Лекция 6. Аутентификация при локальном и удаленном доступе

- Программно-аппаратная защита от локального НСД.
- Аутентификация пользователей по их биометрическим характеристикам.
- Прямая аутентификация при удаленном доступе.

Программно-аппаратная защита от локального НСД

Порядок активизации программ после включения питания компьютера и до загрузки операционной системы:

1. программа самопроверки устройств компьютера POST (Power On – Self Test);
2. программа BIOS Setup (может быть вызвана пользователем во время выполнения программы POST, обычно для этого необходимо нажать клавишу Delete),
3. программы BIOS;

Порядок активизации программ

4. программы расширения BIOS (BIOS Extension), если соответствующая плата установлена на компьютере;
5. программа начальной загрузки, которая размещается в первом секторе нулевой головки нулевого цилиндра жесткого диска компьютера (Master Boot Record, MBR) и в функции которой входит определение активного раздела жесткого диска и вызов программы загрузки операционной системы;
6. программа загрузки операционной системы, которая размещается в первом секторе активного раздела жесткого диска, загрузочного компакт-диска или загрузочной дискеты;
7. оболочка операционной системы.

Невозможность надежной аутентификации только программными средствами

- Если программа начальной загрузки содержит вредоносный код, то и загруженная затем операционная система будет фактически функционировать под управлением программы нарушителя.
- Если нарушитель получит доступ к коду процедуры хеширования пароля пользователя и его хеш-значению, он сможет подобрать пароль любого пользователя КС и осуществить несанкционированный доступ к информации.

Программно-аппаратная защита от локального НСД

- Для гарантированной работы программно-аппаратного средства защиты от несанкционированной загрузки операционной системы достаточно, чтобы программа защиты и хеш-значения паролей пользователей были аппаратно защищены от чтения программными средствами во время сеанса работы пользователя (после загрузки ОС).

Модель (возможности) нарушителя

- установка системы защиты производится в его отсутствие;
- нарушитель не может вскрыть системный блок компьютера;
- нарушитель не может перезаписать информацию в ПЗУ BIOS при работающем компьютере;
- нарушитель не имеет пароля установки системы защиты;
- нарушитель не имеет пароля пользователя КС;
- нарушитель не имеет копии ключевой информации пользователя, хранящейся в элементе аппаратного обеспечения (например, в элементе Touch Memory).

Программно-аппаратная защита от локального НСД

- Программные средства системы защиты должны быть записаны на плате расширения BIOS, для каждой из которых определен уникальный пароль установки. Установка системы защиты производится на компьютере, свободном от вредоносных программ типа закладок и вирусов. После установки платы расширения BIOS выполняется процедура установки системы защиты.

Электронный замок для защиты от локального НСД

Установка системы защиты

1. После включения питания компьютера программа, записанная на плате расширения BIOS, выдает запрос на ввод пароля.
2. После ввода пароля установки P_S (как правило, администратором системы) происходит загрузка операционной системы и запуск собственно программы установки (проверочные функции системы защиты при этом отключаются).
3. По запросу программы установки вводятся пароль пользователя P, ключевая информация с элемента аппаратного обеспечения (например, серийный номер элемента Touch Memory) KI и имена подлежащих проверке системных и пользовательских файлов F_1, F_2, … , F_n.

Установка системы защиты

4. Для каждого указанного файла F_i вычисляется и сохраняется проверочная информация в виде

$E_k(H(P_S, P, KI, F_i))$ (E – функция шифрования, k – ключ шифрования, H – функция хеширования).

Проверочная информация сохраняется в скрытых областях жесткого диска (или на самом электронном замке).

Вход пользователя в КС

1. После включения питания компьютера программа на плате расширения BIOS запрашивает имя и пароль пользователя и просит установить элемент аппаратного обеспечения с его ключевой информацией.
2. Осуществляется проверка целостности выбранных при установке системы защиты файлов путем вычисления хеш-значения для них по приведенному выше правилу и сравнения с расшифрованными эталонными хеш-значениями;
3. В зависимости от результатов проверки выполняется либо загрузка операционной системы, либо запрос на повторный ввод пароля.

