2. ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ КС-СУБЪЕКТОВ ДОСТУПА К ДАННЫМ

2.1. Основные понятия и концепции

С каждым объектом компьютерной системы (КС) связана некоторая информация, однозначно идентифицирующая его. Это может быть *число, строка символов, алгоритм,* определяющий данный объект. Эту информацию называют *идентификатором объекта.* Если объект имеет некоторый идентификатор, зарегистрированный в сети, он называется законным (легальным) объектом; остальные объекты относятся к незаконным (нелегальным).

Идентификация объекта - одна из функций подсистемы защиты. Эта функция выполняется в первую очередь, когда объект делает попытку войти в сеть. Если процедура идентификации завершается успешно, данный объект считается законным для данной сети.

Следующий шаг-аутентификация объекта (проверка подлинности объекта). Эта процедура устанавливает, является ли данный объект именно таким, каким он себя объявляет.

После того как объект идентифицирован и подтверждена его подлинность, можно установить сферу его действия и доступные ему ресурсы КС. Такую процедуру называют *предоставлением полномочий (авторизацией).*

Перечисленные три процедуры инициализации являются процедурами защиты и относятся к одному объекту КС.

При защите каналов передачи данных *подтверждение подлинности* (аутентификация) объектов означает взаимное установление подлинности объектов, связывающихся между собой по линиям связи. Процедура подтверждения подлинности выполняется обычно в начале сеанса в процессе установления соединения абонентов. (Термин "соединение" указывает на логическую связь (потенциально двустороннюю) между двумя объектами сети.

Цель данной процедуры - обеспечить уверенность, что соединение установлено с законным объектом и вся информация дойдет до места назначения.

После того как соединение установлено, необходимо обеспечить выполнение требований защиты при обмене сообщениями:

(а) получатель должен быть уверен в подлинности источника данных;

(б) получатель должен быть уверен в подлинности передаваемых данных;

(в) отправитель должен быть уверен в доставке данных получателю;

(г) отправитель должен быть уверен в подлинности доставленных данных.

Для выполнения требований (а) и (б) средством защиты является *цифровая подпись.* Для выполнения требований (в) и (г) отправитель должен получить *уведомление о вручении* с помощью удостоверяющей почты (certified mail). Средством защиты в такой процедуре является цифровая подпись подтверждающего ответного сообщения, которое в свою очередь является доказательством пересылки исходного сообщения.

Если эти четыре требования реализованы в КС, то гарантируется защита данных при их передаче по каналу связи и обеспечивается функция защиты, называемая функцией подтверждения (неоспоримости) передачи. В этом случае отправитель не может отрицать ни факта посылки сообщения, ни его содержания, а получатель не может отрицать ни факта получения сообщения, ни подлинности его содержания.

2.2. Идентификация и аутентификация пользователя

Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс представления компьютерной системе, который включает две стадии:

- идентификацию - пользователь сообщает системе по ее запросу свое имя (идентификатор);

- аутентификацию - пользователь подтверждает идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль).

Для проведения процедур идентификации и аутентификации пользователя необходимы:

- наличие соответствующего *субъекта (модуля) аутентификации;*
- наличие *аутентифицирующего объекта,* хранящего уникальную информацию для аутентификации пользователя.

Различают две формы представления объектов, аутентифицирующих пользователя:

- внешний аутентифицирующий объект, не принадлежащий системе;
- внутренний объект, принадлежащий системе, в который переносится информация из внешнего объекта.

Внешние объекты могут быть технически реализованы на различных носителях информации - магнитных дисках, пластиковых картах и т. п. Естественно, что внешняя и внутренняя формы представления аутентифицирующего объекта должны быть семантически тождественны.

Типовые схемы идентификации и аутентификации пользователя

Рассмотрим структуры данных и протоколы идентификации и аутентификации пользователя. Допустим, что в компьютерной системе зарегистрировано n пользователей. Пусть i-й аутентифицирующий объект i-го пользователя содержит два информационных поля:

ID_i-неизменный идентификатор i-го пользователя, который является аналогом имени и используется для идентификации пользователя;

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

Описанная структура соответствует практически любому ключевому носителю информации, используемому для опознания пользователя. Например,

для носителей типа пластиковых карт выделяется неизменяемая информация ID_i первичной персонализации пользователя и объект в файловой структуре карты, содержащий $К_i$.

Совокупную информацию в ключевом носителе можно назвать первичной аутентифицирующей информацией i-го пользователя! Очевидно, что внутренний аутентифицирующий объект не должен существовать в системе длительное время (больше времени работы конкретного пользователя). Для длительного хранения следует использовать данные в защищенной форме.

Рассмотрим две типовые схемы идентификации и аутентификации.

