Методы аутентификации пользователя

Студент группы ИУ7-56Б Киселёва Марина Сергеевна

Научный руководитель Григорьев Александр Сергеевич

Москва, 2022

Цель и задачи

Целью данной работы является классификация существующих методов аутентификации пользователя.

Задачи:

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

Основные виды атак на пароли

1) полный перебор;
2) подглядывание из-за плеча;
3) троянский конь;
4) перехват данных.

Базовые понятия

1) Хэш-функция — 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.
2) OTP-токен — мобильное персональное устройство, которое принадлежит определенному пользователю и генерирует одноразовые пароли.
3) Открытый и закрытый ключи — парные, зависимые друг от друга ключи. Открытый ключ позволяет 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.

Парольная аутентификация

Парольная аутентификация — аутентификация на основе обладания неким секретным знанием (многоразовым паролем).

Принцип работы:

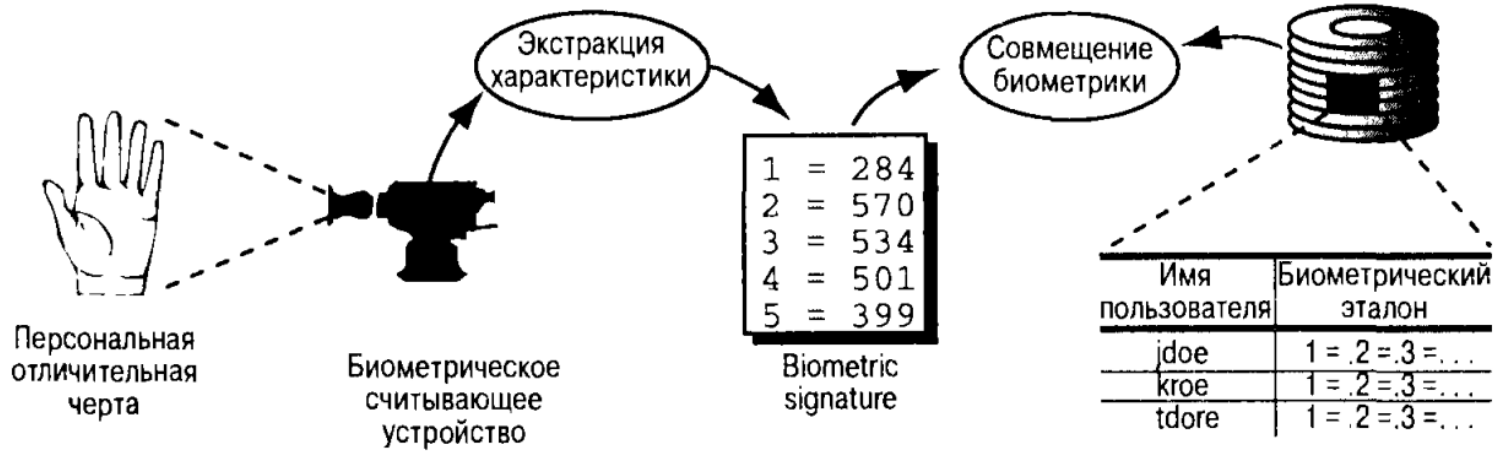
1) пользователь вводит свое имя и пароль на рабочей станции;
2) имя и пароль передаются в открытом доступе по сети;
3) сервер находит учетную запись в базе данных и сравнивает введенные данные с ее содержимым.

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

Аутентификация с использованием биометрических характеристик

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

Схема работы биометрической системы:



Аутентификация с помощью одноразовых паролей

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

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.

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.

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.

Для его хранения закрытого ключа используют специальные устройства:

1) Таблетка Touch Memory;
2) смарт-карта;

3) USB-ключ.

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

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. Достоинством такого метода является надежность и относительная дешевизна аппаратуры GPS. Ее использование необходимо в тех случаях, когда пользователь должен находиться в нужном месте, например офисном здании. Координаты спутников меняются постоянно, поэтому вероятность их перехвата равна нулю.

Графическая аутентификация

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

В большинстве случаев графические системы основаны на том, что в качестве пароля выступают либо координаты щелчков мыши, либо определенный набор символов, присвоенный графическим объектам.

Самыми часто используемыми схемами являются Passlogix, PassFaces, Pass-string и Deja Vu.

Сокращения для категорий

1) ПА — парольная аутентификация;
2) БА — биометрическая аутентификация;
3) ОП — аутентификация с помощью одноразовых паролей;
4) ОК — аутентификация с помощью открытого ключа;
5) ГМ — аутентификация через географическое местоположение;
6) ГА — графическая аутентификация.

Сокращения для критериев

1) К1 — стоимость установки и обслуживания;
2) К2 — удобство использования;
3) К3 — возможность возникновения ошибок;
4) К4 — требование наличия дополнительных программных и аппаратных средств;
5) А1 — возможность полного перебора;
6) А2 — возможность подглядеть из-за плеча;
7) А3 — возможность перехвата пароля;
8) А4 — возможность троянского коня.

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

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 была достигнута — классифицированы методы аутентификации пользователя.

Были выполнены следующие задачи:

1) описаны основные виды атак на пароли;
2) рассмотрены базовые элементы и понятия, используемые при проектировании методов аутентификации;
3) проведен анализ существующих методов аутентификации пользователя;
4) проведена классификация на основе выделенных критериев.