Программно-аппаратная защита от локального НСД

- После завершения работы пользователя элемент аппаратного обеспечения с его ключевой информацией изымается из компьютера. Доступ же к хеш-значению пароля фактически заблокирован, так как программное обеспечение для его вычисления и сравнения с эталоном «исчезает» из адресного пространства компьютера и не может быть прочитано никакими программными средствами без извлечения платы расширения BIOS.

Программно-аппаратная защита от локального НСД

- Если у нарушителя нет пароля пользователя или копии элемента аппаратного обеспечения с его ключевой информацией, то он не сможет выполнить загрузку операционной системы.
- Если у нарушителя есть пароль установки системы защиты, что позволит ему загрузить операционную систему без проверочных функций, или он получил доступ к терминалу с уже загруженной операционной системой, то он сможет осуществить несанкционированный доступ (НСД) к информации, но не сможет внедрить программные закладки для постоянного НСД.
- Наличие пароля установки без знания пароля пользователя или его ключевой информации не позволит нарушителю переустановить систему защиты для постоянного НСД.

Компоненты систем биометрической аутентификации

- Устройства считывания биометрических характеристик.
- Алгоритмы сравнения измеренных биометрических характеристик с эталонными из учетной записи пользователя.

Биометрические характеристики

- Физические характеристики человека (статические).
- Поведенческие характеристики (динамические).

- Максимальная уникальность (в т.ч. для близнецов), постоянство в течение длительного периода, отсутствие воздействия состояния человека или косметики.
- Не требуется измерение одного и того же параметра для снижения риска воспроизведения.

