4. Идентификация и аутентификация субъектов

4.1. Классификация подсистем идентификации и аутентификации субъектов

Реализация никакой из политик безопасности не будет возможна в случае, если компьютерная система не сможет распознать (идентифицировать) субъекта, пытающегося получить доступ к объекту компьютерной системы. Поэтому защищенная КС обязательно должна включать в себя *подсистему идентификации*, позволяющую идентифицировать инициирующего доступ субъекта.

Под *идентификацией* понимают присвоение пользователю некоторого уникального *идентификатора*, который он должен предъявить СЗИ при осуществлении доступа к объекту, то есть назвать себя. Используя предъявленный пользователем идентификатор, СЗИ может проверить наличие данного пользователя в списке зарегистрированных и *авторизовать* его (то есть наделить полномочиями) для выполнения определенных задач.

В качестве идентификаторов могут использоваться, например, имя пользователя (логин), аппаратные устройства типа iButton (Touch Memory), бесконтактные радиочастотные карты proximity, отдельные виды пластиковых карт и т.д.

Идентификаторы субъектов не являются секретной информацией и могут храниться в КС в открытом виде.

Для нейтрализации угроз, связанных с хищением идентификаторов и подменой злоумышленником легального пользователя необходимы дополнительные проверки субъекта, заключающиеся в подтверждении им владения предъявленным идентификатором. Данные проверки проводятся на этапе аутентификации пользователя.

Под *аутентификацией* понимают подтверждение пользователем предъявленного идентификатора, проверка его подлинности и принадлежности именно данному пользователю. Аутентификация выполняется для устранения фальсификации на этапе идентификации.

В качестве аутентифицирующей информации может использоваться, например, пароль, секретный код, пин-код и т.д. Информация, используемая субъектом для аутентификации, должна сохраняться им в секрете. Хищение данной информации злоумышленником ведет к тому, что злоумышленник сможет пройти этап идентификации и аутентификации без обнаружения фальсификации.

Этапы идентификации и аутентификации пользователя объединяются в единой подсистеме, называемой *подсистемой идентификации и аутентификации (И/АУ)*.

Атаки на подсистему идентификации и аутентификации пользователя являются одними из наиболее распространенных и привлекательных для злоумышленника, так как пройдя этап И/АУ злоумышленник получает все права легального пользователя, идентификатор которого был использован. В связи с этим, обеспечение стойкости ко взлому подсистемы И/АУ пользователя является очень важной задачей для безопасного функционирования компьютерной системы.

Стойкость к взлому подсистемы идентификации и аутентификации определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор, либо украв его.

Наиболее распространенными методами идентификации и аутентификации пользователя являются:

– Парольные системы.

– Идентификация/аутентификация с использованием технических устройств.

– Идентификация/аутентификация с использованием индивидуальных биометрических характеристик пользователя.

При идентификации/аутентификации пользователей с использованием физических устройств, в качестве пользовательского идентификатора используется некоторое техническое устройство, содержащее уникальный идентификационный номер, используемый для решения задач

идентификации владельца, а в отдельных случаях и секретную аутентифицирующую информацию, ограничивающую доступ к устройству. Широко распространенными техническими устройствами, используемыми для решения задач идентификации/аутентификации пользователей являются:

– идентификаторы iButton (Touch Memory);

– бесконтактные радиочастотные карты proximity;

– пластиковые карты;

– ключи e-Token.

4.2. Парольные системы идентификации и аутентификации пользователей

Парольные системы идентификации/аутентификации является одними из основных и наиболее распространенных в СЗИ методов пользовательской аутентификации. В данном случае информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Совокупность идентификатора и пароля пользователя - основные составляющие его *учетной записи*. *База данных пользователей* парольной системы содержит учетные записи всех пользователей КС.

Парольные системы являются зачастую «передним краем обороны» всей системы безопасности. Отдельные ее элементы могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику (в том числе и база данных учетных записей пользователей). В связи с этим, парольные системы становятся одним из наиболее привлекательных для злоумышленника объектов атаки. Основными типами угроз безопасности парольных систем являются следующие.

1. Перебор паролей в интерактивном режиме.
2. Подсмотр пароля.
3. Преднамеренная передача пароля его владельцем другому лицу.

4. Кража базы данных учетных записей с дальнейшим ее анализом, подбором пароля.

