Программно-аппаратные средства обеспечения информационной безопасности. Аутентификация. Лекция 7

Аутентификация

- **Аутентифика́ция** (*Authentication*) — проверка принадлежности субъекта доступа по предъявленному им идентификатору; подтверждение подлинности.
- Учитывая степень доверия и прочие свойства систем, проводимая проверка может быть односторонней или взаимной. Обычно она проводится с помощью криптографической обработки, позволяющей защитить передаваемые данные от злоумышленников.
- Аутентификацию не следует путать с идентификацией (процедурой распознавания субъекта по его идентификатору) и авторизацией (процедурой предоставления определенных прав субъекту). Идентификация и аутентификация являются тесно связанными процессами распознавания и проверки подлинности пользователей

ТИПОВЫЕ СХЕМЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

ID_i - неизменный идентификатор i- ого пользователя

K_i - аутентифицирующая информация пользователя, которая может изменяться и служит для аутентификации (например, пароль $P_i = K_i$).

Схема 1. Структура эталона

Номер пользователя	Идентификатор	Аутентификатор
1	Id_1	$E_1=F(Id_1,K_1)$
2	Id_2	$E_2=F(Id_2,K_2)$
3	Id_3	$E_3=F(Id_3,K_3)$
…	…	…
n	Id_n	$E_n=F(Id_n,K_n)$

Протокол идентификации и аутентификации

1.Предъявление идентификатора ID.

2.Проверка существования ID_i = ID для прохождения аутентификации.

3.Запрс у пользователя его аутентификатора K.

4.Вычисление значения $Y = F(ID_i ,K)$.

5. Сравнение значений Y и E_i . Допуск при равенстве Y и E_i.

ТИПОВЫЕ СХЕМЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

- В **схеме1** F- функция, которая обладает свойством «невосстановимости» значения K_i по E_i и ID_i . «Невосстановимость» оценивается некоторой пороговой трудоемкостью T_o решения задачи восстановления K_i по E_i и ID_i. На практике задают $T_o = 10^{20} \ldots 10^{30}$.
- Для пары K_i и K_j возможно совпадение соответствующих значений E. В связи с этим вероятность ложной аутентификации не должна быть больше некоторого порогового значения P_o . На практике задают $P_o = 10^{-7} \ldots 10^{-9}$.

ТИПОВЫЕ СХЕМЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ (2)

ID_i - неизменный идентификатор i- ого пользователя

K_i - аутентифицирующая информация пользователя, которая может изменяться и служит для аутентификации (например, пароль $P_i = K_i$)

S_i - случайный вектор, создаваемый при создании идентификатора пользователя

Схема 2. Структура эталона

Номер пользователя	Идентификатор	Аутентификатор
1	Id_1, S_1	$E_1=F(S_1,K_1)$
2	Id_2 , S_2	$E_2=F(S_2,K_2)$
3	Id_3, S_3	$E_3=F(S_3,K_3)$
…	…	…
n	Id_n , S_n	$E_n=F(S_n ,K_n)$

Протокол идентификации и аутентификации

1.Предъявление идентификатора ID.

2.Проверка существования ID_i = ID для прохождения аутентификации.

3. По идентификатору ID_i выделяется вектор S_i .

4.Запрос у пользователя его аутентификатора K.

5.Вычисление значения $Y = F(S_i ,K)$.

6. Сравнение значений Y и E_i . Допуск при равенстве Y и E_i.

аутентификации/идентификац

Средства аутентификации/идентификации можно разделить на три группы, в соответствии с применяемыми принципами:

- принцип «что вы знаете» («you know»), лежащий в основе методов аутентификации по паролю;
- принцип «что вы имеете» («you have»), когда аутентификация осуществляется с помощью магнитных карт, токенов и других устройств;
- принцип «кто вы есть» («you are»), использующий персональные свойства пользователя (отпечаток пальца, структуру сетчатки глаза и т.д.).

