Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ ИУ «Информатика и системы управления»

КАФЕДРА ИУ-7 «Программное обеспечение ЭВМ и информационные технологии»

РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

К НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

НА ТЕМУ:

«Методы аутентификации пользователя»

Студент группы ИУ7-56Б _____ **Киселёва М.С.**
(Подпись, дата) (Фамилия И.О.)

Руководитель _____ **Григорьев А.С.**
(Подпись, дата) (Фамилия И.О.)

2022 г.

РЕФЕРАТ

Расчетно-пояснительная записка содержит 23 стр., 1 рис., 2 таб., 10 ист.

АУТЕНТИФИКАЦИЯ, КРИПТОГРАФИЯ, ПАРОЛЬ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, АТАКИ.

Цель работы: классификация методов аутентификации пользователя.

Результат: были классифицированы такие методы аутентификации, как парольная, графическая, биометрическая, с использованием одноразовых паролей, с использование открытого ключа, а также через географическое положение.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ

OTP — One-Time Password — одноразовый пароль.

PIN — Personal Identification Number — персональный идетификационный номер.

FAR — False Acceptance Rate — коэффициент ложного пропуска.

FRR — False Rejection Rate — коэффициент ложного отказа.

RFID — Radio-frequency identification — радиочастотная аутентификация.

USB — Universal Serial Bus — универсальная последовательная шина.

GPS — Global Positioning System — система глобального позиционирования.

ВВЕДЕНИЕ

В современном мире важным вопросом является обеспечение информационной безопасности любых информационных систем, так как в них хранится и обрабатывается большой объем информации ограниченного доступа. Вместе с быстрым развитием информационных технологий активно развиваются и злоумышленные действия над информацией, такие как кража, изменение или удаление данных [1].

Поэтому сейчас защита информации является одной из ключевых задач в информационных системах. В основе защиты информации лежит базовый принцип — разграничение доступа в систему. Для его соблюдения необходимо проверять подлинность субъекта, получающего доступ к информации. Данный процесс называется аутентификацией [2].

Цель данной работы — классификация существующих методов аутентификации пользователя.

Для достижения поставленной цели требуется решить следующие задачи:

— описать основные виды атак на пароли;
— рассмотреть базовые элементы и понятия, используемые при проектировании методов аутентификации пользователя;
— провести анализ существующих методов аутентификации пользователя;
— провести классификацию методов аутентификации пользователя на основе выделенных критериев.

1 Анализ предметной области

1.1 Виды атак на пароли

Сейчас существует огромное количество различных атак для того, чтобы получить доступ к информации ограниченного доступа.

Основные виды атак [3]:

— полный перебор;
— подглядывание из-за плеча — злоумышленник подсматривает набор пароля пользователем и затем использует его сам;
— троянский конь — злоумышленник скрытно устанавливает программу, имитирующую обычный механизм аутентификации, но на самом деле она собирает информацию об именах и паролях пользователей при их попытках входа в систему;
— перехват данных в момент их перемещения от пользователя к механизму аутентификации или между устройствами.

1.2 Базовые понятия

1.2.1 Хэш-функция

Хэш-функция [4] — функция, осуществляющая преобразование массива входных данных произвольной длины в выходную битовую строку установленной длины, выполняемое определенным алгоритмом.

Она является ключевым инструментом защиты пароля при его хранении и передачи на сервер. Хэш-функции применяются:

— при проверки целостности информации;
— при хранении паролей;
— в авторском праве (для создания электронно-цифровой подписи);
— при решении задачи дедубликации.

Криптографическая стойкость [5] — это способность криптографического алгоритма противостоять криптоанализу. Алгоритм считается стойким, когда успешная атака требует от атакующего обладания недостижимым объемом вычислительных ресурсов или значительных затрат времени на раскрытие, что к его моменту информация уже потеряет актуальность.

При рассмотрении хэш-функций под алгоритмом подразумевается процесс вычисления значения хэш-функции, а под атакой на алгоритм — решение обратной задачи: нахождение для заданного значения хэш-функции *Y1* такого массива входных данных *X1*, что *f(X1) = Y1*. Хэш-функцию, которая является стойкой по определению криптографической стойкости по отношению к такой задаче, называют криптостойкой.

У криптостойких функций имеется следующее свойство: при наличии массива входных данных *X1* и значения хэш-функции для него *f(X1)*, сложной задачей является не только нахождение обратного значения, но и задача нахождения такого отличного от *X1* значения массива входных данных *X2*, для которого верно *f(X1) = f(X2)*. Такие значения *X1* и *X2*, для которых верно равенство *f(X1) = f(X2)*, называются коллизиями.

