Методы идентификации и установление подлинности объекта и субъекта

Одной из важных задач обеспечения информационной безопасности при взаимодействии пользователей является использование методов и средств, позволяющих одной (проверяющей) стороне убедиться в подлинности другой (проверяемой) стороны. Для этого применяются средства аутентификации.

Идентификация (Identification) - процедура распознавания пользователя по его идентификатору. Эта функция выполняется, когда пользователь делает попытку войти в сеть. Пользователь сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

Аутентификация (Authentication) - процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль или сертификат).

После удачной идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация (Authorization) - процедура предоставления субъекту определенных полномочий и ресурсов в данной системе.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Администрирование (Accounting) - регистрация действий пользователя в сети, включая его попытки доступа к ресурсам.

Для подтверждения своей подлинности субъект может предъявлять системе разные сущности. В зависимости от них процессы аутентификации могут быть разделены на основе:

- знания чего-либо; примером могут служить пароль, персональный идентификационный номер PIN (Personal Identification Number);

– обладания чем-либо; обычно это магнитные карты, смарт-карты, сертификаты;
– каких-либо неотъемлемых характеристик; эта категория включает методы, базирующиеся на проверке биометрических характеристик пользователя; в данной категории не используются криптографические методы и средства; подобная аутентификация применятся для контроля доступа в помещения или к какой-либо технике;

Объектом идентификации могут быть человек, техническое средство, документы, носители информации и информация, отображаемая на дисплее и т.д.

Для установления подлинности субъектов используют различные опознавательные характеристики.

Основными и наиболее часто применяемыми методами установления подлинности пользователей являются методы, основанные на использовании *паролей.* Под паролем при этом понимается некоторая последовательность символов, сохраняемая в секрете и предъявляемая при обращении к КС. Ввод пароля, как правило, выполняют с клавиатуры.

Рассмотрим наиболее распространенные методы применения *паролей.*

Метод простого пароля предполагает ввод пользователем одного пароля с клавиатуры. При использовании данного метода пароль не изменяется от сеанса к сеансу в течение установленного администратором времени его существования.

Метод выборки символов заключается в запросе системой определенных символов пароля, выбираемых случайным образом. Каждому пользователю выделяется достаточно длинный пароль, причем каждый раз для опознавания используется не весь пароль, а только его некоторая часть. В процессе проверки подлинности система запрашивает у пользователя группу символов под данными порядковыми номерами. Количество символов и их порядковые номера для запроса определяются с помощью датчика псевдослучайных чисел. Такой способ не позволяет нарушителю определять пароль по однократному введению.

Метод паролей однократного использования предполагает наличие списка паролей, хранящихся в системе. При каждом обращении к системе пользователь вводит пароль, который после окончания работы вычеркивается системой из списка. Каждому пользователю выделяется список паролей. В процессе запроса номер пароля, который необходимо ввести, выбирается последовательно по списку или по схеме случайной выборки. Недостатком последних двух методов является необходимость запоминания пользователями длинных паролей или их списков.

Метод групп паролей. В данном случае система для каждого пользователя может потребовать пароли из 2 групп: первая включает пароли, которые являются ответами на общие для всех пользователей вопросы (имя, адрес, номер телефона). Вторая включает ответы на вопросы, которые устанавливаются администратором системы при регистрации пользователя. Эти запросы сформированы персонально для каждого пользователя. При каждом обращении пользователя система случайно выбирает несколько вопросов из каждой группы. Опознавание считается положительным, если пользователь правильно ответил на все вопросы. Недостаток данного метода в том, что необходим большой объем памяти для вопросов и ответов при большом числе пользователей.

Метод функционального преобразования предполагает некоторое преобразование, предложенное системой при регистрации пользователя, которое он может выполнять в уме. Паролем является результат этого преобразования.

Наиболее важными характеристиками пароля является его длина и период действия.

Ожидаемое безопасное время использования пароля или ожидаемое время раскрытия пароля вычисляют по формуле:

$$T_б = \frac{A^S t}{2}$$

где

A – число символов в алфавите, из которых составлен пароль;

S – длина пароля в символах;

t – время, требуемое на попытку введения пароля.

В случае удаленного доступа:

$$t = \frac{N}{V}$$

где

N – число символов передаваемых при попытке получить доступ;

V – скорость передачи данных, символов/мин.

