Система Kerberos

Kerberos — это сетевая служба, предназначенная для централизованного решения задач аутентификации в крупных сетях. Kerberos реализует процедуру единого логического входа в пределах домена, где клиенты и серверы поддерживают этот протокол.

Система централизованной аутентификации тесно связана с системой централизованного управления доступом, так как последняя должна основываться на результатах аутентификации каждый раз, когда вычислительный процесс, представляющий пользователя, пытается получить доступ к ресурсу компьютера, входящего в некоторый домен.

Система Kerberos может работать в среде многих популярных ОС, например в ОС семейства Windows система Kerberos встроена как основной компонент безопасности. Существуют реализации Kerberos для семейства Unix, включая Red Hat Linux, Fedora, Centos, Ubuntu, и для Mac OS X. Первая версия Kerberos была разработана для проекта Athena в Массачусетском технологическом институте. Текущей версией является версия 5, которая стандартизована IETF в RFC 4120.

В основе функционирования этой достаточно громоздкой системы лежит несколько простых принципов:

- в сетях, использующих систему безопасности Kerberos, все процедуры аутентификации между клиентами и серверами сети выполняются через посредника, которому доверяют обе стороны процесса аутентификации, причем таким авторитетным арбитром является сама система Kerberos;
- в системе Kerberos клиент должен доказывать свою аутентичность для доступа к каждой службе, услуги которой он запрашивает;
- все обмены данными в сети выполняются в защищенном виде с применением симметричного алгоритма шифрования AES (или DES в ранних реализациях Kerberos).

Сетевая служба Kerberos построена в архитектуре клиент-сервер, что позволяет ей работать в самых сложных сетях. Kerberos-клиент устанавливается на всех компьютерах сети, которые могут обратиться к какой-либо сетевой службе. В таких случаях Kerberos-клиент от лица пользователя передает запрос на Kerberos-сервер и поддерживает с ним диалог, необходимый для выполнения функций системы Kerberos.

Итак, в системе Kerberos имеются следующие участники: Kerberos-сервер, Kerberos-клиенты, ресурсные серверы (рис. 1). Kerberos-клиенты пытаются получить доступ к сетевым ресурсам — файлам, приложениям, принтеру и т. д., находящимся на ресурсных серверах. Этот доступ может быть предоставлен, во-первых, только легальным пользователям, а во-вторых, при наличии у них достаточных полномочий, определяемых службами авторизации соответствующих ресурсных серверов — файловым сервером, сервером приложений, сервером печати. Однако в системе Kerberos ресурсным серверам запрещается «напрямую» принимать запросы от клиентов, им разрешается начинать рассмотрение запроса клиента только тогда, когда на это поступает разрешение от Kerberos-сервера. Таким образом, путь клиента к ресурсу в системе Kerberos состоит из трех этапов:

1. Определение легальности клиента, логический вход в сеть, получение разрешения на продолжение процесса получения доступа к ресурсу.
2. Получение разрешения на обращение к ресурсному серверу.
3. Получение разрешения на доступ к ресурсу.

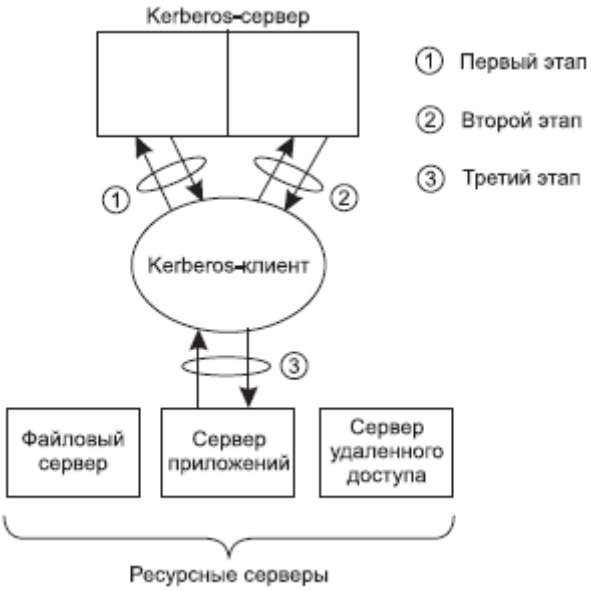

Рис. 1. Три этапа работы системы Kerberos

Для решения первой и второй задач клиент обращается к Kerberos-серверу. Каждая из этих двух задач решается отдельным сервером, входящим в состав Kerberos-сервера. Выполнение первичной аутентификаций и выдача разрешения на продолжение процесса получения доступа к ресурсу осуществляются так называемым *Kersberos-сервером аутентификации* (Authentication Server, AS). Этот сервер хранит в своей базе данных информацию об идентификаторах и паролях пользователей. Пароли пользователей, а точнее — хэш-функции от паролей, являются секретными ключами пользователей.