Схема 1. В компьютерной системе выделяется объект-эталон для идентификации и аутентификации пользователей. Структура объекта-эталона для схемы 1 показана в табл. 5.1. Здесь $E_i=F(ID_i\ K_i)$, где F-функция, которая обладает свойством "невосстановимости" значения $К_i$ по E_i и ID_i. "Невоостановимость" K_i оценивается некоторой пороговой трудоемкостью T_0 решения задачи восстановления аутентифицирующей информации $К_i$ по E_i и ID_i. Кроме того, для пары K_i и Kj возможно совпадение соответствующих значений E. В связи с этим вероятность лажной аутентификации пользователя не должна быть больше некоторого порогового значения P_0.

На практике задают $T_o=10^{20}.,,10^{30}$, $P_o=10^{-7}...10^{-9}$

Таблица 2.1

Структура объекта-эталона для схемы 1

Номер пользователя	Информация для идентификации	Информация для аутентификации
1	**ID_1**	**E_1**
2	**ID_2**	**E_2**
N	**ID_n**	**$E_п$**

Протокол идентификации и аутентификации (для схемы 1).

1. Пользователь предъявляет свой идентификатор ID.

2. Если ID не совпадает ни с одним ID_i, зарегистрированным в компьютерной системе, то идентификация отвергается - пользователь не допускается к работе, иначе (существует ID_i = ID) устанавливается, что пользователь, назвавшийся пользователем i, прошел идентификацию.

3. Субъект аутентификации запрашивает у пользователя его аутентификатор К.

4. Субъект аутентификации вычисляет значение $Y=F(ID_i , К)$.

5. Субъект аутентификации производит сравнение значений Y и E_i. При совпадении этих значений устанавливается, что данный пользователь успешно аутентифицирован в системе. Информация об этом пользователе передается в программные модули, использующие ключи пользователей (т.е. в систему шифрования, разграничения доступа и т.д.). В противном случае аутентификация отвергается - пользователь не допускается к работе.

Данная схема идентификации и аутентификации пользователя может быть модифицирована. Модифицированная схема 2 обладает лучшими характеристиками по сравнению со схемой 1.

Схема 2. В компьютерной системе выделяется модифицированный объект-эталон, структура которого показана в табл. 2.2.

Таблица 2.2

Структура модифицированного объекта-эталона

Номер пользователя	Информация для идентификации	Информация для аутентификации
1	**ID_1, S_1**	**E_1**
2	**ID_2, S_2**	**E_2**
N	**ID_n , S_n**	**E_n**

В отличие от схемы 1, в схеме 2 значение E_i. равно $F(S_i\ K_i)$, где S_i- случайный вектор, задаваемый при создании идентификатора пользователя, т.е. при создании строки, необходимой для идентификации и аутентификации пользователя; F-функция, которая обладает свойством "невосстановимости" значения K_i по E_i и S_i.

Протокол идентификации и аутентификации (для схемы 2).

1. Пользователь предъявляет свой идентификатор ID.

2. Если ID не совпадает ни с одним IDi, зарегистрированным в компьютерной системе, то идентификация отвергается - пользователь не допускается к работе, иначе (существует IDi=ID) устанавливается, что пользователь, называвшийся пользователем i, прошел идентификацию.

3. По идентификатору IDi выделяется вектор Si.

4. Субъект аутентификации запрашивает у пользователя аутентификатор K.

5. Субъект аутентификации вычисляет значение Y= F(Si, K).

6. Субъект аутентификации производит сравнение значений Y и Ei. При совпадении этих значений устанавливается, что данный пользователь успешно аутентифицирован в системе. В противном случае аутентификация отвергается - пользователь не допускается к работе.

Вторая схема аутентификации применяется в ОС UNIX. В качестве идентификатора ID используется имя пользователя (запрошенное по Loqin), в качестве аутентификатора Ki - пароль пользователя (запрошенный по Password), функция F представляет собой алгоритм шифрования DES. Эталоны для идентификации и аутентификации содержатся в файле Etc/passwd.

Следует отметить, что необходимым требованием устойчивости схем аутентификации к восстановлению информации Ki является случайный равновероятный выбор Ki из множества возможных значений.

Системы парольной аутентификации имеют пониженную стойкость, поскольку в них выбор аутентифицирующей информации происходит из

относительно небольшого множества осмысленных слов. Мощность этого множества определяется энтропией соответствующего языка.

Особенности применения пароля для аутентификации пользователя

Традиционно каждый законный пользователь компьютерной системы получает идентификатор и/или пароль. В начале сеанса работы пользователь предъявляет свой идентификатор системе, которая затем запрашивает у пользователя пароль.

Простейший метод подтверждения подлинности с использованием пароля основан на сравнении представляемого пользователем пароля P_A с исходным значением P_A', хранящимся в компьютерном центре (рис. 2.1). Поскольку пароль должен храниться в тайне, он должен шифроваться перед пересылкой по незащищенному каналу. Если значения P_A и P_A' совпадают, то пароль P_A считается подлинным, а пользователь - законным.

