, наименование организации, в которой он работает, и т.п.;
- наименование сертифицирующей организации, выдавшей данный сертификат.

Так же, сертификат имеет электронную подпись сертифицирующей организации – зашифрованные закрытым ключом этой организации.

Применение сертификатов базируется на предположении, что количество сертифицирующих организаций ограничено и их открытые ключи могут быть всем доступны из официальных источников. Если пользователю требуется подтвердить свою личность, он может предоставить свой сертификат в двух формах – открытой (в том виде, в каком выдана сертифицирующей организацией) и зашифрованной с помощью своего закрытого ключа. Сторона, проводящая аутентификацию, берет из открытого сертификата открытый ключ пользователя, посредством которого расшифровывает зашифрованный сертификат. Идентичность результата с открытым сертификатом доказывает, что предъявитель действительно является владельцем закрытого ключа, парного с указанным открытым.[7]

На следующем этапе с помощью известного открытого ключа производятся криптографические операции по расшифровыванию подписи этой организации. Если при проверке получается такой же сертификат с тем же именем пользователя и его открытым ключом, то это подтверждает достоверность регистрации в сертификационном центре.

Отметим тесную связь открытых ключей с сертификатами. Сертификат одновременно выступает и как удостоверение личности, и как удостоверение принадлежности открытого ключа. Безусловно, он гарантирует соответствие между открытым ключом и его владельцем, что устраняет угрозу подмены открытого ключа. Если некоторому абоненту поступает открытый ключ в составе сертификата, то он может не сомневаться, что этот открытый ключ гарантированно принадлежит отправителю.

Достоинства. *Цифровые сертификаты работают автоматически и требует минимальных действий или участия со стороны любого отправители или получатели.*

Недостатки. Органы, выдающие цифровые сертификаты, подвергаются атакам со стороны злоумышленников, и информация сертификата может быть изменена.

Рекомендации по использованию. Предлагается использовать для аутентификации инфраструктуру открытых ключей Государственного предприятия «Инфоком» при ГРС при ПКР, которая предназначена для управления сертификатами открытых ключей пользователей.

3.Заключение

Аутентификация, будь то пароль, смарт-карта или биометрические данные - важный процесс в любой системе тестирования. На основе вышеизложенного можно сделать следующие общие выводы:

- Для любой системы тестирования пароль должен состоять не менее чем из 12 знаков с мощностью 94 символа.
- Смарт-карты предлагается использовать вместе с PIN-кодами.
- Следует ограничить количество попыток ввода пароля или PIN-кода.
- Биометрия - самый надежный метод аутентификации. Хотя аутентификация через отпечаток пальца удобна, она также имеет некоторые слабые стороны, которые необходимо устранить в будущем.
- Комбинация из нескольких биометрических характеристик может обеспечить более высокую безопасность аутентификации.
- Для усиленная безопасности цифровые сертификаты могут быть включены в современные системы тестирования.

Литература

1. Константин Мытник, Сергей Панасенко, «Информационная безопасность и смарт-карты» , ДМК Пресс, 2018
2. Удостоверяющий центр «Инфоком», [Электронный ресурс]. Доступен: https://infocom.kg/ru/pki/
3. Идентификационная карта - паспорт гражданина Кыргызской Республики образца 2017 года, [Электронный ресурс].

Доступен: https://grs.gov.kg/ru/eid/

4. Bioelectronix, "Biometric Security," [Электронный ресурс]. Доступен: http:/bioelectronix.com/what_is_biometrics.html
5. Ошибки первого и второго рода, [Электронный ресурс]. Доступен: http://wikipedia.org/wiki/Ошибки_первого_и_второго_рода
6. Ричард Э. Смит, «Аутентификация: от паролей до открытых ключей», М.: Вильямс, 2002.
7. Стамкулова Г.К. Информационная система для поддержки прохождения аккредитации учебных заведений в Министерстве образовании и науки КР / Г.К. Стамкулова, Т. Биримкулов // Известия Кыргызского государственного технического университета им. И. Раззакова. №4 (52). 2019. С. 77-82