1.2.2 OTP-токен

OTP-токен [2] — мобильное персональное устройство, которое принадлежит определенному пользователю и генерирует одноразовые пароли, используемые для аутентификации данного пользователя.

OTP-токены условно можно разбить на две группы [6]: либо у пользователя есть физические инструменты для такой генерации, например аппаратные устройства с экраном, мобильные приложения (Google Authenticator, Яндекс.Ключ, Aladdin 2FA, Microsoft Authenticator) и т.д., либо пароли приходят по какому-то каналу — в виде SMS-сообщения, пуш-уведомления и др.

1.2.3 Открытый и закрытый ключи

Открытый и закрытый ключи [7] — парные, зависимые друг от друга ключи. Открытый ключ позволяет кому-либо обмениваться с пользователем шифрованными сообщениями и проверять подлинность его подписи. Закрытый ключ хранится в секрете, позволяет читать зашифрованные сообщения и ставить защищенную от подделки подпись. Ключи в шифровальных системах с открытым ключом — очень большие числа, иногда из более чем тысячи цифр. Ключи математически связаны так, что, зная открытый ключ, практически невозможно вычислить закрытый ключ.

2 Классификация существующих решений

2.1 Парольная аутентификация

Парольная аутентификация [2] — аутентификация на основе обладания неким секретным знанием. В большинстве случаев пароли могут обеспечить достаточный уровень защиты системы, но в крупных организациях применение многоразовых паролей не обеспечивает необходимой безопасности.

Аутентификация на основе открытого пароля является самым старым и простым методом.

Принцип работы:

1) пользователь вводит свое имя и пароль на рабочей станции;
2) имя и пароль передаются в открытом доступе по сети;
3) сервер аутентификации находит учетную запись пользователя в базе данных аутентификации и сравнивает введенные данные с ее содержимым.

Усовершенствованным вариантом многоразового пароля является использование его хэш-значения, получаемого с помощью криптографической хэш-функции.

Принцип работы:

1) пользователь вводит свое имя и пароль на рабочей станции;
2) рабочая станция вычисляет от введенного пароля хэш-значение;
3) имя и хэш-значение передаются в открытом доступе по сети серверу аутентификации;
4) сервер аутентификации сравнивает результат хэш-значения от введенного пользователем пароля с хэш-значением, хранящимся в учетной записи пользователя.

Так как невозможно восстановить исходный пароль даже при владении хэш-значением, то вероятность доступа к информации ограниченного доступа злоумышленником минимальна.

PIN-код [2] — это разновидность пароля, который в основном используют для аутентификации на локальном устройстве.

Отличие PIN-кода от пароля в условиях и области его использования. PIN-код можно ввести только с использванием клавиатуры конкретного устройства, то есть его не передают по сети, поэтому никто не может его перехватить.

2.2 Аутентификация с помощью биометрических характеристик

Биометрическая характеристика [2] — это измеримая физиологическая или поведенческая черта живого человека, которую можно использовать для установления личности или проверки декларируемых личных данных.

Биометрические характеристики делятся на два вида: физиологические и поведенческие.

Физиологическими характеристиками являются данные, полученные измерением анатомических характеристик человека.

К физиологическим характеристикам относятся:

— отпечаток пальца;
— радужная оболочка глаза;
— сетчатка глаза;
— геометрия рук;
— лицо.

Поведенческими характеристиками являются данные, полученные измерением действий человека.

К поведенческим характеристикам относятся:

— голос;
— подпись;
— ритм работы сердца;
— динамика работы на клавиатуре.

Все биометрические системы имеют одинаковый принцип работы. Поль-

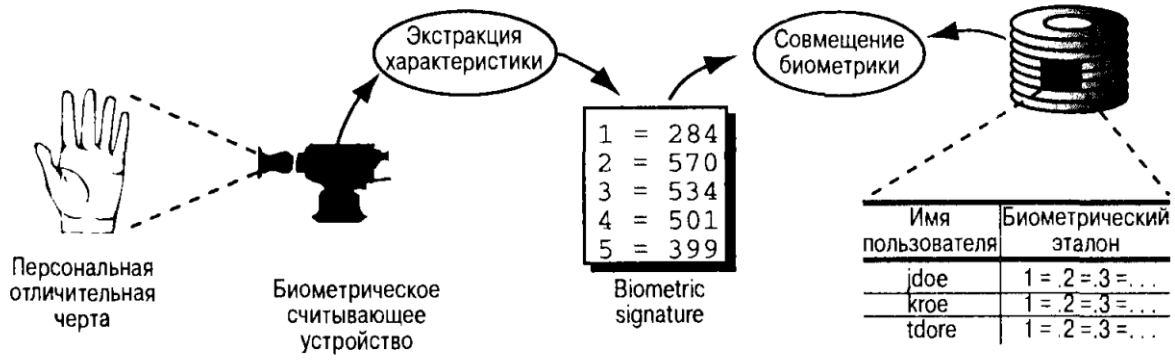

Рисунок 1 – Схема работы биометрической системы [2]