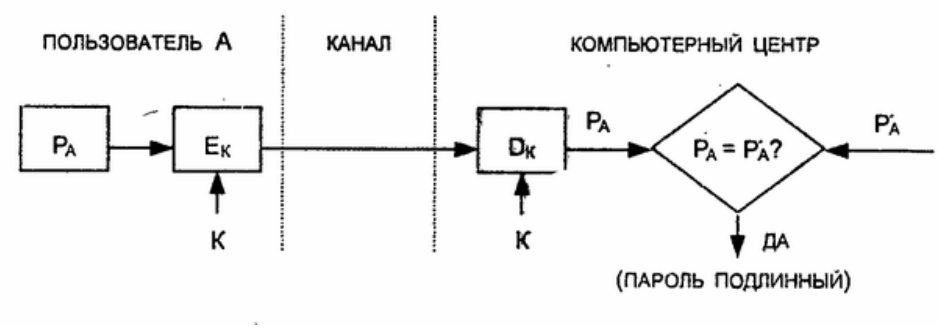

Рисунок 2.1 – Схема простой аутентификации с помощью пароля

Если кто-нибудь, не имеющий полномочий для входа в систему, узнает каким-либо образам пароль и идентификационный номер законного пользователя, он получает доступ в систему.

Иногда получатель не должен раскрывать исходную открытую форму пароля. В этом случае отправитель должен пересылать вместо открытой формы пароля отображение пароля, получаемое с использованием односторонней функции a(.) пароля. Это преобразование должно гарантировать невозможность раскрытия противником пароля по его отображению, так как противник наталкивается на неразрешимую числовую задачу.

Например, функция a(.) может быть определена следующим образом:

$$a(P)Ep(ID),$$

где P - пароль отправителя; ID-идентификатор отправителя; E_P - процедура шифрования, выполняемая с использованием пароля P в качестве ключа.

Такие функции особенно удобны, если длина пароля и ключа одинаковы. В этом случае подтверждение подлинности с помощью пароля состоит из пересылки получателю отображения a(P) и сравнения его с предварительно вычисленным и хранимым эквивалентом a'(P).

На практике пароли состоят только из нескольких букв, чтобы дать возможность пользователям запомнить их. Короткие пароли уязвимы к атаке полного перебора *всех* вариантов. Для того чтобы предотвратить такую атаку, функцию a(P) определяют иначе, а именно:

$$a(P)=Ep_{p+к}(ID),$$

где К и ID-соответственно ключ и идентификатор отправителя.

Очевидно, значение a(P) вычисляется заранее и хранится в виде a'(P) в идентификационной таблице у получателя (рис. 2.2). Подтверждение подлинности состоит из сравнения двух отображений пароля $a(P_A)$ и $a'(P_A)$ и признания пароля P_A, если эти отображения равны.

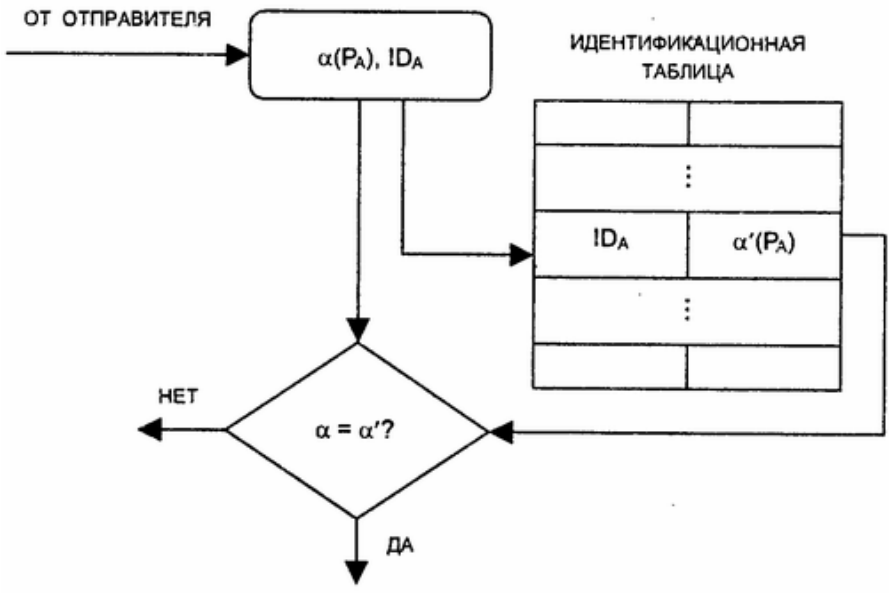

Рисунок 2.2 – Схема аутентификации с помощью пароля с использованием идентификационной таблицы

Конечно, любой, кто получит доступ к идентификационной таблице, может незаконно изменить ее содержимое, не опасаясь, что эти действия будут обнаружены.

