Презентация по информационной безопасности

Протокол Kerberos

Саргсян А. Г.

18 октября 2023

Российский университет дружбы народов, Москва, Россия

Основные понятия и термины

Kerberos — это сетевой протокол централизованной аутентификации клиентов компьютерных сетей на основе архитектуры клиент-сервер.

Аутентификация — это процесс проверки личности пользователя или устройства.

Авторизация — это процесс определения разрешений и прав доступа, которые пользователь получает после успешной аутентификации.

Основные компоненты

1. Клиент (Client)
2. Ключевой распространитель (Key Distribution Center - KDC)
3. Билет (Ticket)
4. Сервер (Server)
5. Сессионный ключ (Session Key)

Схема работы протокола

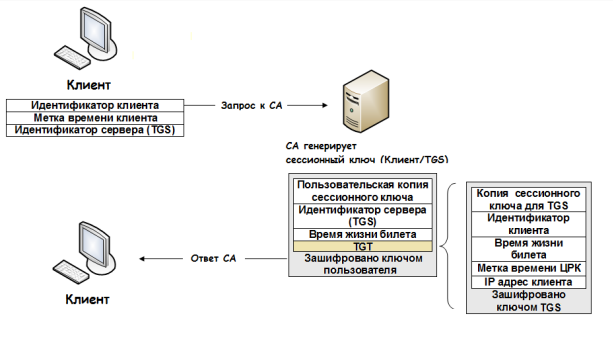

Рис. 1: Схема работы протокола

Преимущества и недостатки

Преимущества Kerberos	Недостатки Kerberos
1. Безопасность	1. Сложность настройки
2. Централизованное управление	2. Зависимость от доверия к KDC
3. Ограниченное время действия билетов	3. Исключение из билетов
4. Интеграция с разными ОС и приложениями	4. Ограничения для мобильных и децентрализованных сетей

Применение протокола

1. Корпоративные сети
2. Операционные системы
3. Системы управления доступом
4. Электронная почта и веб-приложения
5. Облачные решения
6. Виртуальные частные сети (VPN)

Вывод

- Централизованное управление: Kerberos облегчает управление безопасностью в сетях благодаря централизованной аутентификации и распределению ключей.
- Интеграция и распространение: Протокол широко используется в различных областях, от корпоративных сетей до образования, что подчеркивает его универсальность.
- Преимущества и недостатки: Понимание преимуществ и недостатков Kerberos помогает в принятии обоснованных решений о его внедрении.
- Безопасность и конфиденциальность: Kerberos обеспечивает надежную защиту данных и поддерживает высокий стандарт безопасности.