Актуальность биометрической аутентификации

Специалистам по информационной безопасности хорошо известны случаи, когда сотрудники передают смарт-карты и пароли своим коллегам. При этом сотрудники могут не осознавать всех рисков, которым они подвергают компанию. В связи с этим возникает задача: как сделать смарт-карты неотчуждаемыми от пользователя? Это особенно актуально для организаций, работающих с критическими данными, несанкционированный доступ к которым может привести к серьёзному ущербу

Биометрическая идентификация и аутентификация

Основные достоинства.

Высокая степень достоверности из-за уникальности биометрических признаков.

Неотделимость биометрических признаков от дееспособной личности.

Трудность фальсификации биометрических признаков.

ВАРИАНТЫ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ

В настоящее время проводятся интенсивные исследования, направленные на расширение возможностей биометрии в таких методах идентификации, как:

- **По отпечаткам пальцев**
- **По геометрии кисти руки** – пользователи предпочитают
- По отпечатку ладони
- По строению кровеносных сосудов
- По термографии лица
- **По форме лица в двух-, трехмерном измерении**
- **По особенностям голоса**
- По запаху
- По подписи
- По динамике печатания
- По походке
- **По радужной оболочке глаза; вероятность повторения – 10^{-78}**
- **По сетчатке глаза**

Реализация физиологических биометрических характеристик (1)

Биометрическая характеристика	Регистрирующее устройство	Образец	Исследуемые черты
Радужная оболочка глаза	Видеокамера	Чёрно-белое изображение радужной оболочки глаза	Полоски и бороздки в радужной оболочке глаза
Отпечаток пальца	Периферийное устройство настольного компьютера, карта стандарта *PC card, мышь, микросхема или считыватель, встроенный в клавиатуру*	Изображение отпечатка пальцев (оптическое, на кремниевом фотоприёмнике, ультразвуковое или бесконтактное)	Расположение и направление гребешковых выступов и разветвлений на отпечатке пальцев, мелкие детали

Реализация физиологических биометрических характеристик (2)

Биометрическая характеристика	Регистрирующее устройство	Образец	Исследуемые черты
Лицо	Видеокамера, камера для ПК, фотоаппарат	Изображение лица (оптическое или тепловое)	Относительное расположение и форма носа, расположение скул
Кисть	Настенное устройство	Трёхмерное изображение верха и боков кисти	Высота и ширина костей и суставов кисти и пальцев
Сетчатка	Специализированная видеокамера	Изображение сетчатки	Расположение кровеносных сосудов на сетчатке

Реализация поведенческих биометрических характеристик

Таблица 2. Реализация поведенческих биометрических характеристик.

Биометрическая характеристика	Регистрирующее устройство	Образец	Исследуемые черты
Голос	Микрофон, телефон	Запись голоса	Тембр, модуляция и продолжительность голосового образа
Подпись	Планшет для подписи, перо для ввода данных	Изображение подписи и показания соответствующих динамических измерений	Скорость, порядок линий, давление и внешний вид подписи
Голос	Микрофон, телефон	Запись голоса	Тембр, модуляция и продолжительность голосового образа
Динамика нажатия клавиш	Специализированная клавиатура	Ритм машинописи	Время задержки (промежуток времени, в течение которого пользователь удерживает конкретную клавишу), время "полёта" (промежуток времени, который требуется пользователю для перехода с одной клавиши на другую)

Программа PIV

В настоящее время решения с использованием биометрии на основе технологии Match-on-Card (вычисления на карте) успешно внедряются крупнейшими мировыми компаниями. Национальный Институт стандартов и технологий (NIST, США) принял решение включить Match-on-Card в программу PIV (Personal Identification Verification), стандартизирующую методы электронной идентификации и аутентификации всех федеральных служащих США. Все правительственные учреждения США внедряют программу PIV с 2012 года.

2 технологии

- Технология Match-on-Card, используемая на смарт-картах, например, ESMART® Token ГОСТ, является более защищенной по сравнению с технологией Template-on-Card (англ. «шаблон на карте»), когда решение о том, совпадают ли шаблоны, принимает программное обеспечение считывателя.