Биометрическая идентификация и аутентификация пользователя

Процедуры идентификации и аутентификации пользователя могут базироваться не только на секретной информации, которой обладает пользователь (пароль, секретный ключ, персональный идентификатор и т.п.). В последнее время все большее распространение получает биометрическая идентификация и аутентификация пользователя, позволяющая уверенно идентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.

Отметим основные достоинства биометрических методов идентификации и аутентификации пользователя по сравнению с традиционными:

- высокая степень достоверности идентификации по биометрическим признакам из-за их уникальности;
- неотделимость биометрических признаков от дееспособной личности;
- трудность фальсификации биометрических признаков.

В качестве биометрических признаков, которые могут быть использованы при идентификации потенциального пользователя, можно выделить следующие:

- узор радужной оболочки и сетчатки глаз;
- отпечатки пальцев;
- геометрическая форма руки;

- форма и размеры лица;
- особенности голоса;
- биомеханические характеристики рукописной подписи;
- биомеханические характеристики "клавиатурного почерка".

При регистрации пользователь должен продемонстрировать один или несколько раз свои характерные биометрические признаки. Эти признаки (известные как подлинные) регистрируются системой как контрольный "образ" законного пользователя. Этот образ пользователя хранится в электронной форме и используется для проверки идентичности каждого, кто выдает себя за соответствующего законного пользователя. В зависимости от совпадения или несовпадения совокупности предъявленных признаков с зарегистрированными в контрольном образе их предъявивший признается законным пользователем (при совпадении) или нет (при несовпадении).

Системы идентификации по узору радужной оболочки и сетчатки глаз могут быть разделены на два класса:

- использующие рисунок радужной оболочки глаза,
- использующие рисунок кровеносных сосудов сетчатки глаза.

Поскольку вероятность повторения данных параметров равна 10^{-78}, эти системы являются наиболее надежными среди всех биометрических систем. Такие средства идентификации применяются там, где требуется высокий уровень безопасности (например, в США в зонах военных и оборонных объектов).

Системы идентификации по отпечаткам пальцев являются самыми распространенными. Одна из основных причин широкого распространения таких систем заключается в наличии больших банков данных по отпечаткам пальцев. Основными пользователями подобных систем во всем мире являются полиция, различные государственные и некоторые банковские организации.

Системы идентификации по геометрической форме руки используют сканеры формы руки, обычно устанавливаемые на стенах. Следует отметить,

что подавляющее большинство пользователей предпочитают системы именно этого типа, а не описанные выше.

Системы идентификации по лицу и голосу являются наиболее доступными из-за их дешевизны, поскольку большинство современных компьютеров имеют видео- и аудиосредства. Системы данного класса широко применяются при удаленной идентификации субъекта доступа в телекоммуникационных сетях.

Системы идентификации личностей по динамике рукописной подписи учитывают интенсивность каждого усилия подписывающего, частотные характеристики написания каждого элемента подписи и начертание подписи в целом.

Системы идентификации по биомеханическим характеристикам "клавиатурного почерка" основываются на том, что моменты нажатия и отпускания клавиш при наборе текста на клавиатуре существенно различаются у разных пользователей. Этот динамический ритм набора ("клавиатурный почерк") позволяет построить достаточно надежные средства идентификации. В случае обнаружения изменения клавиатурного почерка пользователя ему автоматически запрещается работа на ЭВМ.

Следует отметить, что применение биометрических параметров при идентификации субъектов доступа автоматизированных систем пока не получило надлежащего нормативно-правового обеспечения, в частности в виде стандартов. Поэтому применение систем биометрической идентификации допускается только в автоматизированных системах, обрабатывающих и хранящих персональные данные, составляющие коммерческую и служебную тайну.

2.3. Взаимная проверка подлинности пользователей

Обычно стороны, вступающие в информационный обмен, нуждаются во взаимной проверке подлинности (аутентификации) друг друга. Этот процесс взаимной аутентификации выполняют в начале сеанса связи.

Для проверки подлинности применяют следующие способы:

- механизм запроса-ответа;
- механизм отметки времени ("временной штемпель").

Механизм запроса-ответа состоит в следующем. Если пользователь А хочет быть уверенным, что сообщения, получаемые им от пользователя В, не являются ложными, он включает в посылаемое для В сообщение непредсказуемый элемент-запрос X (например, некоторое случайное число). При ответе пользователь В должен выполнить над этим элементом некоторую операцию (например, вычислить некоторую функцию f(X)). Это невозможно осуществить заранее, так как пользователю В неизвестно, какое случайное число X придет в запросе. Получив ответ с результатом действий В, пользователь может быть уверен, что В - подлинный. Недостаток этого метода-возможность установления закономерности между запросом и ответом.