5. Перехват вводимого пароля путем внедрения в КС программных закладок (клавиатурных шпионов); перехват пароля, передаваемого по сети.

6. Социальная инженерия.

Многие недостатки парольных систем связаны с наличием человеческого фактора, который проявляется в том, что пользователь, зачастую, стремится выбрать пароль, который легко запомнить (а значит и подобрать), записать сложно запоминаемый пароль. Легальный пользователь способен ввести пароль так, что его могут увидеть посторонние, передать пароль другому лицу намеренно или под влиянием заблуждения.

Для уменьшения деструктивного влияния человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей [**Ошибка! Источник ссылки не найден.**].

1. Задание минимальной длины пароля для затруднения подбора пароля злоумышленником «в лоб» (полный перебор, brute-forcing) и подсмотра.

2. Использование в пароле различных групп символов для усложнения подбора злоумышленником пароля «в лоб».

3. Проверка и отбраковка пароля по словарю для затруднения подбора пароля злоумышленником с использованием словарей.

4. Установление максимального срока действия пароля для затруднения подбора пароля злоумышленником «в лоб», в том числе и в режиме «off-line» при взломе предварительно похищенной базы данных учетных записей пользователей.

5. Применение эвристического алгоритма, бракующего «плохие» пароли для усложнения подбора пароля злоумышленником «по словарю» или с использованием эвристического алгоритма.

6. Ограничение числа попыток ввода пароля для предотвращения интерактивного подбора пароля злоумышленником.

7. Использование задержки при вводе неправильного пароля для предотвращения интерактивного подбора пароля злоумышленником.

8. Поддержка режима принудительной смены пароля пользователя для эффективности реализации требования, ограничивающего максимальный срок действия пароля.

9. Запрет на выбор пароля самим пользователем и автоматическая генерация паролей для затруднения использования злоумышленником эвристического алгоритма подбора паролей.

Количественная оценка стойкости парольных систем может быть выполнена с помощью следующего подхода [**Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**].

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля). Например, если при составлении пароля могут быть использованы только малые английские буквы, то A=26.

L – длина пароля.

$S = A^L$ - число всевозможных паролей длины L, которые можно составить из символов алфавита A. S также называют пространством атаки.

V – скорость перебора паролей злоумышленником.

T – максимальный срок действия пароля.

Тогда, вероятность P подбора пароля злоумышленником в течении срока его действия T определяется по следующей формуле.

$$P = \frac{V * T}{S} = \frac{V * T}{A^L}$$

Эту формулу можно обратить для решения следующей задачи:

ЗАДАЧА. Определить минимальные мощность алфавита паролей A и длину паролей L, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T.

Данная задача имеет неоднозначное решение. При исходных данных *V,T,P* однозначно можно определить лишь нижнюю границу *S** числа всевозможных паролей. Целочисленное значение нижней границы вычисляется по формуле

$$S^* = \left\lceil \frac{V * T}{P} \right\rceil \qquad (4.1)$$

где $\lceil\ \rceil$ - целая часть числа, взятая с округлением вверх.

После нахождения нижней границы *S** необходимо выбрать такие *A* и *L*, чтобы выполнялось неравенство (4.2).

$$S^* \le S = A^L \qquad (4.2)$$

При выборе *S*, удовлетворяющего неравенству (4.2), вероятность подбора пароля злоумышленником (при заданных *V* и *T*) будет меньше или равна *P*.

При вычислениях по формулам (4.1) и (4.2), величины должны быть приведены к одной размерности.

Пример

Исходные данные – $P=10^{-6}$, *T*=7 дней = 1 неделя, *V*=10 паролей / минуту = 10*60*24*7=100800 паролей в неделю.

Тогда, $S^* = \left\lceil \frac{100800 * 1}{10^{-6}} \right\rceil = 1008 * 10^8$.

Условию $S^* \le A^L$ удовлетворяют, например, такие пары величин *A* и *L*, как *A*=26, *L*=8 (пароли состоят из 8 малых символов английского алфавита), *A*=36, *L*=6 (пароли состоят из 6 символов, среди которых могут быть малые латинские буквы и цифры).

4.3. Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя

Под биометрикой понимается использование для аутентификации личности индивидуальных признаков человека. В качестве биометрических

характеристик, которые могут быть использованы при аутентификации субъекта доступа, достаточно часто применяют следующие:

1. отпечатки пальцев;
2. геометрическая форма рук;
3. узор радужной оболочки и сетчатки глаз;
4. форма и размеры лица;
5. особенности голоса;
6. биомеханические характеристики почерка;
7. биомеханические характеристики «клавиатурного почерка».

