Идентификация и аутентификация, управление доступом.

Подготовил:

Панченко Денис Дмитриевич
1132229056
НБИбд-03-22

Российский университет дружбы народов, Москва, Россия

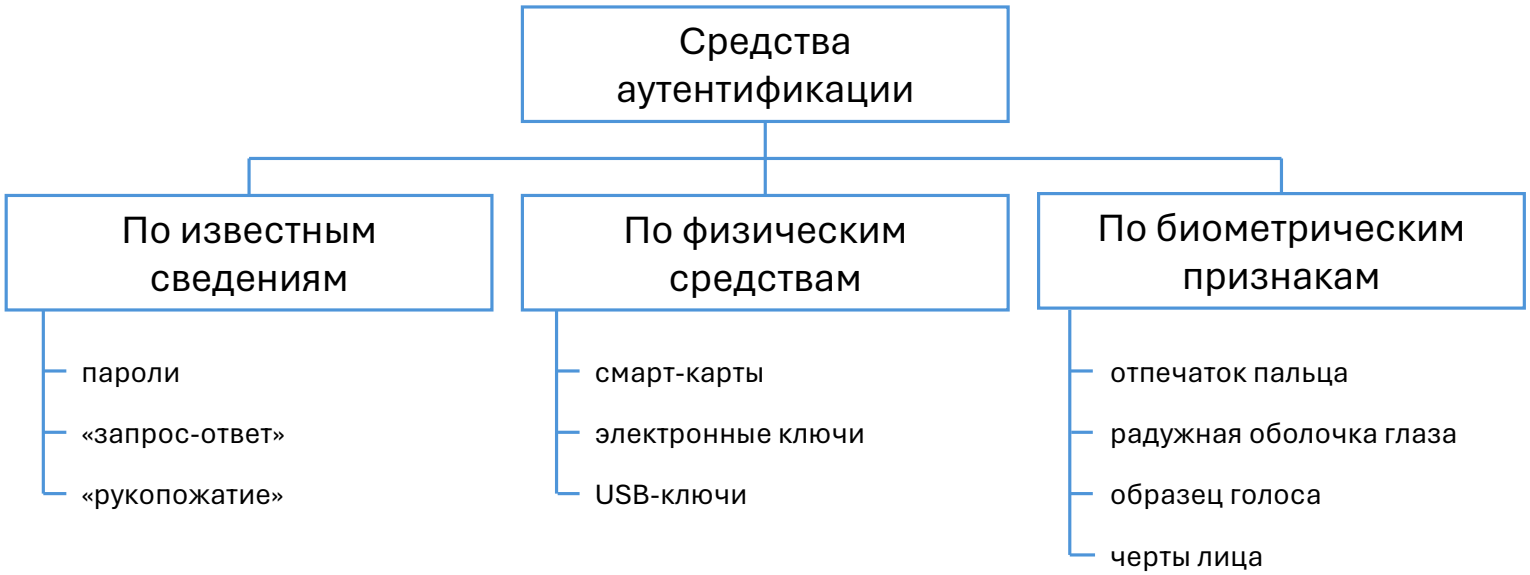
Идентификация и аутентификация

Идентификация – это процесс распознавания субъекта с помощью заранее присвоенного идентификатора.

Аутентификация – это процесс, который обеспечивает проверку законности субъекта аутентификации и устанавливает, является ли он тем, за кого себя выдает.

Идентификация является частью **аутентификации** и заключается в работе с именем субъекта (логин).

Классификация средств аутентификации



Парольные средства аутентификации

Главное достоинство парольной аутентификации – простота и привычность.

Недостатки парольных средств аутентификации:

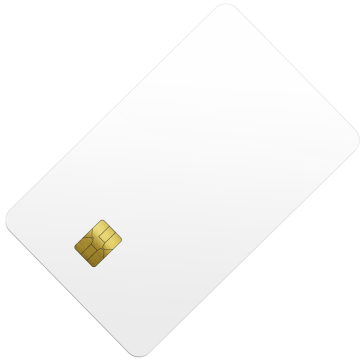
- пароли должны быть надежными;
- необходимость периодической смены паролей;
- необходимость использования разных паролей для разных систем, требующих аутентификации.