Механизм отметки времени подразумевает регистрацию времени для каждого сообщения. В этом случае каждый пользователь сети может определить, насколько "устарело" пришедшее сообщение, и решить не принимать его, поскольку оно может быть ложным.

В обоих случаях для защиты механизма контроля следует применять шифрование, чтобы быть уверенным, что ответ послан не злоумышленником.

При использовании отметок времени возникает проблема *допустимого временного интервала задержки* для подтверждения подлинности сеанса. Ведь сообщение с "временным штемпелем" в принципе не может быть передано мгновенно. Кроме того, компьютерные часы получателя и отправителя не могут быть абсолютно синхронизированы. Какое запаздывание "штемпеля" является подозрительным?

Для взаимной проверки подлинности обычно используют *процедуру "рукопожатия"*. Эта процедура базируется на указанных выше механизмах контроля и заключается во взаимной проверке ключей, используемых сторонами. Иначе говоря, стороны признают друг друга законными партнерами, если докажут друг другу, что обладают правильными ключами.

Процедуру рукопожатия обычно применяют в компьютерных сетях при организации сеанса связи между пользователями, пользователем и хост - компьютером, между хост - компьютерами и т.д.

Рассмотрим в качестве примера процедуру рукопожатия для двух пользователей А и В. (Это допущение не влияет на общность рассмотрения.

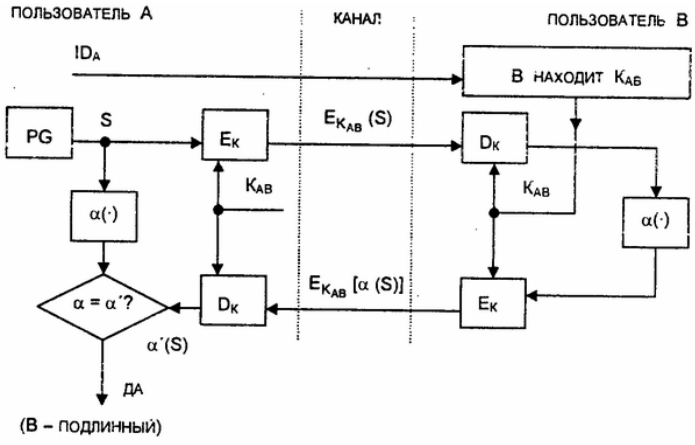

Рисунок 2.3 – Схема процедуры рукопожатия (пользователь А проверяет подлинность пользователя В)

Такая же процедура используется, когда вступающие в связь стороны не являются пользователями). Пусть приценяется симметричная криптосистема. Пользователи А и В разделяют один и тот же секретный ключ $К_{АВ}$. Вся процедура показана на рис. 2.3.

• Пусть пользователь А инициирует процедуру рукопожатия, отправляя пользователю В свой идентификатор ID_A в открытой форме.

• Пользователь В, получив идентификатор ID_A, находит в базе данных секретный *ключ* $К_{АВ}$ и вводит его в свою криптосистему.

• Тем временем *пользователь А* генерирует случайную *последовательность S с* помощью псевдослучайного генератора PG и отправляет ее *пользователю В* в виде криптограммы

$$E_{К_{АВ}}(S).$$

• Пользователь В расшифровывает эту криптограмму и раскрывает исходный вид последовательности S.

• Затем оба пользователя A и B преобразуют последовательность S, используя открытую одностороннюю функцию a(.).

• Пользователь B шифрует сообщение a(S) и отправляет эту криптограмму *пользователю A*.

• Наконец, пользователь A расшифровывает эту криптограмму и сравнивает полученное сообщение a'(S) с исходным a(S). Если эти сообщения равны, пользователь A признает подлинность пользователя B.

Очевидно, пользователь B проверяет подлинность пользователя A таким же способом. Обе эти процедуры образуют процедуру рукопожатия, которая обычно выполняется в самом начале любого сеанса связи между любыми двумя сторонами в компьютерных сетях.

Достоинством модели рукопожатия является то, что ни один из участников сеанса связи не получает никакой секретной информации во время процедуры подтверждения подлинности.

Иногда пользователи хотят иметь непрерывную проверку подлинности отправителей в течение всего сеанса связи. Один из простейших способов непрерывной проверки подлинности показан на рис. 5.4. Передаваемая криптограмма имеет вид

$$Ек(ID_A,M),$$

где ID_A-идентификатор отправителя A; M - сообщение.

Получатель B, принявший эту криптограмму, расшифровывает ее и раскрывает пару (ID_A, M). Если принятый идентификатор ID_A совпадает с хранимым значением ID_A, получатель B признает эту криптограмму.