Для получения пароля с вероятностью раскрытия не превышающую заданную, используют формулу:

$$4{,}32 * 10^4 \frac{VT}{NP} \leq A^S$$

где

T – период времени, в течение которого могут быть предприняты попытки отгадывания пароля;

P – задаваемая вероятность того, что правильный пароль может быть подобран нарушителем.

Процессы аутентификации можно также классифицировать по уровню обеспечиваемой безопасности:

- аутентификация, использующая пароли и PIN-коды;
- строгая аутентификация на основе использования криптографических методов и средств;
- биометрическая аутентификация пользователей.

С точки зрения безопасности каждый из перечисленных типов способствует решению своих специфических задач, поэтому каждый из них активно используется на практике.

Методы аутентификации, использующие пароли и PIN-коды. Одной из распространенных схем аутентификации является простая аутентификация, которая основана на применении паролей. К данной группе относятся все методы использования паролей - метод простого пароля, метод выборки символов, метод паролей однократного использования, метод групп паролей и метод функционального преобразования.

Наиболее распространенным методом аутентификации держателя пластиковой карты и смарт-карты является ввод секретного числа, которое обычно называют PIN-кодом.

Строгая аутентификация. Идея строгой аутентификации, реализуемая в криптографических протоколах, заключается в следующем. Проверяемая сторона доказывает свою подлинность проверяющей стороне, демонстрируя знание некоторого секрета. Например, этот секрет может быть предварительно распределен безопасным способом между сторонами аутентификационного обмена. Доказательство знания секрета осуществляется с помощью последовательности запросов и ответов с использованием криптографических методов и средств.

В зависимости от используемых криптографических алгоритмов протоколы строгой аутентификации делятся на протоколы, основанные на:

- симметричных алгоритмах шифрования;
- однонаправленных ключевых хэш-функциях;
- асимметричных алгоритмах шифрования;
- алгоритмах электронной цифровой подписи.

В большинстве случаев строгая аутентификация заключается в том, что каждый пользователь аутентифицируется по признаку владения своим секретным ключом.

Биометрическая аутентификация пользователя. Данный способ позволяет уверенно аутентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения. Основные достоинства биометрических методов:

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

При регистрации в системе пользователь должен продемонстрировать один или несколько раз свои характерные биометрические признаки. Эти признаки (известные как подлинные) регистрируются системой как контрольный «образ» (биометрическая подпись) законного пользователя. Этот образ пользователя хранится системой 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 предъявивший их признается законным пользователем или незаконным.

Дактилоскопические системы аутентификации. Одна из основных причин широкого распространения таких систем - наличие больших банков данных отпечатков пальцев. В общем случае биометрическая технология распознавания отпечатков пальцев заменяет защиту доступа с использованием пароля. Большинство систем используют отпечаток одного пальца. Небольшой размер и относительно невысокая цена датчиков отпечатков пальцев на базе интегральных схем превращает их в идеальный интерфейс для системы защиты.

Системы аутентификации по форме ладони используют сканеры формы ладони, обычно устанавливаемые на стенах. Устройства считывания создают объемное изображение ладони, измеряя длину пальцев, толщину и площадь поверхности ладони. Данные системы достаточно точны и обладают довольно низким коэффициентом ошибочного отказа.

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

Системы аутентификации по узору радужной оболочки и сетчатки глаза. Сетчатка человеческого глаза представляет собой уникальный объект для аутентификации. Рисунок кровеносных сосудов глазного дна отличается даже у близнецов. Такие системы являются наиболее надежными среди всех биометрических систем и применяются там, где требуется высокий уровень безопасности.

Взаимная идентификация удаленных рабочих станций. Для взаимной идентификации удаленных рабочих станций является предположение, что потенциальный злоумышленник прослушивает канал связи. Идентификация удаленных рабочих станций может быть выполнена по схеме, основанной на использовании алгоритма шифрования *E* и общего секретного ключа *K* для удаленных станций *A* и *B:*

1. Станция A посылает запрос на соединение со станцией B.
2. Станция B посылает случайное число *R*.

3. Станция *A* зашифровывает *R* по секретному ключу *K*, получая шифртекст *Ca* = *E(R,K)* и направляет станции *B* значение *Ca*.

4. Станция *B* вычисляет *Cb* = *E(R,K)*, и сравнивает значение *Cb* и *Ca*. Если *Cb* = *Ca* ,то подтверждается подлинность станции *A*, в противном случае связь прерывается.

Данная схема позволяет станции *B* удостовериться в том, что связь устанавливается со станцией *A*.

Такая схема взаимного распознавания удаленных абонентов (станций) называется *протоколом «рукопожатия»*.