Аутентификация по отпечаткам пальцев

Мышь со сканером

Папиллярные узоры уникальны

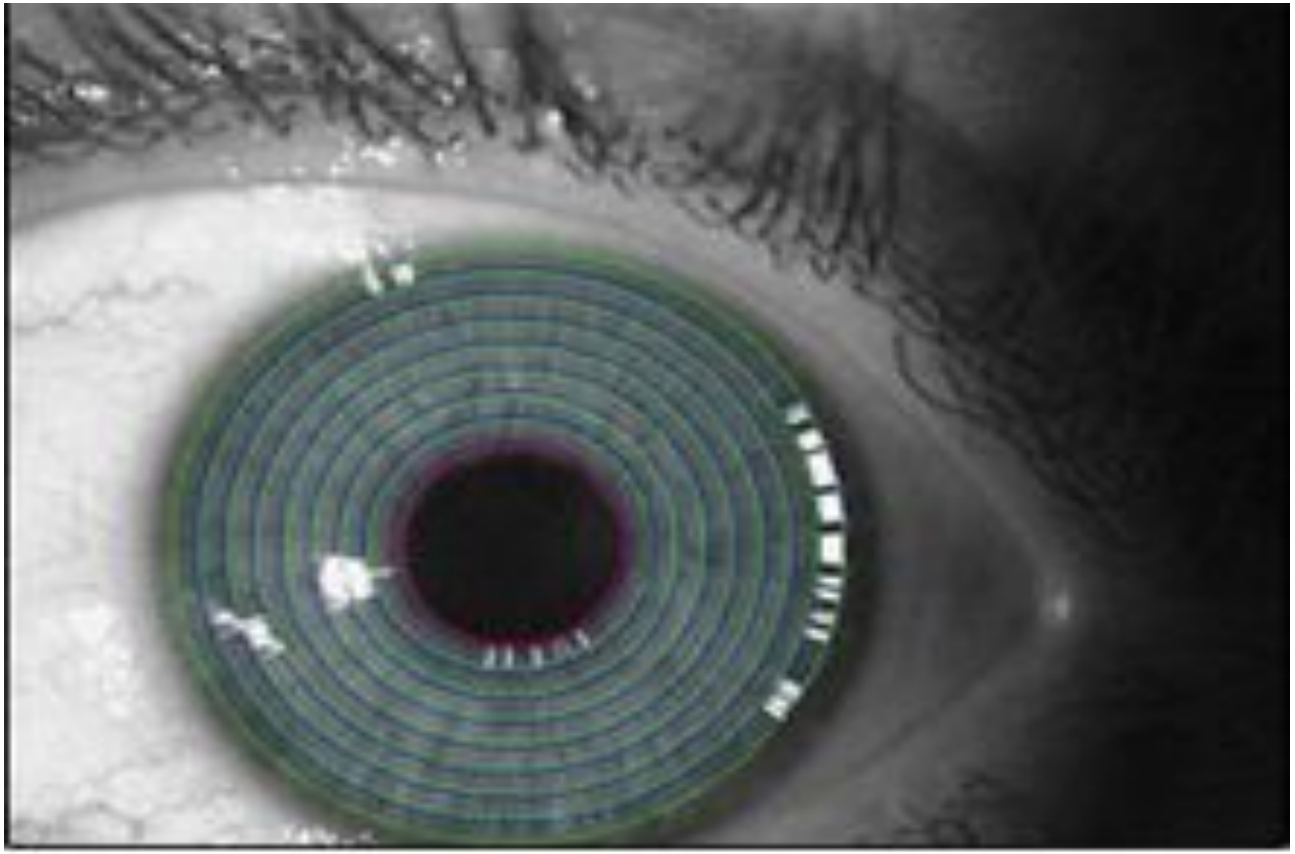
Ноутбук со сканером

Аутентификация по геометрической форме руки

Камера и несколько подсвечивающих диодов

Система распознавания по радужной оболочке глаза

Портативный сканер сетчатки глаза



Может поместиться, например, в мобильном телефоне.

3D-сканер лица

Работает в инфракрасном диапазоне.

Другие статические биометрические характеристики

- Термограмма лица (схема расположения кровеносных сосудов лица). Используется специально разработанная инфракрасная камера.
- Фрагменты генетического кода (ДНК) - в настоящее время эти средства применяются редко по причине их сложности и высокой стоимости.

Термограмма лица, шеи и передней поверхности груди