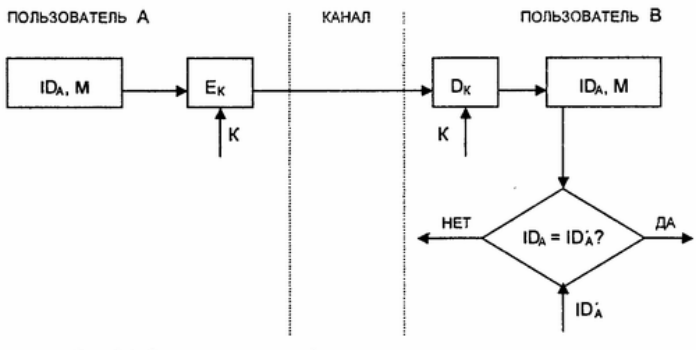

Рис. 5.4. Схема непрерывной проверки подлинности отправителя

Рисунок 2.4 – Схема непрерывной проверки подлинности отправителя

Другой вариант непрерывной проверки подлинности использует вместо идентификатора отправителя его секретный пароль. Заранее подготовленные пароли известны обеим сторонам. Пусть P_A и $P_в$-пароли пользователей А и В соответственно. Тогда пользователь А создает криптограмму

$$C = E_K(P_A,M).$$

Получатель криптограммы расшифровывает ее и сравнивает пароль, извлеченный из этой криптограммы, с исходным значением. Если они равны, получатель признает эту криптограмму.

Процедура рукопожатия была рассмотрена в предположении, что пользователи А и В уже имеют общий *секретный сеансовый ключ.* Реальные процедуры предназначены для распределения ключей между подлинными партнерами и включает как этап распределения ключей, так и этап собственно подтверждения подлинности партнеров по информационному обмену.

2.4. Протоколы идентификации с нулевой передачей знаний

Широкое распространение интеллектуальных карт (смарт-карт) для разнообразных коммерческих, гражданских и военных применений (кредитные карты, карты социального страхования, карты доступа в охраняемое помещение, компьютерные пароли и ключи, и т.п.) потребовало обеспечения безопасной идентификации таких карт и их владельцев. Во многих приложениях главная проблема заключается в том, чтобы при предъявлении интеллектуальной карты оперативно обнаружить обман и отказать обманщику в допуске, ответе или обслуживании.

Для безопасного использования интеллектуальных карт разработаны протоколы идентификации с нулевой передачей знаний. Секретный ключ владельца карты становится неотъемлемым признаком его личности. Доказательство знания этого секретного ключа с нулевой передачей этого знания служит доказательством подлинности личности владельца карты.

Упрощенная схема идентификации с нулевой передачей знаний

Схему идентификации с нулевой передачей знаний предложили в 1986 г. У. Фейге, А. Фиат и А. Шамир. Она является наиболее известным доказательством идентичности с нулевой передачей конфиденциальной информации.

Рассмотрим сначала упрощенный вариант схемы идентификации с нулевой передачей знаний для более четкого выявления ее основной концепции. Прежде всего, выбирают случайное значение модуля n, который является произведением двух больших простых чисел. Модуль n должен иметь длину 512... 1024 бит. Это значение n может быть представлено группе пользователей, которым придется доказывать свою подлинность. В процессе идентификации участвуют две стороны:

- сторона А, доказывающая свою подлинность,
- сторона В, проверяющая представляемое стороной А доказательство.

Для того чтобы сгенерировать открытый и секретный ключи для стороны А, доверенный арбитр (Центр) выбирает некоторое число V, которое является квадратичным вычетом по модулю n. Иначе говоря, выбирается такое число V, что сравнение

$$x^2 = V(\mathrm{mod}\ n)$$

имеет решение и существует целое число

$$V^{-1} \mathrm{mod}\ n.$$

Выбранное значение V является *открытым ключом* для А. Затем вычисляют наименьшее значение S, для которого

$$S = \mathrm{sqrt}(V^{-1})(\mathrm{mod} n).$$

Это значение S является *секретным ключом* для А.

Теперь можно приступить к выполнению протокола идентификации.

1. Сторона А выбирает некоторое случайное число r, r<n. Затем она вычисляет

$$x = r^2 \mathrm{mod}\ n$$

и отправляет x стороне В.

2. Сторона B посылает A случайный бит b.

3. Если b = 0, тогда A отправляет r стороне B. Если b = 1, то A отправляет стороне B

$$y = r * S \bmod n.$$

4. Если b = 0, сторона B проверяет, что

$$x = r^2 \bmod n,$$

чтобы убедиться, что A знает sqrt(x). Если b = 1, сторона B проверяет, что

$$x = y^2 * V \bmod n,$$

чтобы быть уверенной, что A знает sqrt(V^1).

Эти шаги образуют один цикл протокола, называемый *аккредитацией.* Стороны A и B повторяют этот цикл t раз при разных случайных значениях r и b до тех пор, пока B не убедится, что A знает значение S.

