Протокол Kerberos

Выполнил: Калинин Тимур

Группа: НФИбд-02-19

Общие сведения

- Kerberos – сетевой протокол аутентификации
- Был разработан в 1988 в MIT
- Работает через незащищенное сетевое соединение

Проблемы при аутентификации по незащищенному соединению

- Проблема передачи пароля. Kerberos решает эту проблему при помощи использования криптографических ключей.
- Проблема обмена паролем. Решается при помощи использования доверенного защищенного посредника (KDC – Key Distribution Center или Центр распределения ключей)

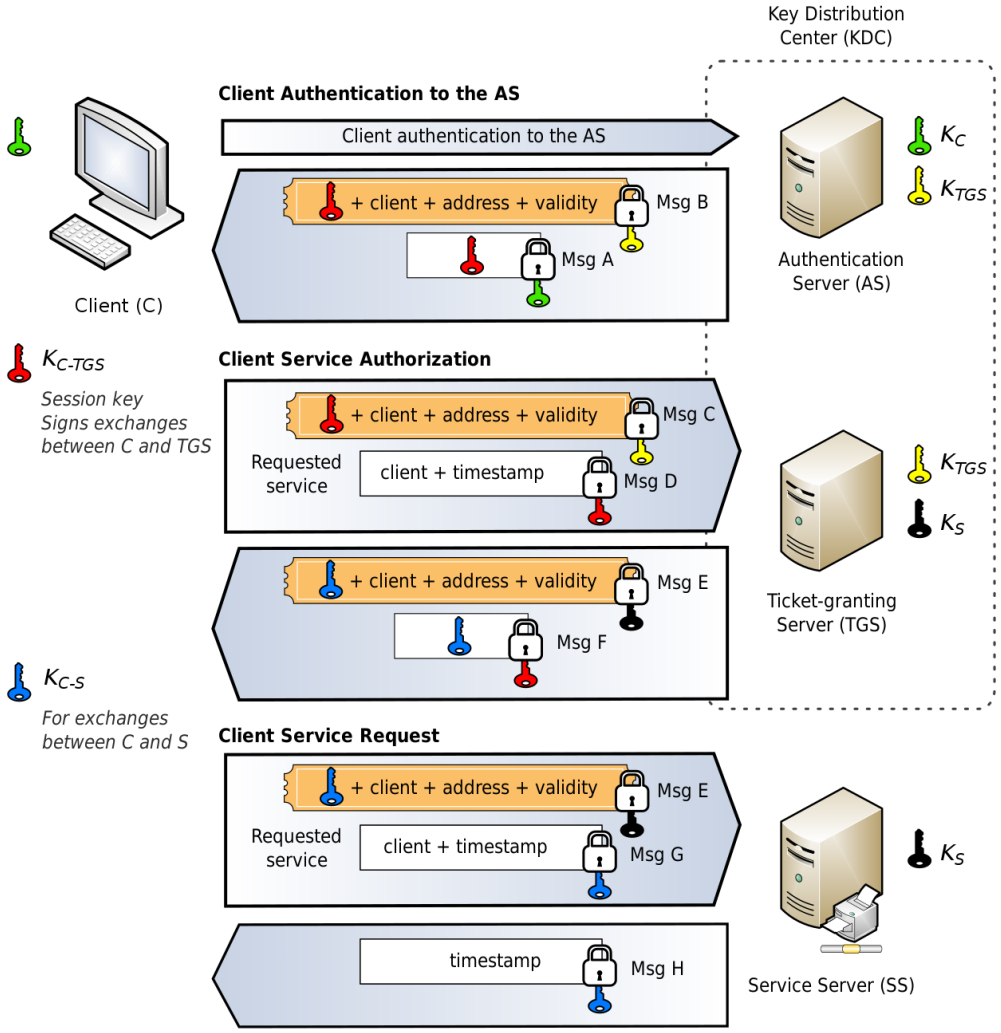
Центр распределения ключей

- Доверенный посредник, который хранит долговременные криптографические ключи для клиента и для сервера.
- При авторизации в качестве данных доступа выдает так называемые сессионные ключи, используемые клиентом для доступа к конкретной службе.

Термины протокола Kerberos

- Билет (ticket) – временные данные, выдаваемые клиенту для аутентификации на сервере, на котором располагается необходимая служба. Выдаются сервером TGS (Ticket Granting Server)
- Клиент (client) – некая сущность в сети, которая может получить билет от Kerberos.
- Центр выдачи ключей (key distribution center, KDC) – сервис, выдающий билеты Kerberos.

Основной принцип работы Kerberos



Версии протокола Kerberos

- Kerberos 4. Выпущена в 1988. Поддержка прекращена в 2006.
- Kerberos 5. Выпущена в 1993.
- Расширение PKINIT. Разработано в 2006.

Поддержка

- Kerberos поддерживается следующими операционными системами:
  - Windows 2000 и более поздние версии
  - различные UNIX и UNIX подобные ОС (Apple Mac OS X, Red Hat Enterprise Linux 4, FreeBSD)

Источники

- 1. Kerberos (protocol) . Wikipedia (электронный ресурс). URL: https://en.wikipedia.org/wiki/Kerberos_(protocol)
- 2. Kerberos. Национальная библиотека им. Н. Э. Баумана (электронный ресурс). URL: https://ru.bmstu.wiki/Kerberos