Особенностью применения биометрических систем идентификации и аутентификации личности по сравнению с другими классами систем И/АУ являются следующие:

1. Необходимость обучения биометрической системы для конкретных пользователей, зачастую, достаточно длительного.

2. Возможность ошибочных отказов и ошибочных подтверждений при аутентификации пользователей.

3. Необходимость использования специальных технических устройств для чтения биометрических характеристик, как правило, достаточно дорогостоящих (за исключением, быть может, аутентификации по клавиатурному подчерку).

Архитектура биометрических систем аутентификации пользователей может быть представлена в следующем виде (рис. 4.1.).

Перед практическим использованием любой биометрической системы необходимо ее обучение, в результате которого формируется база данных, содержащая эталонные биометрические характеристики зарегистрированных пользователей. Модуль идентификации и аутентификации в дальнейшем использует сформированные на этапе обучения эталоны для сравнения их с предъявляемыми пользователем на этапе аутентификации.

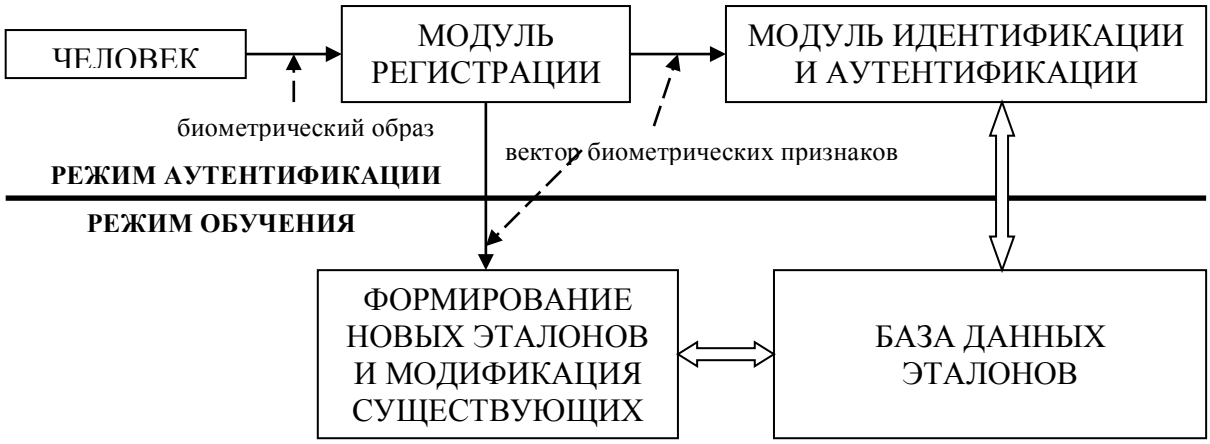


Рис. 4.1. Архитектура биометрической системы аутентификации пользователя

Биометрические системы практически никогда не хранят непосредственные биометрические образы пользователей (например, отпечатки пальцев) и не выполняют сравнение с ними *биометрических образов*, предъявляемых на этапе аутентификации. Предъявляемый пользователем биометрический образ, как правило, преобразуется модулем регистрации в *вектор биометрических признаков*, который и обрабатывается в дальнейшем. Данный вектор содержит признаки, наиболее полно, не избыточно и уникально характеризующие предъявляемый биометрический образ. Например, в качестве одной из составляющей вектора биометрических признаков при использовании в качестве биометрической характеристики геометрической формы рук, можно использовать длины пальцев руки человека.

Одним из важнейших вопросов при проектировании биометрических систем является вопрос совмещения вектора биометрических характеристик пользователя, проходящего аутентификацию, с эталонным вектором, хранимом в базе данных эталонов.

Отличительная черта человека считается хорошей с точки зрения биометрики, если она обеспечивает получение для каждого человека набора уникальных значений измерений (измерения хорошо кластеризуются). Если схожие результаты измерений получаются для многих людей, то биометрика уязвима в плане успешности маскировки под законного пользователя.

Достаточно часто для совмещения векторов биометрических характеристик используют некоторую метрику в векторном пространстве, например, расстояние по Хэммингу или расстояние по Евклиду.