зователь предоставляет образец биометрической характеристики, регистрирующее устройство обрабатывает его, в результате получается контрольный шаблон. Под шаблоном подразумевается большая числовая последовательность.

При регистрации в биометрической системе на основе нескольких образцов создается эталонный шаблон, с которым и производится сравнение контрольного шаблона. Поскольку они никогда не смогут совпасть, необходимо настроить пороговую величину, которую степень совпадения должна превысить.

На рисунке 1 изображена базовая схема работы биометрической системы.

Главными, для оценки точности биометрических систем, являются два параметра [8]:

FAR — коэффициент ложного пропуска, т.е. процент возникновения ситуаций, когда система разрешает доступ пользователю, который незарегистрирован в системе.

FRR — коэффициент ложного отказа, т.е. отказ в доступе пользователю, который зарегистрирован в системе.

Так как все люди обладают индивидуальными характеристиками, а украсть или подменить их практически невозможно, то данный метод можно считать устойчивым к злоумышленным действиям. Однако существуют другие проблемы, например: некоторые люди не имеют частей тела, необходимых для внесения в систему, есть и те, кто считают, что сбор биометрических данных — это

вмешательство в их частную жизнь или это оскорбляет их культурные или религиозные ценности.

2.3 Аутентификация с помощью одноразовых паролей

Одноразовые пароли [2] — динамическая аутентификационная информация, генерируемая для единственного использования с помощью аутентификационных устройств (программных или аппаратных).

Такие устройства называются OTP-токенами. Для генерации одноразовых паролей OTP-токены используют хэш-функции или криптографические алгоритмы. Обычно в OTP-токенах применяют симметричную криптографию (криптографию с одним ключом). Устройство пользователя содержит уникальный секретный ключ, используемый для шифрования некоторых данных для генерации OTP. Такой же ключ хранится на сервере аутентификации, там он шифруется. В итоге, сравниваются два результата шифрования: если совпали, значит аутентификация прошла успешно.

Методы, используюмые OTP-токенами, которые применяют симметричную криптографию, можно разделить на две группы, работающие: в асинхронном и в синхронном режимах.

В асинхронном режиме работает метод «запрос-ответ», а методы «только ответ», «синхронизация по времени» и «синхронизация по событию» в синхронном режиме.

В методе «запрос-ответ» OTP является ответом пользователя на случайный запрос от сервера аутентификации.

В методе «только ответ» аутентификационное устройство и сервер аутентификации генерирует «скрытый» запрос, используя значения предыдущего запроса. Чтобы изначально инициализировать данный процесс используют уникальное случайное начальное значение, которое генерируется при инициализации OTP-токена.

В методе «синхронизация по времени» OTP генерируется на основе значения внутренних часов аутентификационного устройства и аутентификационного сервера.

В методе «синхронизация по событию» OTP-токен и сервер аутентификации ведут количественный учет прохождения аутентификации данным пользователем, и на основе этого числа генерируют OTP.

2.4 Аутентификация с помощью открытого ключа

В криптографии с открытым ключом (асимметричная криптография) алгоритмы используют связанные между собой пары ключей, состоящие из открытого и закрытого ключа [2]. Информация, зашифрованная с помощью одного ключа из ключевой пары, может быть расшифрована только с помощью другого ключа из это же пары.

Идея в том, что аутентификационный сервер хранит файл всех открытых ключей, а пользователь сам хранит свой закрытый ключ.

Принцип работы:

1) сервер посылает пользователю случайную строку, созданную генератором случайных чисел;
2) пользователь шифрует эту строку своим закрытым ключом и посылает ее обратно серверу вместе со своим именем;
3) сервер находит в базе данных открытый ключ пользователя и расшифровывает сообщение, используя этот открытый ключ;
4) если отправленная и расшифрованная строки совпадают, сервер предоставляет пользователю доступ к системе.

