РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

РЕФЕРАТ

на тему

«Идентификация и аутентификация, управление доступом»

Выполнил

Студент группы НБИбд-03-22

Студенческий билет №: 1132229056

Панченко Д. Д.

Москва 2024

Оглавление

Введение

В мире информационных технологий и безопасности данных, идентификация, аутентификация и управление доступом играют ключевую роль в обеспечении конфиденциальности, целостности и доступности информации. Эти понятия обозначают различные этапы процесса проверки личности пользователя и решения о предоставлении доступа к ресурсам.

Глава 1. Идентификация и аутентификация

1.1. Идентификация и аутентификация

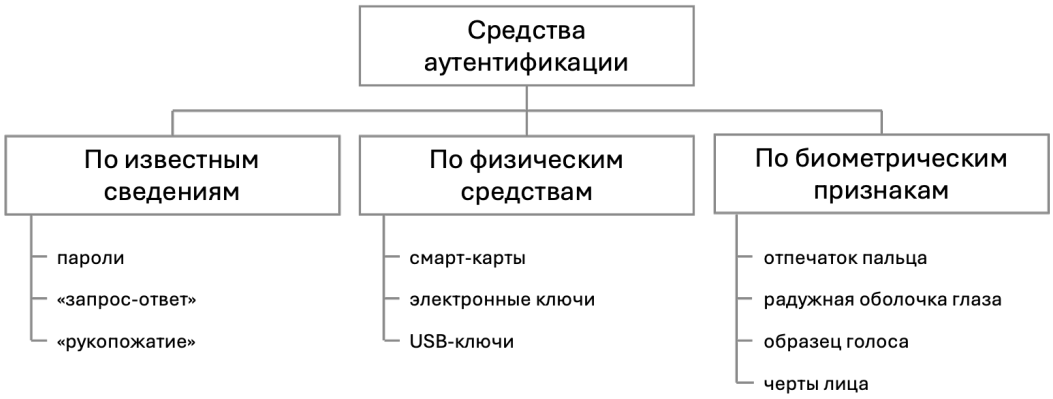
Идентификация – это процесс распознавания субъекта с помощью заранее присвоенного идентификатора.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя).

Аутентификация – это процесс, который обеспечивает проверку законности субъекта аутентификации и устанавливает, является ли он тем, за кого себя выдает. Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова " аутентификация " иногда используют словосочетание "проверка подлинности".

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

1.2. Классификация средств аутентификации



1.3. Парольные средства аутентификации

Главное достоинство парольной аутентификации – простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Недостатки парольных средств аутентификации:

1. Пароли должны быть надежными;

2. Необходимость периодической смены паролей;

3. Необходимость использования разных паролей для разных систем, требующих аутентификации.

1.4. Носимые средства аутентификации

Электронный ключ (iButton) 48-битный код;

Смарт-карта код от 64 бит;

USB-ключ.

1.5. 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.

1.6. 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. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

1.7. Общие правила разработки протокола аутентификации

1. Инициатор сеанса должен подтверждать свою личность прежде, чем это сделает отвечающая сторона. Это помешает злоумышленнику получить ценную для него информацию, прежде чем он подтвердит свою личность.

2. Следует использовать два раздельных общих секретных ключа: один для инициатора сеанса, а другой для отвечающего.

3. Инициатор и отвечающий должны выбирать оклики из различных непересекающихся наборов. Например, инициатор должен пользоваться четными номерами, а отвечающий — нечетными.

4. Протокол должен уметь противостоять атакам, при которых запускается второй параллельный сеанс, информация для которого извлекается при помощи первого сеанса (или наоборот). Если нарушается хотя бы одно из этих правил, протокол оказывается уязвимым.

1.8. 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.

Термин авторизация (authorization) происходит от латинского слова auctoritas, показывающее уровень престижа человека в Древнем Риме и соответствующие этому уровню привилегии.

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

Глава 2. Управление доступом

2.1. 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.

Правило строится с учетом различных факторов, например:

• длительность сеанса связи;

• возраст;

• время суток и т. п.

2.2. Разграничение доступа может осуществляться несколькими способами

• По спискам контроля доступа (ACL – Access Control List):

Разграничение доступа по спискам контроля доступа заключается в том, что для каждого элемента защищаемых данных (файла, базы, программы) составляется список всех тех пользователей, которым предоставлено право доступа к соответствующему элементу, или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа.

• С использованием избирательного или дискреционного управления доступом (DAC – Discretionary Access Control, матрицей контроля доступа):

Избирательное или дискреционное управление доступом (разграничение доступа по матрицам полномочий) предполагает формирование двумерной матрицы, по строкам которой содержатся идентификаторы зарегистрированных пользователей, а по столбцам – идентификаторы защищаемых элементов данных

• С помощью полномочного или мандатного управления доступом (MAC – Mandatory Access Control) – по уровням секретности:

Полномочное (мандатное) управление доступом есть способ разового разрешения на допуск к защищаемому элементу данных. Заключается он в том, что каждому защищаемому элементу присваивается персональная уникальная метка, после чего

доступ к этому элементу будет разрешен только тому пользователю, который в своем запросе предъявит метку элемента (мандат), которую ему может выдать администратор защиты или владелец элемента.

• По ролевому доступу (RBAC – Role-based Access Control) – недискреционному методу доступа:

Ролевое управление доступом использует роли, которые, по сути, соответствуют понятиям «должность» и «круг должностных обязанностей». Набор ролей должен соответствовать перечню различных должностей, существующих на предприятии. Одна и та же роль может быть приписана разным субъектам.

2.3. Применение методов разграничения доступа

Популярной мерой ограничения доступа в сеть Интернет является капча.

2.4. 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.