РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

**Реферат**

**«Протокол kerberos»**

*Дисциплина: «Информационная безопасность»*

Студент: Абакумов Егор Александрович

Группа: НПИбд-01-18

**МОСКВА**

2021 г.

Оглавление

**Введение3**

**Протокол Kerberos4**

История создания и применения4

Устройство протокола Kerberos4

**Порядок взаимодействия компонентов в сети8**

**Заключение12**

**Список литературы13**

# **Введение**

Обеспечение информационной безопасности строится на использовании защищенных каналов связи, однако не менее важным параметром является разграничение доступа к таким каналам. Вопрос надежной идентификации и аутентификации пользователей является основополагающим в построении безопасной информационной сети.

Одним из наиболее удачных решений проблемы аутентификации является повсеместно используемый протокол Kerberos, в частности его 5-я версия под названием Heimdal. Именно данную модификацию мы и рассмотрим в данной работе.

Итак, целью работы является ознакомление с основными механизмами устройства протокола Kerberos как с точки зрения структурного устройства, так и программного взаимодействия компонент.

Предметом исследования является протокол обеспечения аутентификации Kerberos.

Задачами работы станут:

1. Рассмотрение основных структурных компонентов сети протокола Kerberos;
2. Изучение порядка взаимодействия составных частей сети протокола Kerberos.

# **Протокол Kerberos**

## История создания и применения

Протокол был разработан в начале 80-х годов XX века программистами из Массачусетского технологического института как решение проблемы построения распределенной вычислительной системы Athena. В рамках этой задачи был разработан и внедрен протокол аутентификации удаленного пользователя. Сочетание специальных криптографических средств позволило, с одной стороны, свести на нет вероятность перехвата пароля и иметь зашифрованный канал передачи данных между компьютерами, а с другой стороны, иметь систему единого входа, которая позволяет пользователю зарегистрироваться один раз при входе в систему, а затем иметь свободный доступ ко всем сетевым ресурсам на основе этой регистрации.

Протокол получился настолько удачным, что скоро вышел отдельным стандартом и получил название Kerberos (по имени трехголового пса из древнегреческих мифов, стерегущего вход в царство мертвых), стал широко применяться независимо от Athena как система регистрации в крупных финансовых и академических учреждениях. [1]

Наиболее известное применение Kerberos получил в качестве средства аутентификации OС Windows — Microsoft Active Directory, где и используется по сей день.

Устройство протокола Kerberos

В общем виде аппаратно сеть для Kerberos состоит из следующих компонентов:

* клиент (англ. Client);
* сетевой ресурс, к которому хочет подключиться клиент (англ. Server);
* центр распределения ключей (англ. Key Distribution Center, сокр. KDC).

Протокол Kerberos подразумевает централизованное распределение симметричных ключей шифрования, что означает, что у каждого абонента сети есть только один основной ключ, который используется для взаимодействия с центром распределения ключей (сервером ключей). Чтобы получить ключ шифрования для защиты обмена данными с другим абонентом, пользователь обращается к серверу ключей, который назначает симметричный сеансовый ключ этому пользователю и соответствующему абоненту.

# Протокол Kerberos обеспечивает распределение симметричных ключей шифрования и аутентификацию пользователей, работающих в незащищенной сети. Реализация Kerberos представляет собой программную систему, построенную на архитектуре клиент-сервер. Клиентская часть устанавливается на всех компьютерах защищенных сетей, за исключением тех, на которых установлены компоненты сервера Kerberos. В частности, сетевые серверы (файловый сервер, серверы печати и т.д.) могут выступать в качестве клиентов Kerberos. [2]

# Серверная часть Kerberos называется Центром Распределения Ключей (англ. Key Distribution Center, сокр. KDC) и состоит из следующих двух компонентов:

# сервер аутентификации (англ. Authentication Server, сокр. AS);

# сервер выдачи разрешений (англ. Ticket Granting Server, сокр. TGS).

# Сервер Kerberos назначает симметричный ключ шифрования, общий для каждого субъекта сети, и поддерживает базу данных субъектов и их секретных ключей. Схема функционирования протокола Kerberos показана на рис. 1. [2]



Рисунок 1. Схема устройства сети Kerberos.

# **Порядок взаимодействия компонентов в сети**

# Рассмотрим процесс аутентификации пользователя посредством протокола Kerberos.

# Получив приглашение на ввод имени пользователя, пароля и домена, пользователь указывает эти данные. Затем компьютер пользователя обращается к службе KDC и передает ей имя пользователя, имя домена, а также текущее время на рабочей станции пользователя, при этом имя пользователя передается в открытом виде, текущее время на рабочей станции пользователя передается в зашифрованном виде и является аутентификатором. Ключ шифрования формируется из пароля пользователя в результате хеширования.

# Далее служба KDC ищет пользователя в базе данных пользователей, выявляет мастер ключ пользователя, который основан на пароле пользователя и расшифровывает аутентификатор, т. е. получает время отправки запроса. Разница во времени отправки запроса и текущего времени на контроллере домена не должно превышать определенного значения, установленного политикой протокола Kerberos.