Точность биометрической системы (1)

Точность биометрической системы измеряется двумя параметрами, заданными администратором при выпуске смарт-карты:

FRR (False Rejection Rate) – коэффициент ложного отказа в доступе или вероятность того, что человек может быть не распознан системой. В биометрических системах называется "type I errors" ("ошибка первого рода") или "чувствительность";

Точность биометрической системы (2)

FAR (False Acceptance Rate) – коэффициент ложного доступа или порог, определяющий вероятность того, что один человек может быть принят за другого. Имеет название "type II errors" ("ошибка второго рода") или "специфичность".

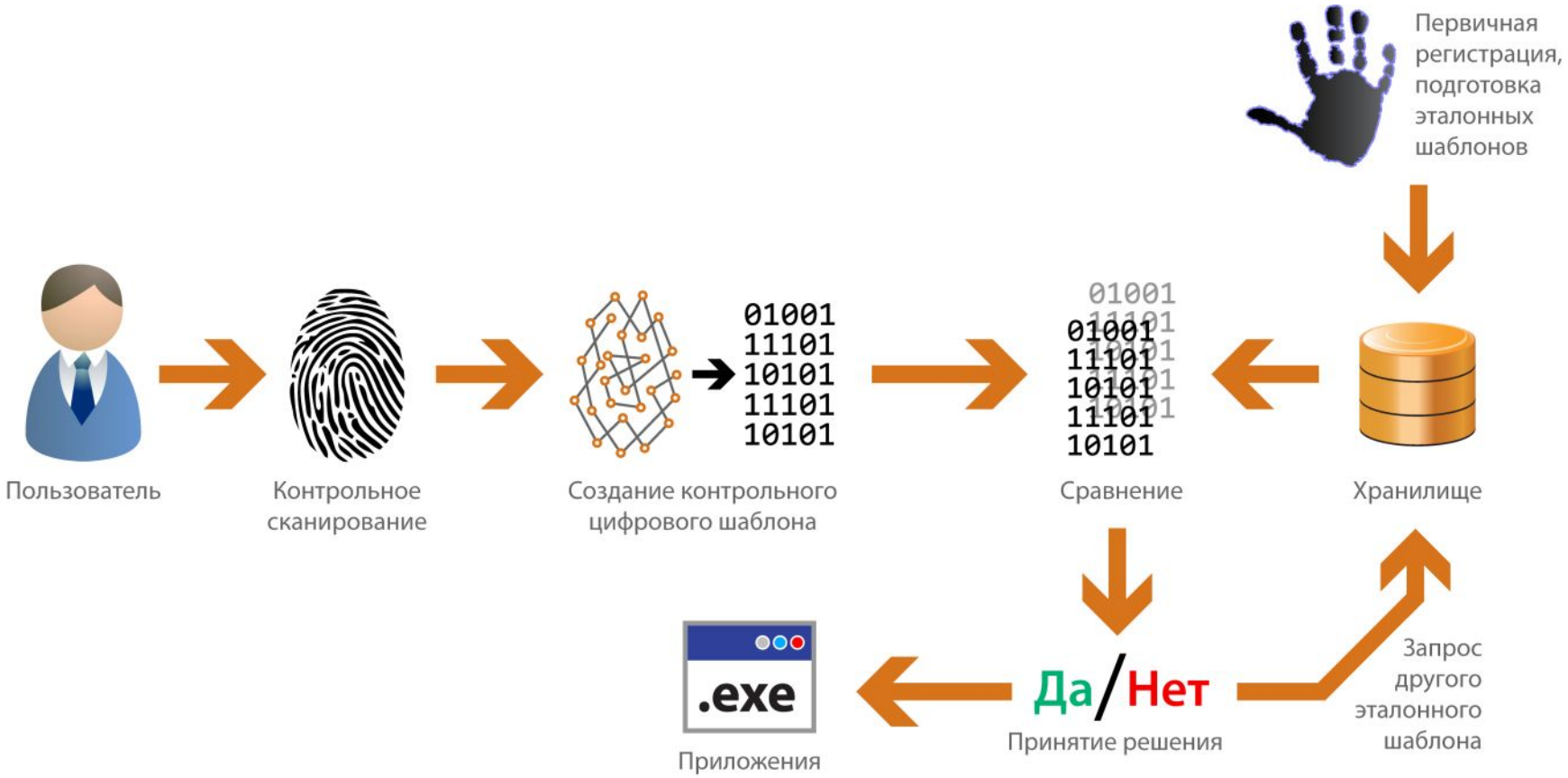
Системы с низким значением FRR более комфортны для пользователей, а системы с низким значением FAR более защищены.