Носимые средства аутентификации

Электронный ключ (iButton)
48-битный код;

Смарт-карта код от 64 бит;

USB-ключ.



Сервер аутентификации Kerberos

Kerberos – это программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений. Клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем.

Биометрия

Биометрия представляет собой совокупность автоматизированных методов идентификации и аутентификации людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности **отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п.**

Протоколы удаленной аутентификации

Общие правила разработки протокола аутентификации:

1. Инициатор сеанса должен подтверждать свою личность прежде, чем это сделает отвечающая сторона.
2. Следует использовать два раздельных общих секретных ключа.
3. Инициатор и отвечающий должны выбирать оклики из различных непересекающихся наборов.
4. Протокол должен уметь противостоять атакам, при которых запускается второй параллельный сеанс.

Авторизация субъектов

Авторизация - это процедура контроля доступа легальных субъектов к ресурсам системы и предоставление каждому из них именно тех прав, которые ему были определены администратором.

Помимо предоставления пользователям прав доступа к каталогам, файлам и принтерам, средства авторизации могут контролировать возможность выполнения пользователями различных системных функций.

Принципы организации разграничения доступа

Ограничение доступа может задаваться в форме правил.

На основании правил система управления доступом в любой момент времени динамически решает вопрос о предоставлении или не предоставлении доступа.

Принципы организации разграничения доступа

Разграничение доступа может осуществляться несколькими способами:

- По спискам контроля доступа (ACL)
- С использованием избирательного или дискреционного управления доступом (DAC)
- С помощью полномочного или мандатного управления доступом (MAC)
- По ролевому доступу (RBAC)

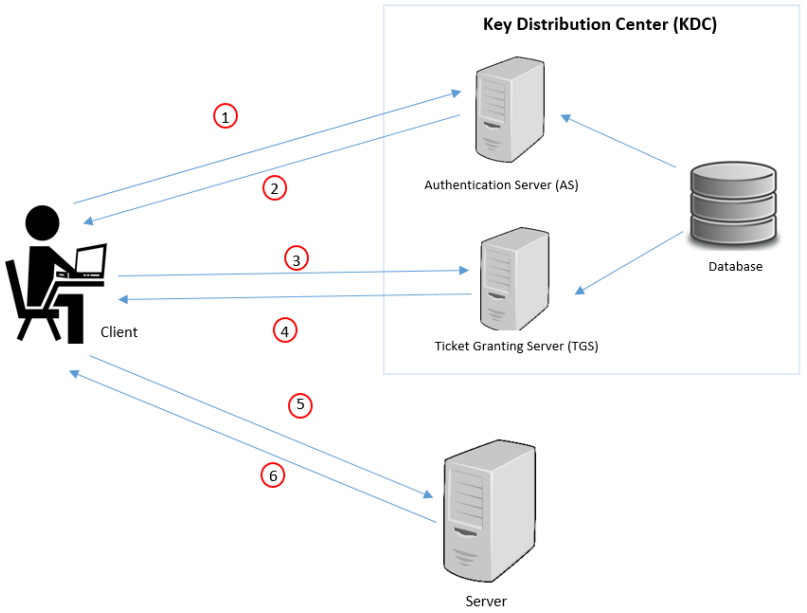
Применение методов разграничения доступа

Популярной мерой ограничения доступа в сеть Интернет является капча.

Управление доступом в операционных системах

В работе протокола Kerberos, помимо рабочей станции, принимают участие еще три сервера:

1. Сервер аутентификации (AS, Authentication Server): проверяет личность пользователей при входе в сеть.
2. Сервер выдачи билетов (TGS, Ticket Granting Server): выдает «билеты, подтверждающие подлинность».
3. Сервер, предоставляющий услуги рабочей станции.



Заключение

Таким образом, идентификация, аутентификация и управление доступом играют важную роль в обеспечении безопасности информации и предотвращении несанкционированного доступа к ресурсам системы. Эти процессы являются основополагающими в области информационной безопасности и требуют комплексного подхода для эффективной реализации.