# Затем KDC создает два объекта:

# ключ сессии, посредством которого будет обеспечиваться зашифрование данных при обмене между клиентом и службой KDC;

# билет на получение билета (англ. Ticket-Granting Ticket, сокр. TGT). TGT включает: вторую копию ключа сессии, имя пользователя, время окончания жизни билета. Билет на получение билета шифруется с использованием собственного мастер ключа службы KDC, который известен только KDC, т. е. TGT может быть расшифрован только самой службой KDC.

# После этого служба KDC зашифровывает аутентификатор пользователя (англ. time stamp) и ключ сессии с помощью ключа клиента. После чего эти данные отправляются клиенту.

# Компьютер клиента получает информацию от службы KDC, проверяет аутентификатор, расшифровывает ключ сессии и таким образом получает ключ сессии и TGT, что предоставляет возможность безопасного взаимодействия со службой KDC. Клиент аутентифицирован в домене и получает возможность осуществлять доступ к ресурсам домена.

# Теперь, имея свободный доступ к службе KDC, клиенту требуется получить доступ к сетевым ресурсам на других серверах в том же домене. Для этого клиент обращается к службе KDC, представляя KDC свой TGT и маркер времени, которые зашифрованы с помощью ключа сессии, известного службе KDC.

# KDC в свою очередь расшифровывает TGT, используя свой собственный ключ. Маркер времени расшифровывается с помощью сессионного ключа. Теперь KDC может подтвердить, что запрос пришел от «правильного» пользователя, т. к. этот пользователь использует соответствующий сессионный ключ.

# KDC создает пару билетов, один для клиента, один для сервера, к ресурсам которого клиент должен будет получать доступ. Каждый билет содержит имя пользователя, запрашивающего доступ, получателя запроса, маркер времени, показывающий, когда был создан билет, а также срок жизни билета. Оба билета будут также содержать новый ключ, K\_cs который, таким образом известен и клиенту, и серверу. Этот ключ будет обеспечивать возможность безопасного взаимодействия между ними. KDC шифрует билет сервера, используя мастер – ключ сервера, затем вкладывает билет сервера внутрь билета клиента, который также содержит ключ K\_cs.

# Далее вся эта структура зашифровывается с помощью сессионного ключа, который стал доступен пользователю при аутентификации. После чего эта информация отправляется клиенту, который расшифровывает его с помощью сессионного ключа, т. е. K\_cs становится доступным клиенту, K\_cs доступен также и серверу. При этом клиент не может прочитать билет сервера, так как он зашифрован на ключе сервера.

# Клиент зашифровывает маркер времени с помощью ключа, K\_cs затем отправляет маркер времени и билет сервера самому серверу, к ресурсам которого он пытается получить доступ.

# Получив эту информацию, на первом этапе сервер расшифровывает свой билет, используя свой долговременный ключ. Это предоставляет возможность получить доступ к K\_cs, с помощью которого будет на втором этапе расшифрован маркер времени, полученный от клиента.

# Теперь и клиент, и сервер обладают ключом K\_cs. Следовательно, сервер может быть уверен в том, что клиент правильно идентифицирован, так как для шифрования маркера времени был использован сессионый ключ K\_cs. В случае необходимости ответа сервера клиенту, сервер воспользуется этим ключом. Клиент будет знать, что сервер правильно идентифицирован, поскольку сервер должен использовать верный ключ сервера, чтобы получить сессионный ключ K\_cs. [3]**Заключение**

Рассмотрев лишь основные аспекты протокола, можно сделать вывод, что Протокол Kerberos предоставляет надежную взаимную аутентификацию пользователя и сетевого ресурса, не передает входных данных, таких как пароль или даже хэш пароля, между устройствами, чем обеспечивает дополнительную безопасность, позволяет практически бесшовно обеспечить безопасность аутентификации ресурсов в сети. Устройство Kerberos позволяет применение протокола даже в самых высоконагруженных сетях, ввиду незначительности создаваемой дополнительной нагрузки.

Таким образом, протокол завоевывает все большую популярность, являясь стандартом безопасности даже в крупных государственных учреждениях, таких как, например, Министерство Обороны США, что дополнительно подтверждает доверие к Kerberos. Своим появлением протокол задал новую планку в вопросе безопасной взаимной аутентификации пользователей в сетях.

# **Список литературы**

1. Изучаем принцип работы Неimdal Kerberos. [Электронный ресурс]. – URL: <https://www.securitylab.ru/analytics/265153.php> (дата обращения 28.11.21).
2. Протокол сетевой аутентификации Kerberos 5 [Электронный ресурс]. – URL: <https://www.ixbt.com/comm/kerberos5.shtml> (дата обращения 28.11.21).
3. Kerberos за 5 минут: знакомство с сетевой аутентификацией [Электронный ресурс]. – URL: <https://bestprogrammer.ru/izuchenie/kerberos-za-5-minut-znakomstvo-s-setevoj-autentifikatsiej> (дата обращения 28.11.21).
4. The Kerberos Network Authentication Service (V5) [Электронный ресурс]. – URL: <https://datatracker.ietf.org/doc/html/rfc4120> (дата обращения 28.11.21).