Пусть $x = (x_1,...,x_n)$ и $y = (y_1,...,y_n)$ - два вектора в векторном пространстве V размерности n. Тогда между векторами x и y определены следующие расстояния:

Расстояние по Хэммингу (метрика городских кварталов)

$$h(x, y) = \sum_{i=1}^{n} |x_i - y_i|$$

Расстояние по Евклиду

$$\rho(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$$

Пример 4.1. Пусть эталонный вектор биометрических характеристик пользователя при аутентификации по геометрической форме рук, определяющий длины пяти его пальцев, есть (390, 418, 502, 471, 355), а вектор биометрических характеристик пользователя, проходящего аутентификацию, есть (389, 416, 501, 468, 353). Тогда расстояние по Хэммингу между данными векторами равно 9, расстояние по Евклиду с точностью до двух знаков равно 4,36.

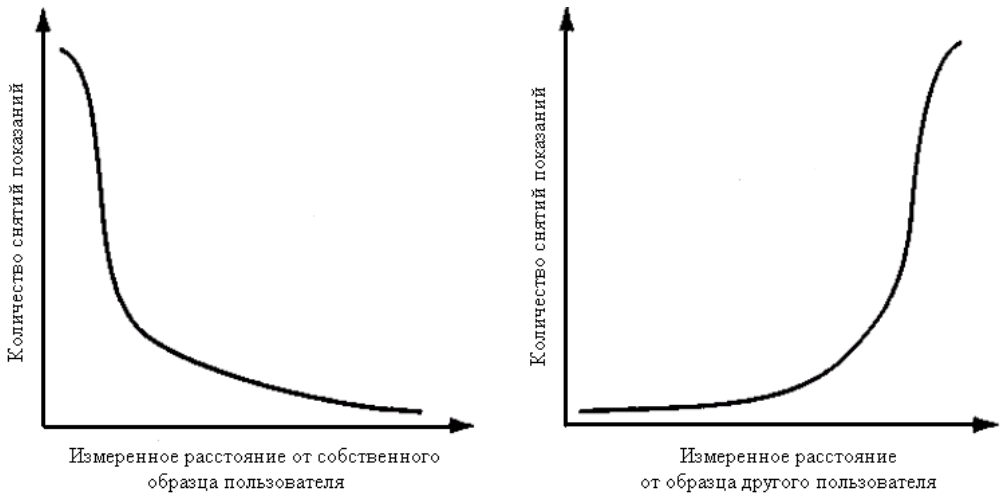
Принятие решения о прохождении либо не прохождении аутентификации пользователя принимается системой идентификации и аутентификации по результатам анализа расстояния между вектором биометрических характеристик, предъявленным пользователем, и эталонным вектором биометрических характеристик для данного пользователя. При этом очень важным является вопрос о выборе *порогового расстояния,* определяющего границу между легальным и нелегальным входом. Выбор порогового расстояния во многом определяет соотношение между ошибочными отказами и ошибочными подтверждениями для биометрической системы.

Пусть N – количество попыток аутентификации легальных пользователей в биометрической системе за достаточно большой промежуток времени, M – количество раз, когда легальным пользователям было отказано в прохождении аутентификации. Тогда, *коэффициентом ошибочных отказов (FRR - false reject rating)* называют отношение $FRR = \frac{M}{N}$, то есть количества отказов в аутентификации легальным пользователям к общему количеству попыток легальной аутентификации.

Пусть K – количество попыток аутентификации нелегальных пользователей в биометрической системе за достаточно большой промежуток времени, L – количество раз, когда нелегальные пользователи получили подтверждение аутентификации. Тогда, *коэффициентом ошибочных подтверждений (FAR – false accept rating)* называют отношение $FAR = \frac{L}{K}$, то есть количества подтверждений аутентификации нелегальных пользователей к общему количеству попыток нелегальной аутентификации [**Ошибка! Источник ссылки не найден.**].

Коэффициенты FAR и FRR являются основными параметрами, по которым оценивают эффективность и надежность реализации биометрических систем. Данные коэффициенты оцениваются на основе экспериментов.

Форма распределения расстояний между вектором биометрических характеристик, предъявленным пользователем, и эталонным вектором биометрических характеристик пользователя для случаев легального и нелегального входов представлена на рис. 4.2.



а) б)

Рис. 4.2. Распределение расстояний между векторами биометрических характеристик для легальных (а) и нелегальных (б) входов

Наложив распределения, представленные на рис. 3.6, друг на друга и изобразив на полученном графике порог принятия решения о прохождении аутентификации пользователем, можно получить геометрическую интерпретацию коэффициентов FAR и FRR (рис. 4.3.).