Вторую задачу, связанную с получением разрешения на обращение к ресурсному серверу, решает другая часть Kerberos-сервера — *Kerberos-сервер квитанций* (Ticket-Granting Server, TGS). Сервер квитанций для легальных клиентов выполняет дополнительную проверку и дает клиенту разрешение на доступ к нужному ему ресурсному серверу, для чего наделяет его электронной формой-квитанцией. Для выполнения своих функций сервер квитанций использует копии секретных ключей всех ресурсных серверов, которые хранятся у него в базе данных. Помимо этих ключей TGS-сервер имеет еще один секретный ключ, общий с AS-сервером.

Третья задача — получение разрешения на доступ непосредственно к ресурсу — решается на уровне ресурсного сервера собственными средствами, *не относящимися* непосредственно к системе Kerberos, но способными взаимодействовать с ней.

Секретные ключи пользователей и ресурсных серверов образуют базу данных ключей Kerberos-сервера. Собственно, обладание секретным ключом и является условием аутентификации пользователя или ресурсного сервера. Помимо секретных ключей пользователей и ресурсных серверов в Kerberos также применяются секретные ключи сеансов аутентификации, которые распределяет Kerberos-сервер. Из-за этого обстоятельства Kerberos-сервер также называется *Kerberos Key Distribution Centre*, или *Kerberos KDC*. Секретные ключи пользователей и ресурсных серверов называют еще мастер-ключами, так как они являются постоянными ключами, аутентифицирующими субъект, в отличие от ключей сеансов, которые имеют непродолжительный срок действия.

Введение центра аутентификации существенно улучшает масштабируемость системы аутентификации на основе симметричного шифрования по сравнению с децентрализованной системой. Действительно, если на предприятии имеется N пользователей и M ресурсных серверов, которым нужна взаимная аутентификация (мы предполагаем, что пользователям взаимная аутентификация не нужна), то при децентрализованной аутентификации необходимо $N \times M$ ключей, что для предприятия с 1000 сотрудников и 50 ресурсными серверами дает 50 000 ключей. При централизованной систем аутентификации необходимо иметь только $N + M$ ключей, что равно 1050 ключей для нашего примера — то есть почти в 50 раз меньше.

Необходимо подчеркнуть, что Kerberos обеспечивает защищенную аутентификацию сторон только в начальный момент сеанса обмена данными между ними. После этого защита данных — их конфиденциальность, аутентичность и целостность — должна обеспечиваться средствами ресурсного

сервера и клиента, если это необходимо.

ПРИМЕЧАНИЕ

При описании протоколов взаимодействия Kerberos-клиента и Kerberos-сервера, а также Kerberos-клиента и ресурсного сервера использован термин «квитанция» (ticket), означающий в данном случае электронную форму, выдаваемую Kerberos-сервером клиенту, которая играет роль некоего удостоверения личности и разрешения на доступ к ресурсу.

Первичная аутентификация

Процесс доступа пользователя к ресурсам включает две процедуры: во-первых, пользователь должен доказать свою легальность (аутентификация), во-вторых, он должен получить разрешение на выполнение определенных операций с определенным ресурсом (авторизация). В системе Kerberos пользователь один раз аутентифицируется во время логического входа в сеть, а затем проходит процедуры аутентификации и авторизации всякий раз, когда ему требуется доступ к новому ресурсному серверу.

Выполняя логический вход в сеть, пользователь, точнее, Kerberos-клиент, установленный на его компьютере, посылает серверу аутентификации AS идентификатор пользователя ID (рис. 2).