Если сторона A не знает значения S, она может выбрать такое значение r, которое позволит ей обмануть сторону B, если B отправит ей b = 0, либо A может выбрать такое r, которое позволит обмануть B, если B отправит ей b = 1. Но этого невозможно сделать в обоих случаях. Вероятность того, что A обманет B в одном цикле, составляет 1/2. Вероятность обмануть B в t циклах равна $(1/2)^t$

Для того чтобы этот протокол работал, сторона A никогда не должна повторно использовать значение r. Если A поступила бы таким образом, а сторона B отправила бы стороне A на шаге 2 другой случайный бит b, то B имела бы оба ответа A. После этого B может вычислить значение S, и для A все закончено.

Параллельная схема идентификации с нулевой передачей знаний

Параллельная схема идентификации позволяет увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.

Как и в предыдущем случае, сначала генерируется число n как произведение двух больших чисел. Для того, чтобы сгенерировать открытый и

секретный ключи для стороны А, сначала выбирают К различных чисел V_1 V_2, ...,V_K, где каждое V; является квадратичным вычетом по модулю n. Иначе говоря, выбирают значение V_i таким, что сравнение

$$x^2 = V_i \bmod n$$

имеет решение и существует V_i^{-1}modn. Полученная строка V_1V_2, ..., V_K является *открытым ключом.*

Затем вычисляют такие наименьшие значения S,, что

$$S_i = \text{sqrt}\ (V_i^1) \bmod n.$$

Эта строка S_1 S_2,..., S_K является *секретным ключом* стороны А. Протокол процесса идентификации имеет следующий вид:

1. Сторона А выбирает некоторое случайное число r, r<n. Затем она вычисляет $x = r^2 \bmod n$ и посылает x стороне В.

2. Сторона В отправляет стороне А некоторую случайную двоичную строку из К бит: b_1, b_2,.... $b_к$.

3. Сторона А вычисляет

$$y = r * (S_1^{b1} * S_2^{b2} *...* S_K^{bk}) \bmod n.$$

Перемножаются только те значения S_i, для которых $b_i = 1$. Например, если $b_i = 1$, то сомножитель S_1 входит в произведение, если же $b_i = 0$, то S_1 не входит в произведение, и т.д. Вычисленное значение y отправляется стороне В.

4. Сторона В проверяет, что

$$x = y^2 * (V_1^{b1} * V_2^{b2} *...*V_k^{bk}) \bmod n.$$

Фактически сторона В перемножает только те значения V_i, для которых $b_i = 1$. Стороны А и В повторяют этот протокол t раз, пока В не убедится, что А знает S_1, S_2.....S_K.

Вероятность того, что. А может обмануть В, равна $(1/2)^{Kt}$. Авторы рекомендуют в качестве контрольного значения брать вероятность обмана В равной $(1/2)^{20}$ при К = 5 и t=4.

Пример. Рассмотрим работу этого протокола для небольших числовых значений . Если n = 35 (n - произведение двух простых чисел 5 и 7), то возможные квадратичные вычеты будут следующими:

Таблица 2.3

1	$x^2 = 1 \pmod{35}$	имеет решения: x = 1, 6. 29, 34;
4	$x^2 = 4 \pmod{35}$	имеет решения: x = 2,12, 23, 33;
9	$x^2 = 9 \pmod{35}$	имеет решения: x = 3, 17, 18, 32;
11	$x^2 = 11 \pmod{35}$	имеет решения: x = 9, 16.19, 26;
14	$x^2 = 14 \pmod{35}$	имеет решения: x = 7, 28;
15	$x^2 = 15 \pmod{35}$	имеет решения: x = 15, 20;
16	$x^2 * 16 \pmod{35}$	имеет решения: x = 4, 11, 24, 31;
21	$x^2 = 21 \pmod{35}$	имеет решения: x = 14, 21;
25	$x^2 = 25 \pmod{35}$	имеет решения: x = 5, 30;
29	$x^2 = 29 \pmod{35}$	имеет решения: x = 8, 13, 22, 27;
30	$x^2 = 30 \pmod{35}$	имеет решения: x - 10, 25.

Заметим, что 14, 15, 21, 25 и 30 не имеют обратных значений по модулю 35. потому что они не являются взаимно простыми с 35. Следует также отметить, что число квадратичных вычетов по модулю 35, взаимно простых с n = p*q = 5*7=35 (для которых НОД (x, 35) = 1), равно

$$(p -1) (q -1)/4 = (5 -1) (7-1)/4 = 6.$$

Составим таблицу квадратичных вычетов по модулю 35, обратных к ним значений по модулю 35 и их квадратных корней.

Таблица 2.4

V	V^{-1}	$S = sqrt(V^{-1}')$
1	1	1
4	9	3
9	4	2
11	16	4
16	11	9
29	29	8

Итак, сторона А получает открытый ключ, состоящий из К=4 значений V:

[4, 11, 16, 29]. Соответствующий секретный ключ, состоящий из K=4 значений S:

[3 4 9 8].