Количество отказов в аутентификации легальным пользователям (ошибочных отказов), используемое при расчете коэффициента ошибочных отказов FRR равно площади криволинейной трапеции, ограниченной сверху кривой (4.2а), а слева - порогом принятия решения (черная область на рис. 4.3.).

Количество подтверждений аутентификации нелегальных пользователей (ошибочных подтверждений), используемое при расчете коэффициента ошибочных подтверждений FAR равно площади криволинейной трапеции, ограниченной сверху кривой (4.2б), а справа - порогом принятия решения (белая область на рис. 4.3.).

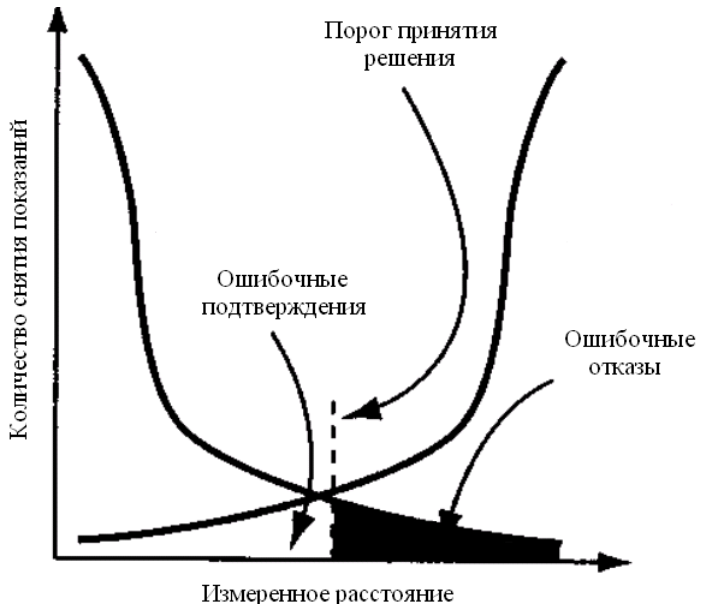


Рис. 4.3. Геометрическая интерпретация ошибочных отказов и ошибочных подтверждений

Анализ рисунка 4.3. показывает, что различным порогам принятия решения при сравнении векторов биометрических характеристик соответствуют различные коэффициенты *FAR* и *FRR*. С другой стороны, каждому из фиксированных коэффициентов *FAR* соответствует свой фиксированный коэффициент *FRR*. Данная зависимость между коэффициентами может быть представлена в виде графика (рис. 4.4.).

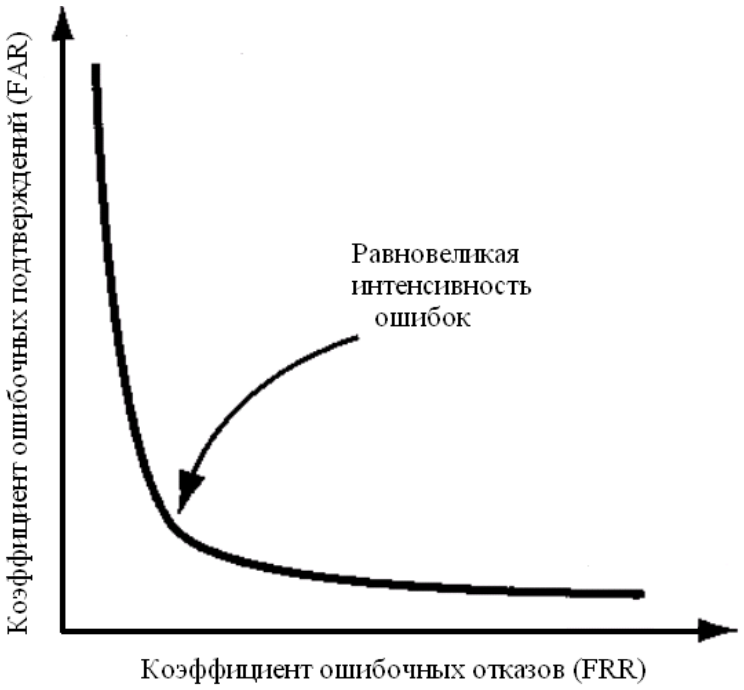


Рис.4.4. Зависимость между коэффициентами FRR и FAR

Представленная на рис. 4.4. зависимость называется *кривой рабочих характеристик приемника* (ROC-кривой). Обычно такая кривая содержит точку, называемую *точкой равновеликой интенсивности ошибок* (*ERR - equal error rate*), в которой значения FAR и FRR равны. Близость точки равновеликой интенсивности ошибок к началу координат обычно свидетельствует о том, что биометрическая система может достигать хорошего уровня безопасности, не давая чрезмерного количества ошибочных отказов в аутентификации.

