Идентификация и аутентификация. Управление доступом.

Доклад по предмету ’Информационная безопсносность

Парфенова Е. Е.

10 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Парфенова Елизавета Евгеньвена
- студент
- Российский университет дружбы народов
- 1032216437@pfur.ru
- https://github.com/parfenovaee

Вводная часть

Актуальность

- Проблема защиты данных в современном мире выходит на первый план, так как им в век быстрой цифровизации всех процессов необходима усиленная защита.
- Компании, работающие с конфиденциальными данными, должны обеспечивать высокие стандарты безопасности для предотвращения несанкционированного доступа.
- Идентификация и аутентификация, а также управление доступом становятся важными инструментами в обеспечении целостности и безопасности данных, что делает изучение и внедрение данных технологий крайне актуальными в современных условиях.

Цели и задачи

Цель: Ознакомление с понятиями идентификации и аутентификации, их классификацией, типовой схемой этих процессов, а также краткое описание наиболее популярных методов. Кроме того, будет рассмотрено управление доступом, включая его основные задачи, распространенные модели и технологии.

Задачи:

- Познакомиться с понятиями идентификации и аутентификации, рассмотреть их классификацию
- Рассмотреть типовую схему этих процессов
- Кратко описать два популярных метода аутентификации
- Изучить задачи управления доступом
- Обозначить распространенные модели и технологии управления доступом

Идентификация и аутентификация

Понятия идентификации и аутентификации

Идентификация - это процесс присвоения уникального идентификатора субъектам и объектам доступа, который затем сравнивается с заданным перечнем.

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

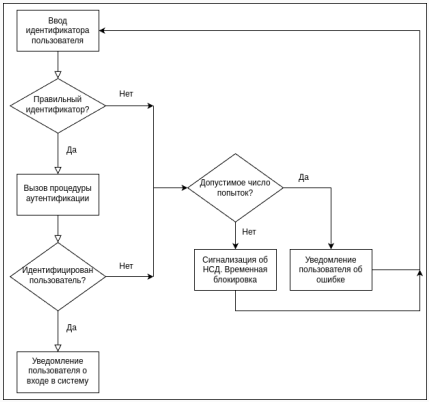

Рис. 1: Классическая процедура аутентификации-идентификации

Способы подтверждения подлинности субъектом

- **Знание** — информация, которую знает субъект
- **Владение** — вещь, которой обладает субъект
- **Часть субъекта (биометрия)** - свойство, которым обладает субъект

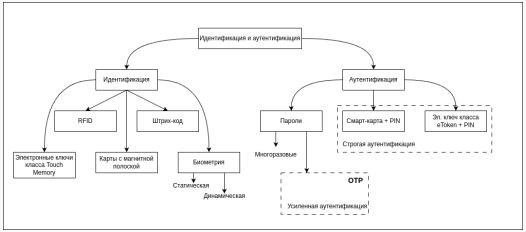

Рис. 2: Способы идентификации-аутентификации

Классификация аутентификации

Классификация аутентификации:

- Односторонняя - только клиент доказывает свою подлинность
- Двусторонняя - обе стороны подтверждают свою подлинность

- Однофакторная - один способ подтверждения
- Двухфакторная - сразу два способа аутентификации. Пример: Github
- Трехфаткорная - все три способа: например, пароль + код из СМС + отпечаток пальца

Связь понятий идентификация и аутентификация

Последовательность процессов:

1) Идентификация: определение личности пользователя
2) Аутентификация: проверка подлинности
3) Авторизация: предоставление прав доступа к ресурсам

Типовая схема идентификации и аутентфиикации

- IDi- неизменный идентификатор i-го пользователя
- Ki - аутентифицирующая информация пользователя
- E_i равно $F(S_iK_i)$, где S_i - случайный вектор, уникальный для каждого пользователя

Таблица 1: Модифицированный объект-эталон

Номер пользователя	Информация для идентификации	Информация для аутентификации
1	ID_1	E_1
2	ID_2	E_1
...	...	...
N	ID_i	E_i

Популярные способы аутентификации

1. Парольная аутентификация

Простая, привычная, но достаточно уязвимая

.

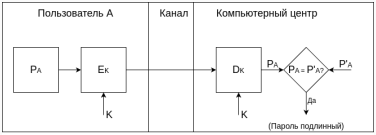

Рис. 3: Схема простой аутентификации с помощью пароля

2. Биометрическая аутентификая

Совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик: отпечатков пальцев, сечатки и роговицы глаз, почерка и так далее

Управление доступом

Задачи управления доступом

Управление доступом включает в себя несколько основных задач:

- Определение объектов доступа и идентификация субъектов доступа
- Разработка матрицы доступа
- Управление учетными записями и аудит прав доступа

Таблица 2: Матрица доступа

Сбуъекты/Объекты	Файл	Программа	Линия связи	База данных
User 1	r	rwe	rw с 9:00 до 18:00	rw
User 2	rw	r	orw	
User 3	rwo	rw		r

Модели управления доступом

1) Дискреционная модель управления доступом (DAC): владелец объекта сам может устанавливать и изменять права доступа к объекту
2) Мандатная модель управления доступом (MAC): доступ определяется на основе меток конфиденциальности
3) Ролевая модель управления доступом (RBAC): Права доступа назначаются ролям, а не отдельным пользователям

Технологии управления доступом

1) Логические системы: обеспечивают контроль доступа к информационным системам с помощью паролей, двухфакторной аутентификации и шифрования
2) Физические системы: используют электронные ключи, биометрические системы и камеры для контроля доступа к физическим объектам
3) Сетевые системы: управляют доступом к сетевым ресурсам и обеспечивают авторизацию пользователей

Вывод

Выводы

В данном докладе были рассмотрены ключевые понятия идентификации и аутентификации, их классификация и типовые схемы. Мы кратко описали два популярных метода аутентификации и изучили задачи управления доступом, а также распространенные модели и технологии. Понимание этих процессов является важным шагом к обеспечению безопасности информации и ресурсов в современных организациях.

Ресрусы

1. С. К. Варлатая М.В.Ш. Аппаратно-программные средства и методы защиты информации. Владивосток: ДВГТУ, 2007. 318 с.

2. Идентификация и аутентификация, управление доступом [Электронный ресурс]. Интернет Университет Информационных Технологий, 2006. URL: https://citforum.ru/security/articles/galatenko/.

3. Многофакторная аутентификация [Электронный ресурс]. Wikimedia Foundation, Inc., 2023. URL: https://ru.wikipedia.org/wiki/Многофакторная_ аутентификация/.

4. Управление доступом и учетными записями [Электронный ресурс]. Интел- лектуальная безопасность» (Security Vision), 2020. URL: https://www.secu rityvision.ru/blog/avtomatizatsiya-protsessov-upravleniya-informatsionnoy-bezopasnostyu-upravlenie-dostupom-i-uchetnymi/.