Динамические биометрические характеристики

- Голос.
- Рукописная подпись.
- Темп работы с клавиатурой (клавиатурный «почерк»).
- Темп работы с мышью («роспись» мышью).

Зависят от физического и психического состояния человека (в определенных случаях может являться преимуществом).

Графический планшет для ввода рукописной подписи

Создание биометрического эталона

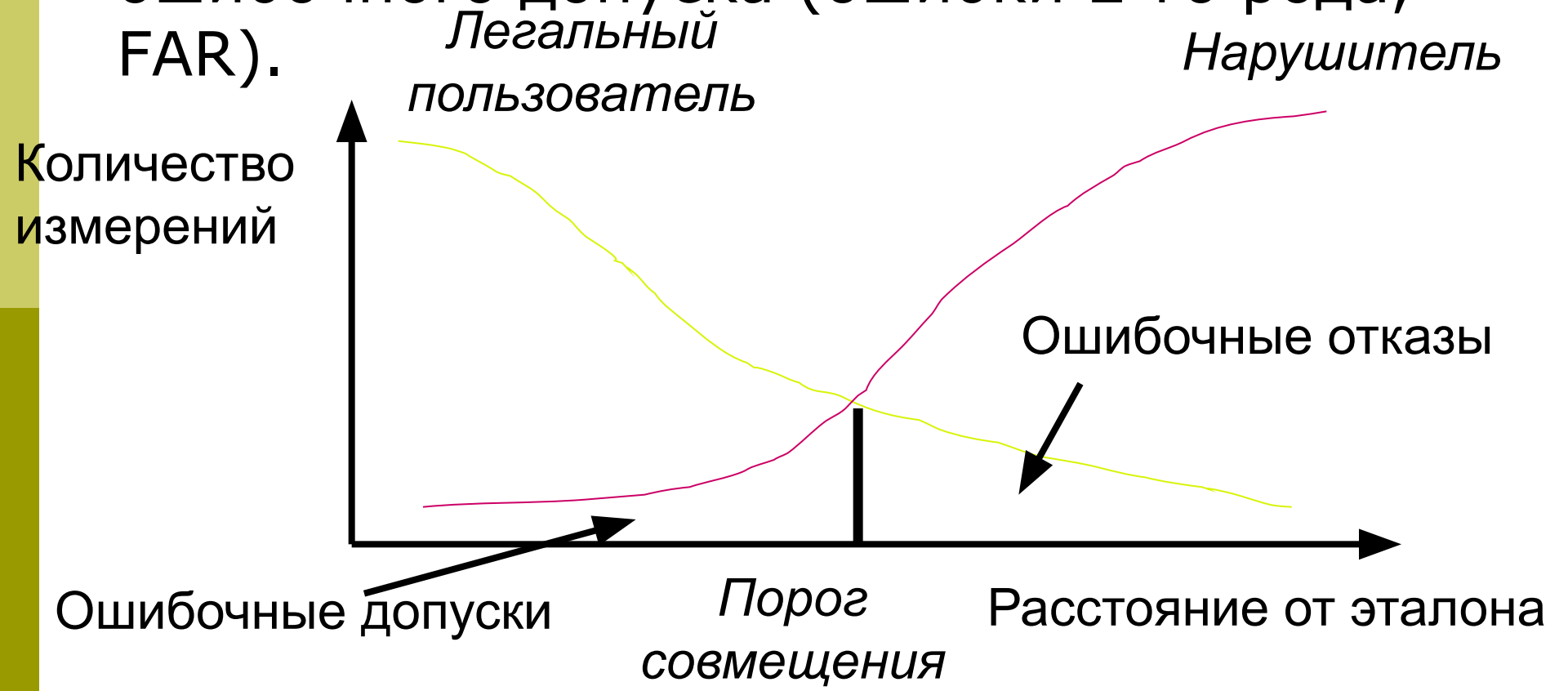
- Требуется достаточное количество измерений (для исключения естественных расхождений в измерениях и получения достоверного эталона).
- Возможно снятие нескольких подписей (например, отпечатков нескольких пальцев) для снижения риска ошибочного отказа.
- Иногда может потребоваться обучение пользователя, если снимаемая характеристика подвержена большим вариациям.