Такой вид аутентификации может быть надежным, однако необходимо решить проблему с безопасным хранением закрытого ключа. Самый простой вариант — это хранить закрытый ключ внутри локального хранилища операционной системы, которое защищено с помощью криптографических методов. Од-

нако жесткий диск уязвим к прямым и сетевым атакам, и в данном случае ключ связан с конкретным компьютером. Решение — специализированные устройства.

Далее были рассмотрены основные виды таких устройств.

Таблетка Touch Memory [2] — это электронное устройство, имеющее энергонезависимую память, размещенную в металлическом корпусе, в которой можно хранить данные пользователя. Устройство активизируется в момент контакта со считывателем.

Смарт-карта [2] — это пластиковая карта, со встроенной микросхемой, микропроцессором и операционной системой, контролирующей устройство и доступ к объектам в памяти. Зачастую она могжет проводить криптографические вычисления.

Все смарт-карты можно разделить на три вида [9]:

1) контактные карты памяти — могут работать, когда электрические контакты, расположенные на поверхности, соприкасаются со считывателем;
2) бесконтактная смарт-карта — информация считывается с карты, если устройство использует определённую радиочастоту (RFID), поэтому физический контакт со считывателем не нужен;
3) многокомпонентная карта — это редко встречающийся тип карт, который создаётся под какое-то конкретное решение, например, может быть встроен считыватель отпечатка пальца.

USB-ключ [2] — аппаратное устройство, со встроенной микросхемой, которое хранит в себе ключ, доступ к которому осуществляется через порт USB.

Смарт-карты и USB-ключи являются интеллектуальными устройствами.

Чтобы использовать закрытый ключ, с устройства можно либо его экспортировать, и криптографические операции осуществлять уже на рабочей станции, либо все вычисления проделать на самом устройстве. Второй вариант является наиболее безопасным.

Слабым местом любых токенов, при всем совершенстве применяемых ал-

горитмов является возможность утери или целенаправленного хищения, либо уничтожения ключевого носителя.

2.5 Аутентификация через географическое местоположение

Данный метод использует GPS. GPS состоит из 24 спутников, положение которых на орбите всегда точно известно. Каждый спутник передает непрерывный поток идентифицирующей информации, которая при объединении с сигналами от других видимых спутников позволяет точно определить географическое местонахождение [3]. Основным достоинством такого метода является то, что аппаратура GPS надежна в использовании и относительно недорога. Ее использование необходимо в тех случаях, когда пользователь должен находиться в нужном месте, например офисном здании. Так как координаты спутников меняются постоянно, то вероятность перехвата этих координат равна нулю.

2.6 Графическая аутентификация

Графическая аутентификация [3] — это метод аутентификации, когда для доступа в систему пользователю необходимо выполнить некоторые операции над изображениями.

Далее были рассмотрены некоторые схемы аутентификации на основе графических паролей.

В схеме *Passlogix* [10] при генерации пароля пользователю показывают картинку, он выбираете на ней несколько мест и нажимет на них мышью. Парольная комбинация строится из 5-6 кликов мышки в определенном порядке. При вводе пароля показывается та же самая картинка, и надо нажать в те же самые места. Допускается, что при аутентификации пользователь попадает хотя бы в окрестность парольных точек. Точки и последовательность их нажатия хранятся в хэшированном виде.

У *Passlogix* есть свои плюсы и минусы. Если в качестве картинки выбрать большую фотографию со множеством мелких деталей - например, городской пейзаж в высоком разрешении, то даже четыре клика на нем окажутся паролем, легким для запоминания, но очень трудным для грубого взлома. Если же, наоборот, выбрать небольшой портрет человека, с двумя родинками и кольцом на руке, то не составит труда перебрать наиболее вероятные варианты пароля.

Схема *PassFaces* [10] основана на распознавании человеческих лиц. Во время создания пароля пользователям предоставляется большой набор изображений на выбор. Чтобы войти в систему, пользователь должен узнать предварительно выбранное лицо из нескольких представленных ему. Лица появляются в случайных позициях.

В схеме *Pass-string* [10] N объектов случайно разбросано на экране. Пользователь выбирает K объектов (пропускное подмножество) и запоминает их. Существуют разные варианты для входа: найти 3 парольных объекта, используя прямые мысленно их соединить и нажать внутри фигуры или щелкнуть объект на пересечении прямых, которые проходят через четыре парольных объекта.

В схеме *Deja Vu* [10] пользователь запоминает M изображений (пропускное подмножество) из P возможных. Чтобы войти пользователь должен правильно выбрать изображения, которые состоят в его пропускном подмножестве.