4.4. Выводы

Доступ к любой компьютерной информации в АСОИ, обладающей какой-либо ценностью, должен быть разрешен только определенному кругу лиц, предварительно прошедших регистрацию и подтвердивших свою подлинность. За решение данных задач отвечает подсистема идентификации и аутентификации.

Основным требованием к реализации данной подсистемы является ее стойкость к взлому путем подбора или подмены информации, подтверждающей подлинность пользователя (пароля, ключа, и т.д.). Информация, подтверждающая подлинность пользователя должна храниться в секрете, лучше – на внешнем аппаратном устройстве, максимально защищенном от НСД.

8. Протоколы безопасной аутентификации пользователей

8.1. Аутентификация на основе сертификатов

Когда число пользователей в сети исчисляется миллионами, процедура предварительной регистрации пользователей, связанная с назначением и хранением паролей пользователей, становится крайне громоздкой и практически плохо реализуемой. В таких условиях аутентификация на

основе *цифровых сертификатов* служит рациональной альтернативой применению паролей.

При использовании цифровых сертификатов компьютерная сеть не хранит никакой информации о своих пользователях. Эту информацию пользователи предоставляют сами в своих запросах – *сертификатах*. При этом задача хранения секретной информации, в частности закрытых ключей, возлагается теперь на самих пользователей.

Цифровые сертификаты, удостоверяющие личность пользователя, выдаются по запросам пользователей специальными уполномоченными организациями – *центрами сертификации CA (Certification Authorities)* при выполнении определенных условий. При этом сама процедура получения сертификата также включает этап проверки подлинности (т.е. аутентификации) пользователя. Здесь в качестве проверяющей стороны выступает сертифицирующая организация.

Для получения сертификата клиент должен представить в центр сертификации CA сведения, удостоверяющие его личность, и свой открытый ключ. Перечень необходимых данных зависит от типа получаемого сертификата. Сертифицирующая организация после проверки доказательств подлинности пользователя помещает свою цифровую подпись в файл, содержащий открытый ключ и сведения о пользователе, и выдает ему сертификат, подтверждая факт принадлежности данного открытого ключа конкретному лицу.

Сертификат представляет собой электронную форму, в которой содержится следующая информация:

1. открытый ключ владельца данного сертификата;
2. сведения о владельце сертификата (имя, электронный адрес, наименование организации, в которой работает данный сотрудник и т.п.);
3. наименование сертифицирующей организации, выдавшей этот сертификат;
4. электронная подпись сертифицирующей организации.

Сертификат является средством аутентификации пользователя при его обращении к сетевым ресурсам.

Роль проверяющей стороны играют *серверы аутентификации* корпоративной сети.

Сертификаты можно использовать не только для аутентификации, но и для предоставления определенных прав доступа. Для этого в сертификат вводятся дополнительные поля, в которых указывается принадлежность его владельца к той или иной категории пользователей.

Следует особо отметить тесную связь открытых ключей с сертификатами. Сертификат является не только удостоверением личности, но и удостоверением принадлежности открытого ключа. Цифровой сертификат устанавливает и гарантирует соответствие между открытым ключом и его владельцем. Это предотвращает угрозу подмены открытого ключа.

Если абонент получает от партнера по информационному обмену открытый ключ в составе сертификата, то он может проверить цифровую подпись СА на этом сертификате с помощью открытого ключа данного СА и убедиться, что полученный открытый ключ принадлежит именно тому пользователю, адрес и другие сведения о котором содержатся в данном сертификате. При использовании сертификатов исчезает необходимость хранить на серверах корпораций списки пользователей с их паролями. На сервере достаточно иметь список имен и открытых ключей сертифицирующих организаций.

Сервер – ЭВМ, выполняющая функции обслуживания пользователей. В сетях выполняет функции управления разделяемыми ресурсами. Существует понятие сервера безопасности.

