РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ДОКЛАД

на тему: Протокол Kerberos

дисциплина: Информационная безопасность

Студент: Калинин Тимур Дмитриевич

Группа: НФИбд-02-19

МОСКВА

2022 г.

Содержание

Введение 3
Проблемы при аутентификации по незащищенному соединению 3
Основные термины 4
Центр распределения ключей 4
Обращение клиента к серверу через KDC 4
Схема работы Kerberos 5
Особенность реализации Kerberos 6
Версии протокола Kerberos 7
Поддержка 7
Список литературы 8

Введение

Протокол Kerberos – сетевой протокол аутентификации, предлагающий механизм взаимной аутентификации клиента и сервера перед установлением связи между ними.

Первая версия протокола Kerberos была создана в 1988 году в Массачусетском технологическом институте (MIT) в рамках проекта «Афина». Основной целью проекта являлась разработка плана по внедрению компьютеров в учебный процесс MIT и сопутствующего этому ПО [1].

Kerberos предлагает возможность аутентификации при условии, что подключение, через который она проходит, не защищено.

Проблемы при аутентификации по незащищенному соединению

Для наглядности представим следующую ситуацию. Предположим, есть два агента в сети, знающих один и тот же секрет (условно, Алиса и Боб). Они хотят обмениваться друг с другом сообщениями. Чтобы Бобу быть уверенным, что информация приходит действительно от Алисы и наоборот, они договорились о пароле, который знают только они. Если собеседник предоставляет в письме пароль, значит, сообщение действительно пришло от него. Возникает вопрос: каким образом передавать этот пароль в сообщении. Можно было бы просто включить пароль в тело сообщения, но откуда Боб и Алиса знают, что их сообщения не перехватываются где-то посередине пути. Очевидно, так делать нельзя. Для решения этой проблемы Kerberos использует симметричное шифрование. Вместо передачи пароля, все сообщение шифруется так, чтобы расшифровать его мог только агент, знающий пароль. Шифрование должно быть симметричным, чтобы один и тот же ключ мог и зашифровать сообщение и расшифровать его [1].

Другая проблема: каким образом договориться о пароле? В реальной жизни Боб и Алиса могут встретиться друг с другом вживую и безопасно сообщить пароль. Но в компьютерной сети это невозможно. Для решения этих проблем проектом «Афина» и был разработан специальный протокол — Kerberos. По аналогии с древнегреческой мифологией, этот протокол был назван в честь трёхголового пса, который защищал выход из царства Аида, — Цербера, или более точно — Кербера. Трём головам Цербера в протоколе соответствуют три участника безопасной связи:

клиент, сервер и доверенный посредник между ними. Роль посредника здесь играет центр распределения ключей «Key distribution center», KDC.

Основные термины

Для начала определим некоторые термины, которые помогут нам понять принцип работы 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.

Центр распределения ключей

Центр распределения ключей (KDC) — это служба, работающая на физически защищенном сервере. Центр хранит базу данных с информацией об учётных записях всех клиентов сети. Вместе с информацией о каждом абоненте в базе центра распределения ключей хранится криптографический ключ, известный только этому абоненту и службе центра. Этот ключ служит для связи клиента с центром [1].

Обращение клиента к серверу через KDC

Если клиент хочет обратиться к серверу — он посылает сообщение центру распределения ключей. Центр направляет каждому участнику сеанса копии сеансового ключа, действующие в течение небольшого промежутка времени. Назначение этих ключей — проведение аутентификации клиента и сервера. Копия сеансового ключа, пересылаемая на сервер, шифруется с помощью долговременного ключа этого сервера, а направляемая клиенту — долговременного ключа данного клиента. Теоретически, для выполнения функций доверенного посредника центру распределения ключей достаточно направить сеансовые ключи непосредственно абонентам безопасности. Однако на практике реализовать такую схему чрезвычайно сложно. Поэтому на практике применяется другая схема управления паролями,

которая делает протокол Kerberos гораздо более эффективным [1].

Схема работы Kerberos

В ответ на запрос клиента, который намерен подключиться к серверу, служба KDC направляет обе копии сеансового ключа клиенту. Сообщение, предназначенное клиенту, шифруется посредством долговременного ключа, общего для данного клиента и KDC, а сеансовый ключ для сервера вместе с информацией о клиенте вкладывается в блок данных, получивший название сеансового мандата («session ticket»). Затем сеансовый мандат целиком шифруется с помощью долговременного ключа, который знают только служба KDC и данный сервер. После этого вся ответственность за обработку мандата, несущего в себе шифрованный сеансовый ключ, возлагается на клиента, который должен доставить его на сервер. Получив ответ KDC, клиент извлекает из него мандат и свою копию сеансового ключа, которые помещает в безопасное хранилище (оно располагается не на диске, а в оперативной памяти) [1].

Когда возникает необходимость связаться с сервером, клиент посылает ему сообщение, состоящее из мандата, который по-прежнему зашифрован с применением долговременного ключа этого сервера, и собственного аутентификатора, зашифрованного посредством сеансового ключа. Этот мандат в комбинации с аутентификатором как раз и составляет удостоверение, по которому сервер определяет «личность» клиента. Сервер, получив «удостоверение личности» клиента, прежде всего с помощью своего секретного ключа расшифровывает сеансовый мандат и извлекает из него сеансовый ключ, который затем использует для дешифрования аутентификатора клиента. Если все проходит нормально — делается заключение, что удостоверение клиента выдано доверенным посредником, то есть — службой KDC. Клиент может потребовать у сервера проведения взаимной аутентификации. В этом случае сервер с помощью своей копии сеансового ключа шифрует метку времени из аутентификатора клиента и в таком виде пересылает её клиенту в качестве собственного аутентификатора [2].