Типичные значения FRR — порядка одной ошибки на 100. FAR — порядка одной ошибки на 10 000.

Точность биометрической системы (3)

В общем случае, при задании пороговых величин действует правило: чем ниже FRR, тем больше FAR и наоборот. Таким образом, безопасность и комфорт конкурируют между собой, а оптимальные параметры настраиваются администратором системы

Основные элементы биометрической системы доступа



СТРУКТУРА СИСТЕМЫ

Продукт компании "Аладдин Р. Д."

Предлагается современное решение биометрической аутентентификации JaCarta PKI/BIO, построенное на основе архитектуры Match-on-Card (вычисления на карте). Важным преимуществом является то, что хранение цифровых образцов отпечатков и принятие решения "свой/чужой" выполняются в защищённой области смарт-карты, а не на сервере биометрической идентификации. Цифровые образы отпечатков никуда не пересылаются и не создаются биометрические базы данных пользователей. Таким образом, даже администраторы системы не имеют доступа к биометрической информации сотрудников.

Аутентификация: факторы и их комбинации

- Внедрение решения аутентификации на основе JaCarta PKI/BIO не означает отмены существующих, а лишь дополняет и усиливает их.
- Возможны следующие комбинации аутентификационных факторов:
- • электронный ключ + PIN-код;
- • электронный ключ + отпечаток пальца;
- • электронный ключ + PIN-код + отпечаток пальца.

Интересно

Столица Индонезии, имя которой фонетически неразличимо с JaCarta, расположена на острове Ява, давшем название одноимённому сорту кофе, в честь которого, в свою очередь, назван язык программирования Java, на котором основана технология Java Card, используемая в продуктах JaCarta.

Трехфакторная аутентификация

- Биометрическую аутентификацию можно совместить с требованием ввода пользователем пароля (PIN-кода) для электронного ключа. Совместное использование биометрических данных и пароля обеспечивает надёжную трёхфакторную аутентификацию.
- Для усиления безопасности рекомендуется использовать пароль, не ограничиваясь только отпечатком пальца

JaCarta PKI

JaCarta PKI предназначена **для корпоративных пользователей**, имеющих развёрнутую инфраструктуру открытых ключей (PKI), при этом поддержка JaCarta PKI в продуктах мировых вендоров обеспечивается **штатными** средствами. JaCarta PKI выполнена на современной открытой технологической платформе Java Card с учётом огромного накопленного опыта разработки как средств строгой аутентификации, средств электронной подписи, так и инфраструктуры применения смарт-карт и USB-токенов.

Одноразовые пароли (1)

- В настоящее время на смену обычным фиксированным паролям пришли одноразовые пароли (One-Time Password (OTP)).

  Одноразовые пароли удобны в использовании, так как их не нужно запоминать, каждый раз генерируется новое значение. Системы одноразовых паролей позволяют противостоять атакам анализатора трафика. Даже если злоумышленник перехватит такой пароль, он не сможет его использовать в дальнейшем. Это делает системы одноразовых паролей более надежными по сравнению с обычными фиксированными паролями.