2.7 Сравнение методов аутентификации

Сокращения для категорий:

— ПА — парольная аутентификация;
— БА — биометрическая аутентификация;
— ОП — аутентификация с помощью одноразовых паролей;
— ОК — аутентификация с помощью открытого ключа;
— ГМ — аутентификация через географическое местоположение;
— ГА — графическая аутентификация.

Сокращения для критериев:

— К1 — стоимость установки и обслуживания (затраты времени, усилий и денежных средств);
— К2 — удобство использования (простота и портативность системы);
— К3 — возможность возникновения ошибок (подразумевается возможность допустить к системе незарегистрированного пользователя или не допустить зарегистрированного пользователя);
— К4 — требование наличия дополнительных программных и аппаратных средств;
— А1 — возможность полного перебора;
— А2 — возможность подглядеть из-за плеча;
— А3 — возможность перехвата пароля;
— А4 — возможность троянского коня.

Классификацию рассмотренных методов аутентификации можно увидеть в таблицах 1 и 2.

Таблица 1 – Классификация методов аутентификации пользователя по качественным характеристикам.

Метод аутентификации	**К1**	**К2**	**К3**	**К4**
ПА	Низкая	Среднее	Нет	Не требуется
БА	Высокая	Высокое	Да	Требуется АО
ОП	Низкая	Низкое	Нет	Требуется
ОК	Средняя	Среднее	Нет	Требуется
ГМ	Средняя	Низкое	Да	Требуется
ГА	Высокая	Высокое	Да	Только ПО

Таблица 2 – Классификация методов аутентификации пользователя на основе возможных атак.

Метод аутентификации	**A1**	**A2**	**A3**	**A4**
ПА	Да	Да	Да	Да
БА	Нет	Нет	Нет	Да
ОП	Да	Нет	Нет	Да
ОК	Нет	Нет	Нет	Нет
ГМ	Нет	Нет	Нет	Нет
ГА	Да	Да	Нет	Да

ЗАКЛЮЧЕНИЕ

Цель работы была достигнута — классифицированы методы аутентификации пользователя.

Все задачи работы были выполнены:

— описаны основные виды атак на пароли;

— рассмотрены базовые элементы и понятия, используемые при проектирование методов аутентификации;

— проведен анализ существующих методов аутентификации пользователя;

— проведена классификация на основе выделенных критериев.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Отчёт об утечках данных за 1 полугодие 2022 года [Электронный ресурс]. — Режим доступа: https://www.infowatch.ru/analytics/analitika/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda, свободный (дата обращения: 10.11.2022).

2. Афанасьев А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Текст] / Афанасьев А. А., Веденьев Л. Т., Воронцов А. А. и др.: Под ред. Шелупанова А.А., Груздева С.Л., Нахаева Ю.С. — М.: «Горячая линия — Телеком», 2012. — 552 с.

3. Ричард Э. Смит. Аутентификация: от паролей до открытых ключей [Текст]: Пер с англ. / Под ред. А. А. Голубченко. — М.: Издательский дом «Вильямс», 2002. — 442 с.

4. Schneier B. Applied Cryptography. Protocols, Algorithms, and Source Code in C [Текст]. Изд. 2-е — «John Wiley & Sons», 1996. — 784 с.

5. Мао В. Современная криптография: Теория и практика [Текст]: Пер с англ. — М.: Издательский дом «Вильямс», 2005 — 768 с.

6. Обзор систем аутентификации на основе одноразовых паролей [Электронный ресурс]. — Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/One-time-password-authentication-systems, свободный (дата обращения: 15.11.2022).

7. Райтман М. Искусство легального, анонимного и безопасного доступа к ресурсам Интернета / Райтман М. — СПб.: «БХВ-Петербург», 2017. — 624 с.

8. Технологии и методы биометрической идентификации [Электронный ресурс]. — Режим доступа: http://www.techportal.ru/security/biometrics/tekhnologii-biometricheskoy-identifikatsii/, свободный (дата обращения: 15.11.2022).

9. Смарт-карта и токен: в чем отличие [Электронный ресурс]. — Режим доступа: https://astral.ru/articles/elektronnaya-podpis/27556/, свободный (дата обращения: 13.12.2022).

10. Давыдов С. Н. Процесс аутентификации с применением графических паролей / Давыдов С. Н., Клепцов М. Я., Любимова Л. В. // Открытое образование. — 2015. — №2. — С. 33-37.

ПРИЛОЖЕНИЕ А

Презентация к научно-исследовательской работе

Презентация содержит 16 слайдов.