Следует отметить, что выполнение функций сертифицирующей организации может взять на себя и само предприятие.

8.2. Процедура «рукопожатия»

Эта процедура базируется на механизме «запрос – ответ» (или может предусматривать дополнительно и механизм метки времени) и заключается во взаимной проверке ключей, используемых сторонами. Пользователи A и B разделяют один и тот же секретный ключ K_{AB}.

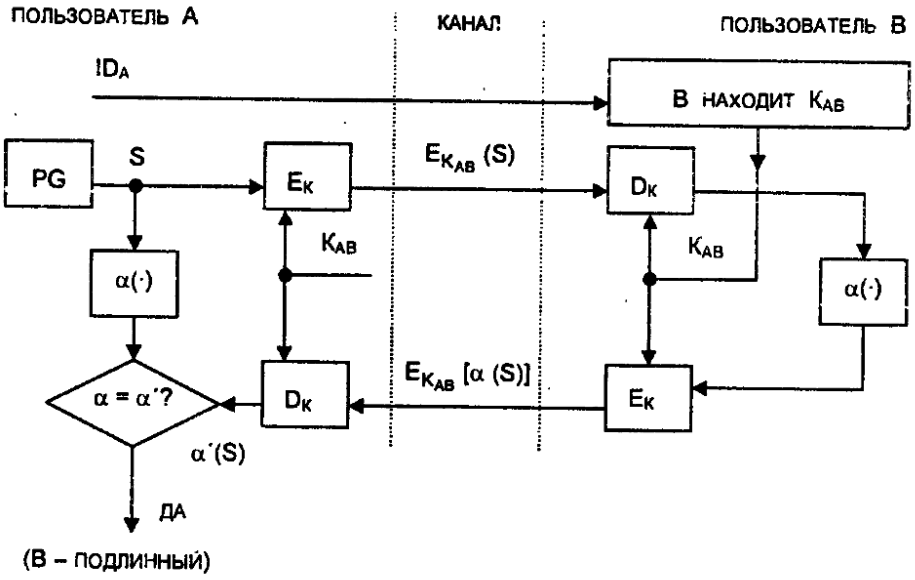


Рисунок 8.1. Процедура рукопожатия.

Пусть пользователь A инициирует процедуру рукопожатия, отправляя пользователю B свой идентификатор ID_A в открытой форме.

Пользователь B, получив идентификатор ID_A, находит в базе данных секретный ключ K_{AB} и вводит его в свою криптосистему.

Тем временем пользователь A генерирует случайную последовательность S с помощью генератора псевдослучайных чисел (ГПСЧ) PG и отправляет его пользователю B в виде криптограммы $E_{K_{AB}}(S)$.

Пользователь B расшифровывает эту криптограмму и раскрывает исходный вид последовательности S.

Затем оба пользователя A и B преобразуют последовательность S, используя открытую одностороннюю функцию $\alpha(\cdot)$.

Пользователь B шифрует сообщение $\alpha(S)$ и отправляет эту криптограмму пользователю A.

Пользователь А расшифровывает криптограмму и сравнивает полученное сообщение α'(S) с исходным α(S). Если α(S)=α'(S), то пользователь А признает подлинность пользователя В.

Очевидно, пользователь В проверяет подлинность пользователя А таким же образом. Обе эти процедуры образуют процедуру рукопожатия, которая выполняется в самом начале сеанса связи в компьютерных сетях.

Достоинство этого метода состоит в том, что ни один из участников сеанса не получает никакой секретной информации во время процедуры подтверждения пользователей.

8.3. Протокол Диффи-Хеллмана

Необходимость в хранении и передаче ключевой информации, зашифрованной с помощью других ключей, привел к развитию концепции иерархии ключей.

Иерархия ключевой информации может включать множество уровней, однако, наиболее часто выделяют главные ключи (мастер-ключи), ключи шифрования ключей и рабочие ключи (сеансовые).

Сеансовые ключи находятся на самом нижнем уровне и используются для шифрования данных. Когда эти ключи необходимо безопасным образом передать между узлами сети или безопасно хранить, их шифруют с помощью ключей следующего уровня – *ключей шифрования ключей*.