Одноразовые пароли (2)

- **Технологии использования одноразовых паролей можно разделить на:**
- Использование генератора псевдослучайных чисел, единого для субъекта и системы
- Использование временных меток вместе с системой единого времени
- Использование базы случайных паролей, единого для субъекта и для системы

Метод аутентификации с одноразовыми паролями (1)

- В методе использования генератора псевдослучайных чисел, единого для субъекта и системы используется генератор псевдослучайных чисел с одинаковым значением для субъекта и для системы. Сгенерированный субъектом пароль может передаваться системе при последовательном использовании односторонней функции

Метод аутентификации с одноразовыми паролями (2)

- Во втором методе используются **временные метки**. В качестве примера такой технологии можно привести **SecurID,** разработанную компанией RSA**.** Она основана на использовании аппаратных ключей (токенов) и синхронизации по времени. Аутентификация основана на генерации случайных чисел через **определенные временные интервалы (60 сек.)**. Уникальный **секретный ключ** хранится только в базе системы и в аппаратном устройстве субъекта. Когда субъект запрашивает доступ в систему, ему предлагается ввести PIN-код (4 цифры), а также случайно генерируемое число, отображаемое в **этот момент** на аппаратном устройстве (токен-код 6 цифр) . **Система** сопоставляет введенный PIN-код и секретный ключ субъекта из своей базы и генерирует случайное число, основываясь на **параметрах секретного ключа из базы и текущего времени.** Далее проверяется идентичность сгенерированного числа и числа, введённого субъектом (токен-кода).

Метод аутентификации с одноразовыми паролями (3)

- Третий метод основан на единой базе паролей для субъекта и системы и **высокоточной** синхронизации между ними. При этом каждый пароль из набора может быть использован только один раз. Благодаря этому, даже если злоумышленник перехватит используемый субъектом пароль, то он уже будет недействителен.

Система S/Key генерации одноразовых паролей.

- **S/Key** — система одноразовых паролей S/Key, определенная в RFC 1760, представляет собой систему генерирования одноразовых паролей на основе стандартов MD4 и MD5. Она предназначена для борьбы с так называемыми «повторными атаками», когда хакер подслушивает канал, выделяет из трафика аутентификатор пользователя и его пароль и в дальнейшем использует их для несанкционированного доступа.

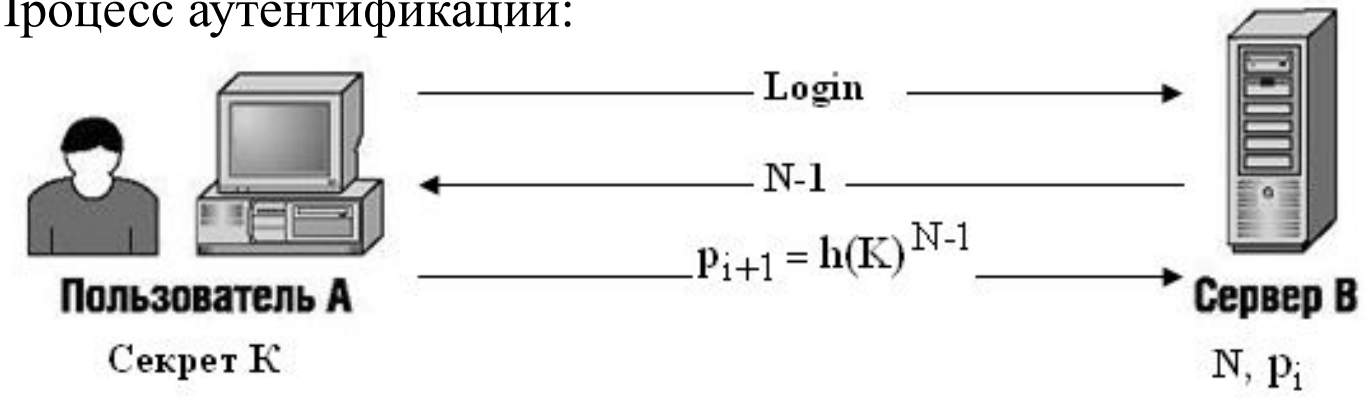
Система S/Key генерации одноразовых паролей. Архитектура.

Генерация одноразовых паролей:

$$p_0 = h(K)^N, \quad p_1 = h(K)^{N-1}, \ldots, \quad p_i = h(K)^{N-i}, \ldots, p_{N-1} = h(K)$$

K – вектор инициализации, N – целое число, h – хэш-функция, $0 \le i \le N-1$.