Одно из достоинств применения сеансовых мандатов состоит в том, что серверу не нужно хранить сеансовые ключи для связи с клиентами. Они сохраняются в кэш-памяти удостоверений («credentials cache») клиента, который направляет

мандат на сервер каждый раз, когда хочет связаться с ним. Сервер, со своей стороны, получив от клиента мандат, дешифрует его и извлекает сеансовый ключ. Когда надобность в этом ключе исчезает, сервер может просто стереть его из своей памяти.

Такой метод дает и ещё одно преимущество: у клиента исчезает необходимость обращаться к центру KDC перед каждым сеансом связи с конкретным сервером. Сеансовые мандаты можно использовать многократно. На случай же их хищения устанавливается срок годности мандата, который KDC указывает в самой структуре данных. Это время определяется политикой Kerberos для конкретной области. Обычно срок годности мандатов не превышает восьми часов, то есть — стандартной продолжительности одного сеанса работы в сети. Когда пользователь отключается от неё, кэш-память удостоверений обнуляется, и все сеансовые мандаты вместе с сеансовыми ключами уничтожаются [1].

Особенность реализации Kerberos

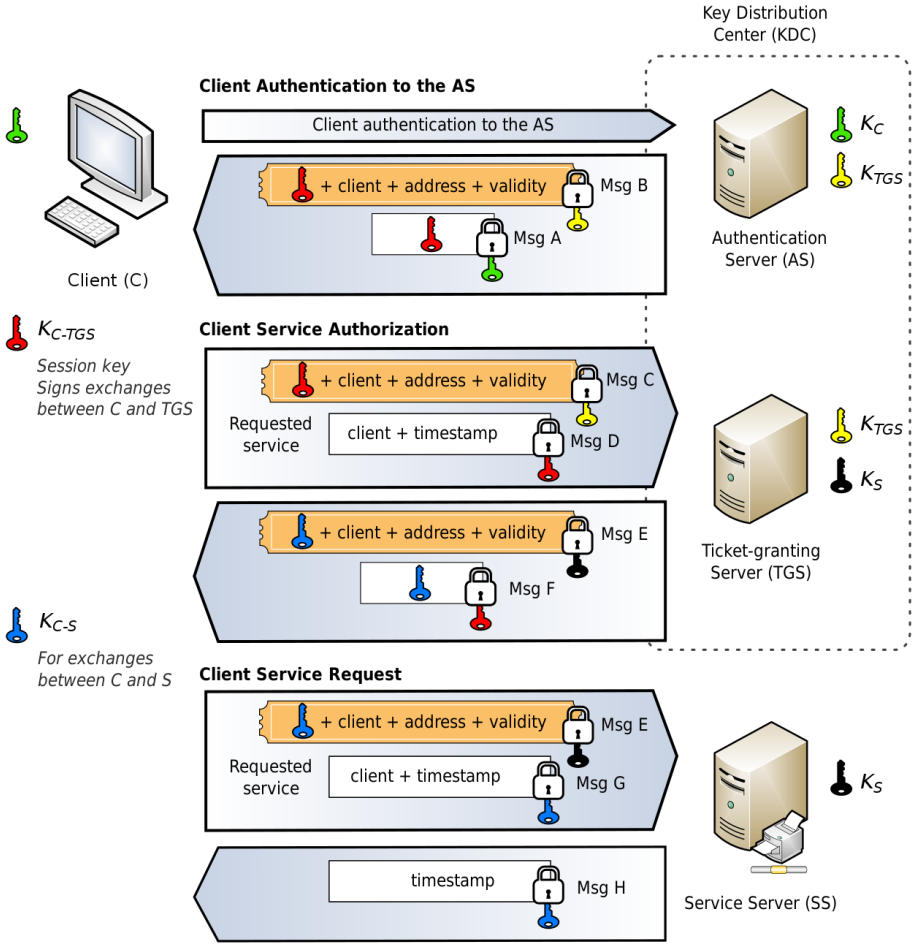

Рис. 1. Схема работы Kerberos

Однако, как видно из Рис. 1, у нас имеются три сервера, а не два. Дело в том, что реализация протокола Kerberos предполагает использование сервера аутентификации и сервера TGS отдельно. Сначала пользователь проходит аутентификацию на сервере аутентификации, а затем обращается к конкретной сетевой службе через TGS, используя ключ сессии (на рисунке обозначен синим цветом). Один AS может быть связан с несколькими TGS, таким образом, пользователю не придется заново проходить аутентификацию, если ему потребуется доступ к другой службе и он сможет обратиться к этой службе используя уже полученный от AS ключ сессии.

Версии протокола Kerberos

Первая стабильная версия протокола называлась Kerberos 4 и была выпущена в 1988 году. В 2006 году было объявлено о прекращении поддержки Kerberos 4.

С целью преодоления проблем безопасности предыдущей версии Джоном Колем (John Kohl) и Клиффордом Ньюманом (Clifford Neuman) была разработана 5 версия протокола, которая была опубликована в 1993 году. По прошествии времени, в 2005 спецификацией начала заниматься IETF Kerberos work group. В июне 2006 года был представлен RFC 4556 описывающий расширение для 5-й версии под названием PKINIT (англ. public key cryptography for initial authentication in Kerberos). Данный RFC описывал, как использовать асимметричное шифрование на этапе аутентификации клиента [2].

Поддержка

Поддержка протокола на данный момент предусмотрена во многих ОС. Среди них:

- Windows 2000 и более поздние версии.
- различные UNIX и UNIX подобные ОС (Apple Mac OS X, Red Hat Enterprise Linux 4, FreeBSD) [1]

Список литературы

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