СИСТЕМЫ АУТЕНТИФИКАЦИИ

Комеков Э.А.

Комеков Эсен Арсланович- студент бакалавриата,
базовая кафедра банковская автоматизация и информационные технологии,
факультет информационные технологии и анализ больших данных
Финансовый университет при правительстве РФ,
г. Москва

Аннотация: *в статье анализируются системы аутентификации.*
Ключевые слова: *информационные технологии, аутентификация, системы аутентификации.*

AUTHENTICATION SYSTEMS

Komekov E.A.

Komekov Esen Arslanovich - Undergraduate student,
BASIC DEPARTMENT OF BANKING AUTOMATION AND INFORMATION TECHNOLOGY,
FACULTY OF INFORMATION TECHNOLOGY AND BIG DATA ANALYSIS,
FINANCIAL UNIVERSITY UNDER THE GOVERNMENT OF THE RUSSIAN FEDERATION,
MOSCOW

Abstract: *The article analyzes authentication systems.*
Keywords: *information technologies, authentication, authentication systems.*

Введение

Информационные технологии представляют собой немаловажную составную часть абсолютно всех областей деятельности человека. Одновременно с процессом эволюции передовых высоких технологий фиксируются всё больше недобросовестных и мошеннических действий в отношении информации. По этой причине проблема обеспечения безопасности данной информации очень актуальна, ведь в информационных системах содержится и систематизируется достаточно внушительный объем конфиденциальной информации ограниченного доступа.[1]

Благодаря информационным системам решается большое количество задач. Это является причиной многообразия информационных систем. Ввиду этого обеспечение информационной безопасности имеет большое значение.

Целью проверки подлинности является удостоверение личности. Безопасность систем нужна дабы пресечь всякого рода несанкционированный противозаконный доступ к секретным данным. Вследствие этого в нынешних информационных системах пользователь до преступления к работе с системой должен пройти процесс подлинности, который заключается в авторизации, идентификации и аутентификации. Эти понятия часто используют как синонимы, так как это три связанные между собой части одного единого операционного процесса. Однако суть каждого различна, и каждый из этих процессов имеет свою определенную задачу.

Авторизация – это системная проверка прав определенного пользователя на допуск к операционным ресурсам, а также разрешение на право выполнять различные операции в системе.

Идентификация – это процесс, в результате которого пользователь сообщает информацию о себе, то есть идентифицирует себя в автоматизированной системе.

Аутентификация – это проверка, при которой система проверяет и подтверждает действительную подлинность пользователя. При аутентификации проверяется достоверность введенного пароля и электронного сообщения.

Необходимость надёжной аутентификации становится всё более острой. Личные данные пользователей являются объектом мошеннического интереса злоумышленников, и выбор способа аутентификации очень важен.

Аутентификация предоставляет пользователю разрешение к дальнейшим действиям в информационной системе, и очень важно, чтобы данные права получил правильный субъект, в противном случае последствия окажутся плачевными. По этой причине важную роль играет способ проверка подлинности, который бы с надежной безопасностью определял бы нужного субъекта от остальных. Нынешние способы аутентификации позволяют выбрать нужную конфигурацию для любых случаев. Для прохождения аутентификации применяются такие системы, как пароли, карты доступа, одноразовые пароли (например, SMS-сообщения), токены, биометрия.

Аутентификация, точнее сам ее процесс, представляет собой основу конфиденциального доступа, является гарантией доверительных и защищенных от кибер-атак отношений между пользователем и самой системой. По этой причине анализ системы аутентификации является насущным и актуальным.[2]

В ультрасовременных новейших информационных системах существует огромное разнообразие систем аутентификации, но наиболее известны и чаще всего используется только шесть из них:

1. использование цифрового сертификата, электронной подписи;
2. посредством пароля;
3. использование биометрии;
4. при помощи географического расположения;
5. посредством SMS-сообщения;
6. графическая аутентификация.

Рассмотрим плюсы и минусы каждого из способов аутентификации.

1.1. Цифровой сертификат, электронная подпись

Цифровой сертификат – это электронное удостоверение, подтверждающее принадлежность ключа шифрования пользователю. Этот способ актуален при закодированных соединениях при удостоверении подлинности сервера Интернета. Пользователь имеет возможность быть уверенным в подключении к реальному сайту. Цифровой сертификат является составляющей частью электронной подписи, которая подтверждает авторство пользователя, и представляет собой его юридическое изъявление намерений.

Электронная подпись может быть простой, квалифицированной, а также неквалифицированной, и представлять собой введение паролей, которые служат доказательством того, что она была составлена определенным лицом при помощи криптографического перекодирования информации с применением ключа электронной подписи. Сервер аутентифицирует электронную подпись на карте пользователя.

Электронная подпись допускает идентификацию пользователя, хозяина ключа подписи, и определяет отсутствие фальсификации информации в документах, хранящихся в электронной системе. Электронная подпись заменяет собственноручную и используют, например, при удаленном обращении граждан в органы власти. Документ с такой подписью обладает той же юридической силой, как и подписанный рукой бумажный документ.