Проверка биометрической подписи

- В отличие от проверки паролей не требуется точное совпадение считанной биометрической подписи и эталона, сравниваются округленные значения.
- Для хранения биометрического эталона не может применяться хеширование.

Оценка точности биометрической аутентификации

Две оценки: вероятность ошибочного отказа (ошибки 1-го рода, FRR) и вероятность ошибочного допуска (ошибки 2-го рода, FAR).

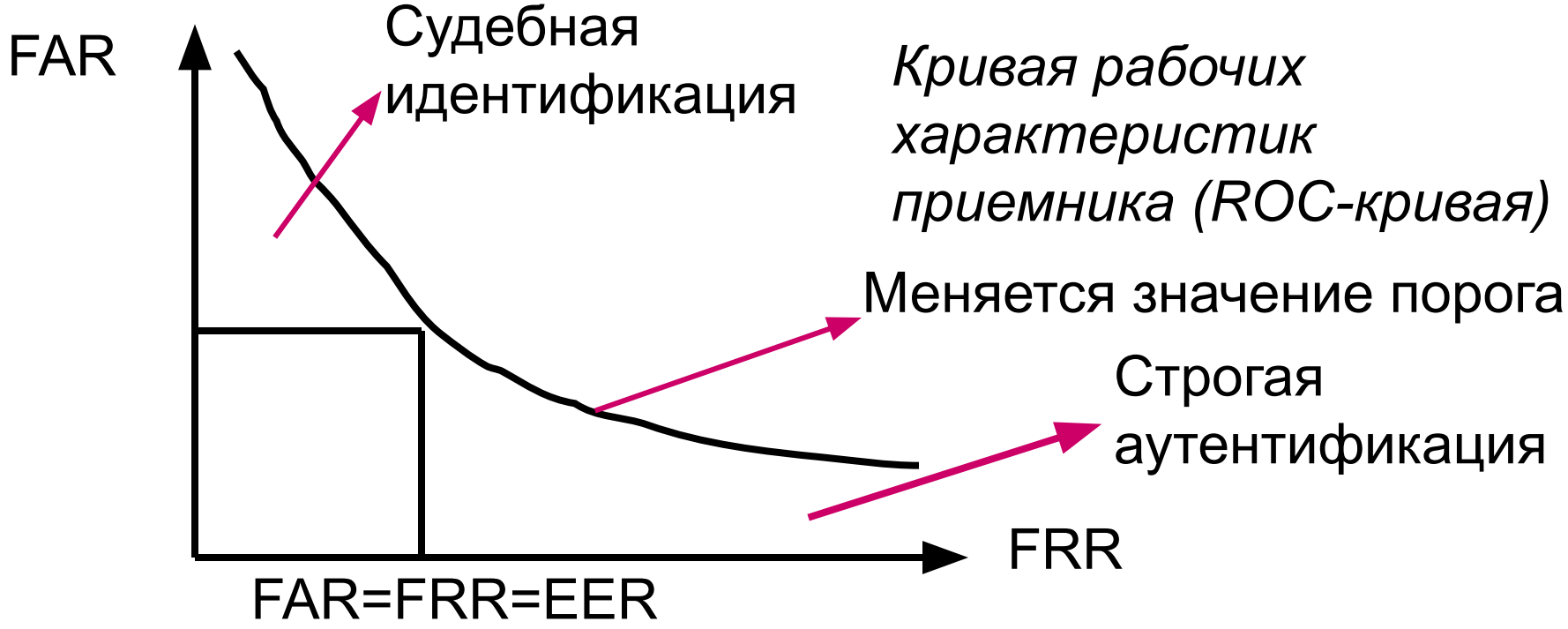


Настройка системы биометрической аутентификации

- Необходимо достижения компромисса между уровнем безопасности и удобством использования.
- Уменьшение порога допустимого отклонения от эталона снижает риск ошибочного допуска, но увеличивает риск ошибочного отказа.

Равная интенсивность ошибок

Т.к. FRR и FAR зависят от порога, для объективной оценки точности биометрической системы используется коэффициент ERR.



Чем меньше ERR, тем выше обеспечиваемый уровень безопасности.

Достоинства и недостатки биометрической аутентификации

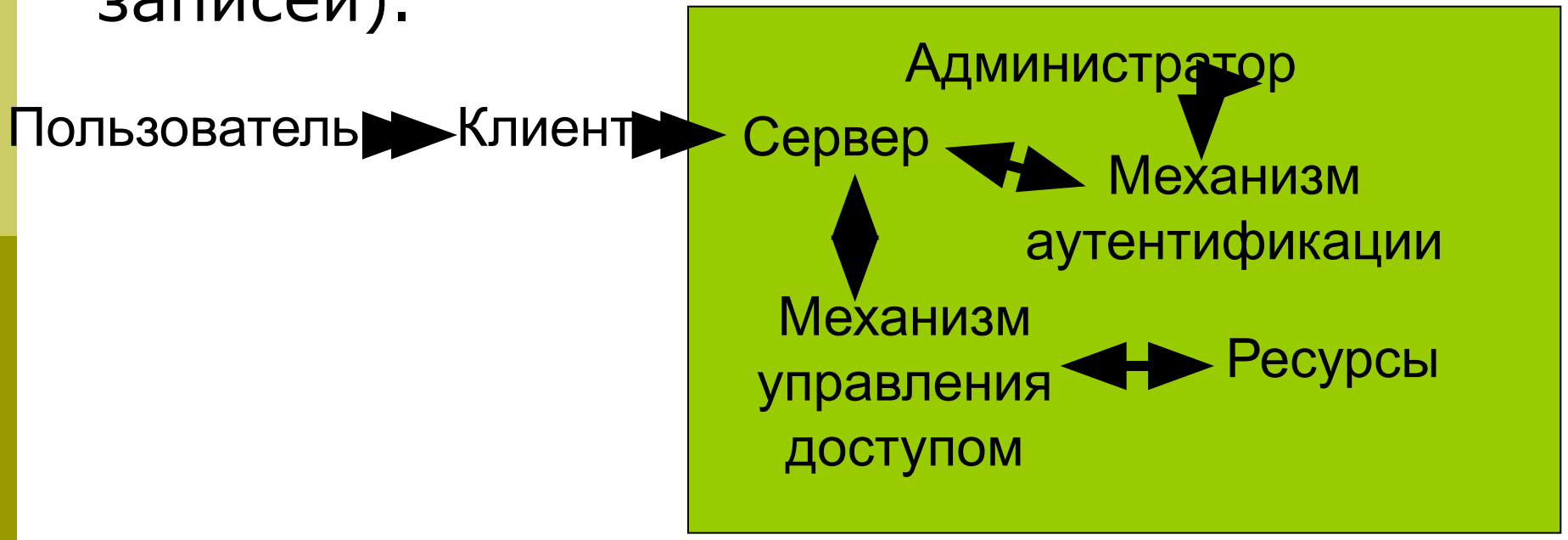
- трудность фальсификации этих признаков;
- высокая достоверность аутентификации из-за уникальности таких признаков;
- неотделимость биометрических признаков от личности пользователя.
- более высокая стоимость по сравнению с другими средствами аутентификации;
- возможность отказа легальному пользователю;
- возможность утечки персональных данных и нарушения тайны частной жизни.