Рассмотрим один цикл протокола.

1. Сторона A выбирает некоторое случайное число r =16, вычисляет

$$x=16^2 \bmod 35=11$$

и посылает это значение x стороне B.

2. Сторона B отправляет стороне A некоторую случайную двоичную строку

[1, 1,0, 1].

3. Сторона A вычисляет значение

$$y = r * (S_1^{b1} * S_2^{b2} *...* S_K^{bk}) \bmod n =16 * (3^1 * 4^1 * 9° * 8^1) \bmod 35 = 31$$

и отправляет это значение y стороне B.

4. Сторона B проверяет, что

$$x = y^2 * (V_1^{b1} * V_2^{b2} *...*V_k^{bk}) \bmod n = 31^2 * (4^1 *11^1 *16° * 29^1) \bmod 35 =11.$$

Стороны A и B повторяют этот протокол t раз, каждый раз с разным случайным числом r, пока сторона B не будет удовлетворена.

При малых значениях величин, как в данном примере, не достигается настоящей безопасности. Но если n представляет собой число длиной 512 бит и более, сторона B не сможет узнать ничего о секретном ключе стороны A, кроме того факта, что сторона A знает этот ключ.

В этот протокол можно включить идентификационную информацию.

Пусть I-некоторая двоичная строка, представляющая идентификационную информацию о владельце карты (имя, адрес, персональный идентификационный номер, физическое описание) и о карте (дата окончания действия и т.п.). Эту информацию I формируют в Центре выдачи интеллектуальных карт по заявке пользователя A.

Далее используют одностороннюю функцию f() для вычисления f(i,j), где j-некоторое двоичное число, сцепляемое со строкой i. Вычисляют значения

$$Vj = f(l, j)$$

для небольших значений j, отбирают К разных значений j, для которых Vj являются квадратичными вычетами по модулю п. Затем для отобранных квадратичных вычетов Vj вычисляют наименьшие квадратные корни из Vj^{-1}(mod n). Совокупность из К значений Vj образует открытый ключ, а совокупность из К значений Sj-секретный ключ пользователя А.

2.5 Схема идентификации Гиллоу-Куискуотера

Алгоритм идентификации с нулевой передачей знания, разработанный Л. Гиллоу и Ж. Куискуотером, имеет несколько лучшие характеристики, чем предыдущая схема идентификации. В этом алгоритме обмены между сторонами А и В и аккредитации в каждом обмене доведены до абсолютного минимума для каждого доказательства требуется только один обмен с одной аккредитацией. Однако объем требуемых вычислений для этого алгоритма больше, чем для схемы Фейге-Фиата-Шамира.

Пусть сторона А-интеллектуальная карточка, которая должна доказать свою подлинность проверяющей стороне В. Идентификационная информация стороны А представляет собой битовую строку I, которая включает имя владельца карточки, срок действия, номер банковского счета и др. Фактически идентификационные данные могут занимать достаточно длинную строку, и тогда их хэшируют к значению I.

Строка I является аналогом открытого ключа. Другой открытой информацией, которую используют все карты, участвующие в данном приложении, являются модуль п и показатель степени V Модуль п является произведением двух секретных простых чисел.

Секретным ключом стороны А является величина G, выбираемая таким образом, чтобы выполнялось соотношение

$$l*G^{v}=1(modn)$$

Сторона А отправляет стороне В свои идентификационные данные I. Далее ей нужно доказать стороне В, что эти идентификационные данные

принадлежат именно ей. Чтобы добиться этого, сторона A должна убедить сторону B, что ей известно значение G.

Вот протокол доказательства подлинности A без передачи стороне B значения G:

1. Сторона A выбирает случайное целое r, такое, что 1<r<n-1. Она вычисляет

$$T=r^{v} \bmod n$$

и отправляет это значение стороне B.

2. Сторона B выбирает случайное целое d, такое, что 1<d<n-1, и отправляет это значение d стороне A.

3. Сторона A вычисляет

$$D = r * G^{d} \bmod n$$

и отправляет это значение стороне B.

4. Сторона B вычисляет значение

$$T'= D^{v}I^{d} \bmod n.$$

Если $T=T' \pmod n$,

то проверка подлинности успешно завершена.

Математические выкладки, использованные в этом протоколе, не очень сложны:

$$T'= D^{v}I^{d} = (rG^{d})^{v}\, I^{d} = r^{v}G^{dv}I^{d} = r^{v}(IG^{v})^{d} = r^{v}=T \pmod n,$$

поскольку G вычислялось таким образом, чтобы выполнялось соотношение

$$IG^{v}=1 \pmod n.$$

2.6 Контрольные вопросы

1. Каковы процедуры инициализации объекта информационной защиты?
2. Опишите типовые схемы идентификации и аутентификации пользователя.
3. Каковы недостатки и достоинства схемы простой аутентификации с помощью пароля?