Однако данный способ имеет свои минусы. Надежность хранения и защита закрытого ключа перекладывается на самого пользователя, а значит возникает риск хищения данных. [3]

Основные критерии данного способа аутентификации:

- стоимость на установку и обслуживание высокая;
- показатель удобства использования средний;
- наличие открытого интерфейса;
- этот способ подвергается атакам;
- ошибки не допускаются;

1.2. Одноразовые и многоразовые пароли

Пароли на столько сильно связаны с аутентификацией, что часто их представляют её сущностью. Существуют одноразовые или многоразовые.

Многоразовые используются в корпоративных информационных системах. Пользователь задает собственный пароль, который сохраняется в базе данных и при аутентификации будет сравниваться с теми, которые уже были введены и сохранены. Такой пароль обеспечивает должный уровень защиты, но в больших организациях использование многоразового пароля недостаточно. Он не гарантируют требуемой защиты информационной системы при проверке достоверности личности сотрудника. Нередко в организациях пароли не держат в секрете, указывают их в документах, почти всегда они просты и легко запоминаемы.

Считаю, что многоразовый пароль в нынешнее время бессмыслен как фактор аутентификации, его без особого усилия можно даже подобрать. Можно применить и сложный пароль, но тогда он трудно запоминаемый.

Аутентификация одноразовым паролем более защищённая и представляет собой введение каждый раз нового пароля при входе в систему. При всей надежности этого способа, он всё же уязвим. Проследив трафик, можно перехватить одноразовый пароль, отправленный пользователем и заблокировать его компьютер, отправляя перехваченные данные уже от себя.

Мы все пользователи Интернета, регистрируемся на многих сервисах, для каждого из которых нужен пароль. Единственный пароль для всех сайтов удобен, но небезопасен. Безопаснее разные пароли, но это неудобно.

Основные критерии проверки подлинности посредством паролей:

- показатель затрат низкий;
- нет возможности интеграции с существующими приложениями;
- существует уязвимость и незащищенность в реализации;
- не допускается к информационной системе незарегистрированный пользователь;

1.3. Биометрия

В отличие от предыдущих способов данный метод имеет высокую степень защиты, потому что биометрические данные довольно трудно заменить. Это сканирование отпечатков пальцев пользователя, его геометрия руки, радужная оболочка глаз, а также лицо, подпись и даже голос.

Биометрическая аутентификация – это ультрасовременный продвинутый способ безопасности доступа. Он базируется на личных параметрах человека, сохранять которые не нужно, так как постоянно при нем.

Биометрические данные уникальны тем, что неразделимы с человеком, что позволяет с уверенностью утверждать о подлинности пользователя. Но и этот способ не может похвастаться своим совершенством в

безопасности. При всей своей высокой степени защиты также, как и остальные методы он подвергается угрозам злоумышленников, которые используют муляжи для несанкционированного входа в систему. А также есть вероятность «двойника» со схожими параметрами с пользователем и изменение характеристики пользователя в результате пластической операции или травмы.

Но биометрия всё же преобладает над остальными способами.

Основные критерии проверки подлинности с использованием биометрии:

- средние расходы на затраченное время и установку с обслуживанием системы;
- высокая оценка универсальности и портативности данной системы проверки подлинности пользователя;
- открытый интерфейс;
- стойкий к атакам, но есть малая возможность подмены;
- есть вероятность просчета, например, допуск незарегистрированного пользователя системы;
- требуется аппаратное обеспечение.

1.4. Метод географического расположения

При этом методе аутентификации используется GPS-аппаратура, она предоставляет возможность определить точное положение места устройства. Данный способ аутентификации предполагает прохождение проверки в несколько факторов, два и более, например, таких, как ввод пароля вместе со сканированием отпечатка пальца или же ввод пароля, но уже с подтверждением по SMS-сообщению.

Именно этот способ аутентификации на базе его местонахождения является новейшим ориентиром безопасности информационной системы. Система космической навигации может GPS с невероятной точностью определить месторасположение определённого пользователя.

Главное преимущество этого способа аутентификации представляет собой относительную доступность и надежность аппаратуры GPS. Применяется GPS в случае, если необходимо определенное местонахождение удаленного пользователя для авторизации.

Я считаю, что аутентификация при помощи географического расположения самая совершенная из всех. Причина в том, что координаты спутников регулярно меняются, поэтому возможность перехватить данные месторасположения абсолютно нулевые.

Основные критерии проверки подлинности при помощи географического расположения:

- показатель затрат средний;
- показатель удобства пользования низкий;
- возможности интеграции с существующими приложениями нет;
- имеется малая вероятность возникновения ошибок;
- требуется дополнительное программное обеспечение.

1.5. Графическая и SMS-аутентификация

Этот метод близок к способу аутентификации одноразовым паролем. Но их главное отличие заключается в том, что при способе аутентификация посредством SMS-сообщения пароли отправляются пользователю на его мобильное устройство. Это дает возможность не использовать тот самый канал, по которому и осуществляется аутентификация. На мобильном устройстве пользователя могут применяться PIN-коды для доступа, эта функция гарантирует дополнительную безопасность системы.