Аутентификация при удаленном доступе

- Аутентифицирующая информация передается по открытым каналам связи.
- Угроза перехвата и воспроизведения нарушителем аутентифицирующей информации (паролей в открытом или хешированном виде, биометрических данных) для «маскарада».
- Угроза подмены ответа выделенного сервера аутентификации.

Прямая аутентификация

Существует одна точка обслуживания (сервер) или каждая точка обслуживания самостоятельно аутентифицирует своих пользователей (имеет свою базу учетных записей).



Протокол S/Key

- Идея протокола S/Key основывается на модели одноразовых паролей, получаемых последовательным применением необратимой (односторонней) функции (например, функции хеширования).
- Протокол S/Key состоит из двух частей – генерации списка одноразовых паролей (парольной инициализации) и собственно аутентификации.

Процедура парольной инициализации

Сервер аутентификации AS вычисляет предварительный одноразовый пароль $Y_{M+1}=H^{(M+1)}(N,P)=H(H(\ldots(H(N,P))\ldots))$ (M+1 раз выполняется хеширование) и сохраняет N (случайное число), M (количество неиспользованных одноразовых паролей), Y_{M+1} вместе с ID и P (именем и секретным паролем пользователя) в регистрационной базе данных.

- N используется для исключения передачи по сети секретного пароля пользователя P для генерации нового списка одноразовых паролей.

Процедура аутентификации по протоколу S/Key

1. Клиент C->AS: ID пользователя U.
2. AS: извлечение из регистрационной базы данных соответствующих ID значений N, M, Y_{M+1}.
3. AS->C: N, M.
4. U->C: P.
5. C: вычисление $Y_M = H^{(M)}(N,P)$.
6. C->AS: Y_M.
7. AS: вычисление $H(Y_M)$ и сравнение этого хеш-значения с Y_{M+1}, если эти значения совпадают, то пользователь авторизуется, а в регистрационной базе данных соответствующее ID значение Y_{M+1} заменяется значением Y_M, а значение M уменьшается на 1.

Протокол CHAP

- Challenge Handshake Authentication Protocol
- Идеей протокола CHAP является передача клиентом пароля в хешированном виде с использованием полученного от сервера случайного числа.

Протокол CHAP

1. Сервер аутентификации AS: генерация случайного числа N.
2. AS->Клиент C: идентификатор сервера ID_S, N и его длина в байтах (вызов).
3. Пользователь U->C: пароль P.
4. C: вычисление хеш-значения $R=H(ID_S, N, P)$.
5. C->AS: ID_U, R (отклик).
6. AS: извлечение из регистрационной базы данных соответствующего ID_U значения P, вычисление хеш-значения $H(ID_S, N, P)$ и сравнение его с R.
7. AS->C: если хеш-значения совпадают, то авторизация U, иначе отказ в доступе и разрыв соединения.

Используемое в протоколе CHAP значение *N*

Обычно при реализации протокола CHAP в качестве *N* выбирается последовательность битов, представляющая значение текущих даты и времени в секундах, к которой присоединяется случайное число, полученное от программного или аппаратного генератора псевдослучайных чисел.