Процесс аутентификации:



1) Пользователь посылает серверу свой логин.
2) Сервер в ответ посылает число N-1.
3) Пользователь вычисляет одноразовый пароль $p_{i+1} = h(K)^{N-1}$ и отправляет результат серверу.
4) Сервер вычисляет $p_i' = h(p_{i+1})$. Если $p_i' = p_i$, пользователь – подлинный.

Алгоритм аутентификации S/Key (1)

- Предполагается, что пользователю известна секретная величина k. На предварительном этапе k объединяется со случайной величиной S, присланной сервером. В результате получается некоторая величина K=(k || S).

Алгоритм аутентификации S/Key (2)

- Далее пользователь выбирает некоторое целое число N, лежащее в диапазоне от 500 до 1000. Генерирует первый одноразовый пароль путем применения хэш-функции к значению (k || S) N раз. Следующий одноразовый пароль будет генерироваться путем применения хэш-функции к значению (k || S) только (N - 1) раз и т.д. Таким образом формируется последовательность одноразовых паролей, используемых для аутентификации.

Алгоритм аутентификации S/Key (3)

- Пользователь посылает на сервер первое значение одноразового пароля Po, вычисленное по формуле и число N.

  Данный пароль для аутентификации не используется, а выступает для сервера в роли начального значения, на основе которого будет проверяться следующий присланный пользователем во время аутентификации одноразовый пароль.

Достоинства системы S/key

а) Защита от повторного использования пароля. Одноразовый пароль действителен только один раз, и повторно для аутентификации его использовать нельзя.

б) Вектор инициализации k не хранится на сервере и не передается по сети. Поэтому у злоумышленника отсутствует возможность его перехватить, следовательно, без знания секрета, он не сможет сгенерировать правильный одноразовый пароль.

Недостатки системы S/key (1)

а) Ограниченное количество генерируемых паролей, заданных величиной N. Так как эта величина каждый раз уменьшается на единицу, то при ее обнулении либо пользователю необходимо заново выбирать вектор инициализации k, либо сервер должен сгенерировать новую случайную величину S. Кроме того, нужно установить новое значение счетчика N. Все это вносит ряд дополнительных неудобств для пользователя.

Данный недостаток будет не так заметен, если выбрать достаточно большое значение счетчика N, но в этом случае возникает проблема б).

Недостатки системы S/key (2)

- б) При больших значениях N увеличивается время генерации одноразового пароля на стороне пользователя. Это связано с тем, что величина N влияет на количество итераций хеширования. Когда значение счетчика равно, например, 1000, чтобы вычислить одноразовый пароль, пользователю потребуется тысячу раз применить хеш-функцию, что в свою очередь требует существенных временных затрат.
- в) Отсутствует аутентификация сервера.

Механизмы проверки взаимной подлинности

Основные механизмы, используемые для подтверждения подлинности:

- запроса-ответа (используется для аутентификации участников)
- временной штемпель (используется для аутентификации связи)

Механизм запрос-ответ

- Пользователь А (проверяющий) включает в посылаемое для В сообщение непредсказуемый элемент- запрос X (например, некоторое случайное число). При ответе В должен вычислить некоторую функцию f(X). Получив правильный ответ, А может быть уверен в подлинности В. Недостаток – возможность установления закономерности между запросом и ответом, т. е. определения вида функции f. Устранение – использование шифрования.

Механизм отметки времени («временной штемпель»)

Механизм подразумевает регистрацию времени для каждого сообщения. В этом случае каждый пользователь может определить, насколько «устарело» пришедшее сообщение, и решить не принимать его, так как это может быть повтор сообщения, потерявшего свою актуальность.

При использовании отметок времени возникает проблема допустимого временного интервала задержки для подтверждения подлинности.

ВЗАИМНАЯ АУТЕНТИФИКАЦИЯ «РУКОПОЖАТИЕ»

Пользователь А инициирует процедуру рукопожатия и осуществляет проверку подлинности В как показано на рисунке. Пользователь В проверяет подлинность А аналогично. Обе процедуры образуют рукопожатие.