На верхнем уровне иерархии ключей располагается мастер-ключ. Этот ключ применяют для шифрования ключей шифрования, когда требуется безопасно хранить их на диске. Обычно в каждом компьютере используется только один мастер ключ, который отчуждается на внешнем носителе, как правило, защищенном от несанкционированного доступа, чтобы раскрыть значение этого ключа было невозможно (смарт-карта, e-Token и т.п.). Значение мастер-ключа фиксируется на длительное время (до нескольких недель или месяцев). Сеансовые ключи меняются намного чаще, например, при построении криптозащищенных туннелей их можно менять каждые 10-

15 минут, либо по результатам шифрования заданного объема трафика (например, 1 Мб).

Для возможности использования при защищенном информационном обмене между противоположными сторонами криптосистемы с секретным ключом, взаимодействующим сторонам необходима выработка общего секрета, на базе которого они смогут безопасно шифровать информацию или безопасным образом вырабатывать и обмениваться сеансовыми ключами. В первом случае общий секрет представляет собой сеансовый ключ, во втором случае – мастер-ключ. В любом случае, злоумышленник не должен быть способен, прослушивая канал связи, получить данный секрет.

Для решения проблемы выработки общего секрета без раскрытия его злоумышленником существует два основных способа:

1. использование криптосистемы с открытым ключом для шифрования и передачи секретного ключа симметричной криптосистемы;

2. использование протокола открытого распространения ключей Диффи-Хеллмана.

Реализация первого способа не должна вызывать вопросов. Рассмотрим более подробно реализацию второго способа.

Протокол Диффи-Хеллмана был первым алгоритмов работы с открытыми ключами (1976 г.). Безопасность данного протокола основана на трудности вычисления дискретных логарифмов в конечном поле.

Пусть пользователи A и B хотят выработать общий секрет. Для этого они выполняют следующие шаги.

1. Стороны A и B договариваются об используемом модуле N, а также о примитивном элементе g, $1 \le g \le N$, степени которого образуют числа от 1 до N-1, то есть во множестве $\{g, g^2, ..., g^{N-1} = 1\}$ присутствуют все числа от 1 до N-1. Числа N и g являются открытыми элементами протокола.

2. Пользователи A и B независимо друг от друга выбирают собственные секретные ключи $СК_A$ и $СК_B$ (случайные большие целые числа, меньшие N, хранящиеся в секрете).

3. Пользователи А и В вычисляют открытые ключи $ОК_A$ и $ОК_B$ на основании соответствующих секретных ключей по следующим формулам:

$$OK_A = g^{CK_A} \pmod N; OK_B = g^{CK_B} \pmod N$$

4. Стороны А и В обмениваются между собой значениями открытых ключей по незащищенному каналу.

5. Пользователи А и В формируют общий секрет *K* по формулам:

Пользователь А: $K = \left(OK_B\right)^{CK_A} = \left(g^{CK_B}\right)^{CK_A} = g^{CK_B \cdot CK_A} \pmod N$

Пользователь В: $K = \left(OK_A\right)^{CK_B} = \left(g^{CK_A}\right)^{CK_B} = g^{CK_A \cdot CK_B} \pmod N$

Ключ *K* может использоваться в качестве общего секретного ключа (мастер-ключа) в симметричной криптосистеме.

Пример 8.1.

Возьмем модуль *N*=47 и примитивный элемент *g*=23. Пусть пользователи А и В выбрали свои секретные ключи $СК_A$=12, $СК_B$=33. Тогда,

$$OK_A = g^{CK_A} \pmod{47} = 23^{12} \pmod{47} = 27$$

$$OK_B = g^{CK_B} \pmod{47} = 23^{33} \pmod{47} = 33$$

В данном случае общий секрет $K = \left(OK_B\right)^{CK_A} = 33^{12} \pmod{47} = 25$.

Алгоритм открытого распределения ключей Диффи-Хеллмана позволяет обойтись без защищенного канала для передачи ключей. Однако, необходима гарантия того, что получатель получил открытый ключ именно от того отправителя, от которого он его ждет. Данная проблема решается с помощью цифровых сертификатов и технологии ЭЦП.

Протокол Диффи-Хеллмана нашел эффективное применение в протоколе SKIP управления ключами. Данный протокол используется при построении криптозащищенных туннелей в семействе продуктов ЗАСТАВА.

8.4. Выводы

Удаленная аутентификация пользователей требует использования протоколов, не передающих в открытом виде по сети закрытую информацию.

В связи с этим, в данном случае должны использоваться протоколы, отличные от локальной аутентификации.

Для выполнения удаленной аутентификации могут быть использованы протоколы, использованные в данном разделе.