Автор:

Завгородний Станислав Дмитриевич

студент

ФГАОУ ВО «Самарский национальный

исследовательский университет

им. академика С.П. Королева»

г. Самара, Самарская область

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ПАРОЛЕЙ. МОДЕЛЬ РУКОПОЖАТИЯ

Аннотация: *в данной статье рассмотрены понятия «идентификация», «идентификатор» и «аутентификация». В работе выделены способы аутентификации, аспекты парольной защиты.*

Ключевые слова: *пользователь, идентификация, аутентификация, пароль, защита.*

Введение

Идентификацией называется процедура распознавания по уникальному идентификатору субъекта. Идентификатор присваивается данному субъекту заранее и заносится в базу данных в момент регистрации субъекта в качестве легального пользователя системы.

Под аутентификацией принято понимать процедуру проверки подлинности входящего в систему объекта, предъявившего свой идентификатор.

Способы аутентификации

Выделяются три основные группы:

1. Основанные на знании пользователем некоторой подтверждающей его подлинность информации. Это парольная аутентификация и аутентификация на основе модели «рукопожатия». К плюсам такого способа аутентификации можно отнести: легкую запоминаемость и простую аппаратную реализацию. Из минусов: кража «секрета» незаметная для пользователя, а также стоит проблема выбор пароля.

2. Основанные на том, что пользователь имеет некоторый материальный объект, который может подтвердить его подлинность (пластиковая карта с идентифицирующей пользователя информацией и т п) – программно-аппаратные методы. Устройства аутентификации делятся на две группы: *активные* (имеют возможность выполнять алгоритмы, например генерация одноразовых паролей; имеют микропроцессор) и *пассивные* (используются только для хранения аутентификационного ключа)

3. Основанные на наличии у пользователя определенных признаков (биометрические данные, особенности клавиатурного почерка и росписи мыши и т. п.).

Аспекты парольной защиты

Сложность подбор пароля определятся мощностью множества символов, используемых для создания пароля, и длинной пароля.

Основные параметры политики парольной защиты:

1. Максимальный срок действия
2. Неповторяемость пароля
3. Минимальный срок действия пароля
4. Не совпадения пароля с логином

Реакция системы на попытки подбора пароля:

1. Ограничение попыток ввода
2. Нарастающий интервал между попытками ввода пароля
3. Учет всех попыток

Возможна реакция виде блокировки учетной записи.

Хранение паролей:

1. Хранение в открытой БД
2. Шифрование БД
3. Хранение Хэшей паролей

Модель рукопожатия

Модель рукопожатия является модификацией парольной защиты и позволяет провести аутентификацию не только пользователя, но и системы. Главным

отличием от парольной защиты является то, что секретом в данном случае выступает функция, а не пароль. Стороны заранее согласовывают функцию. К такой функции предъявляется следующее требование: не возможность восстановления функции по ее значениям.

В соответствии с этой моделью пользователь П и система С согласовывают при регистрации пользователя в КС функцию f, известную только им. Протокол аутентификации пользователя в этом случае выглядит следующим образом:

1. С: генерация случайного значения x; вычисление y = f(x); вывод x для пользователя.

2. П: вычисление y' =f'(x); ввод y'.

3. С: если y и y' совпадают, то пользователь допускается к работе в системе, иначе попытка входа в систему отклоняется.

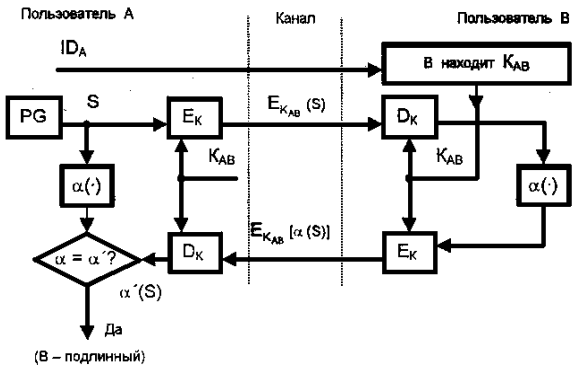

Рис. 1. Схема процедуры рукопожатия

Преимущества аутентификации на основе модели «рукопожатия» перед парольной аутентификацией:

– между пользователем и системой не передается никакой конфиденциальной информации, которую нужно сохранять в тайне;

– каждый следующий сеанс входа пользователя в систему отличен от предыдущего, поэтому даже длительное наблюдение за этими сеансами ничего не даст нарушителю.

К недостаткам аутентификации на основе модели «рукопожатия» относится большая длительность этой процедуры по сравнению с парольной аутентификацией.