Основные критерии проверки подлинности:

- не безопасный способ защиты, возможен перехват SMS и подделка карты, очень много атак на этот метод;
- показатель удобства высокий, прост в использовании, понятен;
- не защищен от вектора атаки прямого перебора.

Национальный институт стандартов и технологий США выступил против SMS-аутентификации еще в 2016 году.

Смысл графической аутентификации заключается в предоставлении пользователю ряда иллюстраций, которые нужно выбрать, одновременно с этим ввести текстовый пароль, который является многоразовым.

Графическая аутентификация надежна и защищает от перехватов. При этом способе сложно провести мониторинг пароля, ведь кроме текстового имеется также и графический пароль.

Основные критерии графической проверки подлинности:

- высокий показатель расходов на затраченное время и установку с обслуживанием системы;
- высокая оценка универсальности и портативности данной системы;
- отсутствует открытый интерфейс;
- возможная подмена исключена;
- система может допустить ошибку;
- требуется дополнительное программное обеспечение.[4]

Вывод

Выбор аутентификации должен соответствовать требованиям государственных законов и соответствующих стандартов, важно учитывать возможные риски и необходимые затраты. Большинство способов проверки подлинности личности основано на случайных признаках, которые не имеют непосредственного отношения к личности пользователя и могут передаваться от одного человека к другому, что определённо является большим риском.

Оптимальное всего использовать многофакторную аутентификацию. Можно предложить, например, усиление электронной системы, основанной на аппаратных ключах, при помощи пароля. Хорош также двойной пароль, одноразовый вместе с многоразовым. Способом доставки одноразового пароля остается мобильная связь, личность пользователя подтвердится в случае знания постоянного многоразового пароля. Двухфакторная аутентификация разными паролями при своей относительной защите достаточна популярна и превосходит однофакторный вариант. Но, если риски велики, то я считаю данный способ проверки подлинности, не решающим проблему, а только немного затрудняющим работу злоумышленников за счет дополнительного фактора защиты.

Безупречной защищенности системы от атак злоумышленников, к сожалению, человечество пока не достигло. Но самую большую гарантию подлинности пользователя обеспечивает биометрическая аутентификация, проверяющая часть тела пользователя, которая не передаются другому.

До террористического акта 11 сентября, который потряс не только США, но весь мир, биометрической аутентификацией пользовались исключительно для защиты военных и сугубо конфиденциальных коммерческих данных. Но после печальных событий 2001-го года отношение к информационной безопасности в мире изменилась. Биометрические системы проверки личности появились сначала в аэропортах и крупных торговых центрах, а позже их стали использовать и в иных местах большого скопления людей.

Я полагаю, что именно биометрия в будущем будет основным способом аутентификации. Но важно внести коррективы для того, чтобы информационные системы с уверенностью полагались на этот метод. Биометрическая аутентификация должна быть:

- по максимуму проста в использовании;
- технически безупречной;
- экономичной и доступной.

И тогда уже можно будет с уверенностью утверждать, что информационные системы с конфиденциальной информацией будут полагаться именно на данный способ проверки подлинности как на основной. Но я бы добавил к биометрии еще и второй фактор (как минимум) для повышения уровня защиты информации. Биометрия в ближайшем будущем может стать первостепенным и значимым фактором в вопросе аутентификации во всех сферах жизни людей, если будет применяться совместно со смарт-картами, ключами и подписями.

Проведя сравнительный анализ на соответствие существующих методов аутентификации требованиям настоящего времени, еще раз подытожу, что лучшую гарантию безопасности предоставляют системы биометрической аутентификации. Главные преимущества биометрической системы проверки подлинности – это почти нулевая подверженность атакам и сравнительно высокий критерий удобства и практичности в использовании, открытый интерфейс и возможность к интеграции.

За последние двадцать лет биометрическая аутентификация сделала значительный рывок вперед благодаря популяризации микропроцессорных технологий. Еще вчера биометрическая проверка личности казалась фантастикой, а сегодня использование биометрии в информационной системе является обычным делом. Даже на каждом мобильном телефоне имеется функция биометрической аутентификации – система распознавания по радужке глаза или лицу в целом, считывание отпечатка пальца.

Список литературы / References

1. Библиотека ГОСТов. Судебная компьютерно-техническая экспертиза. Термины и определения. [Электронный ресурс]. Режим доступа: http://vsegost.com/Catalog/64/64335.shtml/ (дата обращения: 28.11.2022).
2. Системы аутентификации – сравнение и выбор. [Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/security/authentication/ (дата обращения: 28.11.2022).
3. Системы и методы аутентификации пользователей. [Электронный ресурс]. Режим доступа: https://www.anti-alware.ru/analytics/Technology_Analysis/overview-of-user-authentication-systems-and-methods/ (дата обращения: 28.11.2022).
4. *Сухаревская Е.В.* Исследование систем аутентификации // Международный студенческий научный вестник. – 2018. – № 1. [Электронный ресурс]. Режим доступа: https://eduherald.ru/ru/article/view?id=18090/ (дата обращения: 28.11.2022).