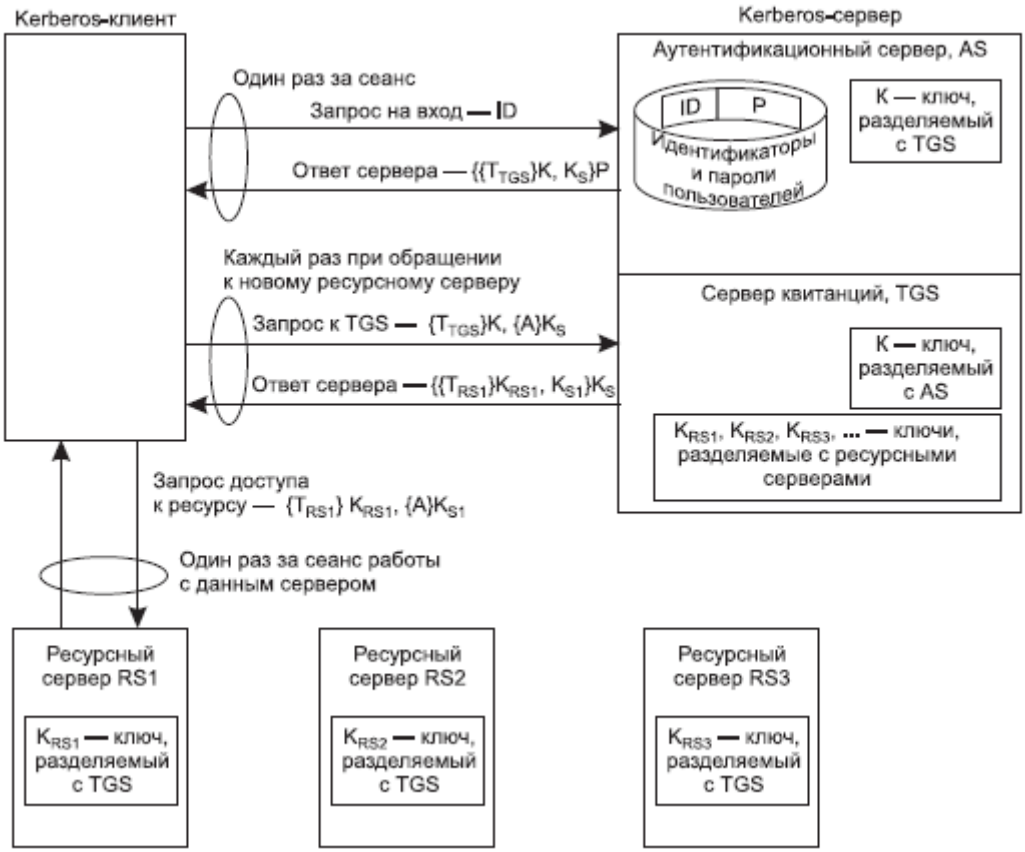

Рис. 2. Последовательность обмена сообщениями в системе Kerberos

Вначале сервер аутентификации проверяет в базе данных, имеется ли в ней запись о пользователе с таким идентификатором. Затем, если такая запись существует, он извлекает из нее пароль пользователя p. Данный пароль потребуется для шифрования всей информации, которую направит сервер аутентификации Kerberos-клиенту в качестве ответа. А ответ состоит из квитанции T_{TGS} на доступ к Kerberos-серверу квитанций и ключа сеанса K_S. Под сеансом здесь понимается все время работы пользователя от момента логического входа в сеть до момента логического выхода. Ключ сеанса потребуется для шифрования в процедурах аутентификации в течение всего пользовательского сеанса. Квитанция шифруется с помощью секретного мастер-ключа K, который разделяют серверы аутентификации и квитанций Kerberos KDC. Все вместе — зашифрованная квитанция и ключ сеанса — еще раз шифруются с помощью хэша пользовательского пароля p. Таким образом, квитанция шифруется дважды ключом K и паролем p. В приведенных обозначениях сообщение-ответ, которое сервер

аутентификации посылает клиенту, выглядит так: $\{\{T_{TGS}\}K, K_S\}p$.

После того как такое ответное сообщение поступает на клиентскую машину, клиентская программа Kerberos просит пользователя ввести свой пароль. Когда пользователь вводит пароль, то Kerberos-клиент пробует с помощью хэша пароля расшифровать поступившее сообщение. Если пароль верен, то из сообщения извлекаются квитанция на доступ к серверу квитанций $\{T_{TGS}\}K$ (в зашифрованном виде) и ключ сеанса K_S (в открытом виде). Успешное дешифрование сообщения означает успешную аутентификацию. Заметим, что сервер аутентификации AS аутентифицирует пользователя без передачи пароля по сети. Нужно отметить, что успешность дешифрования будет проверена позже, когда пользователь попытается применить полученную квитанцию и ключ сеанса при обращении к серверу квитанций TGS.

Квитанция T_{TGS} на доступ к серверу квитанций TGS является удостоверением легальности пользователя и разрешением ему продолжать процесс получения доступа к ресурсу. Эта квитанция содержит:

- идентификатор пользователя;
- идентификатор сервера квитанций, на доступ к которому получена квитанция;
- отметку о текущем времени;
- период времени, в течение которого может продолжаться сеанс;
- копию ключа сеанса K_S.

Как уже отмечалось, клиент обладает квитанцией в зашифрованном виде. Шифрование повышает уверенность в том, что никто, даже сам клиент — обладатель данной квитанции — не сможет квитанцию подделать, подменить или изменить. Только TGS-сервер, получив от клиента квитанцию, сможет ее расшифровать, так как в его распоряжении имеется ключ шифрования K.

Время действия квитанции ограничено длительностью сеанса. Разрешенная длительность сеанса пользователя, содержащаяся в квитанции на доступ к серверу квитанций, задается администратором и может изменяться в зависимости от требований к защищенности сети. В сетях с жесткими требованиями к безопасности время сеанса может быть ограничено 30 минутами, в других условиях это время может составить 8 часов. Информация, содержащаяся в квитанции, определяет ее срок годности. Предоставление квитанции на вполне определенное время защищает ее от неавторизованного пользователя, который мог бы ее перехватить и применить в будущем.

Получение разрешения на доступ к ресурсному серверу

Итак, следующим этапом для пользователя является получение разрешения на доступ к ресурсному серверу (например, к файловому серверу или серверу приложений). Но для этого надо обратиться к TGS-серверу, который выдает такие разрешения (квитанции). Чтобы получить доступ к серверу квитанций, пользователь уже обзавелся квитанцией $\{T_{TGS}\}K$, выданной ему AS-сервером. Несмотря на защиту паролем и шифрование, пользователю, помимо квитанции, нужно кое-что еще, чтобы доказать серверу квитанций, что он имеет право на доступ к ресурсам сети.

Как уже упоминалось, первое сообщение от сервера аутентификации содержит не только квитанцию, но и секретный ключ сеанса K_S, который разделяется с сервером квитанций (TGS). Клиент задействует этот ключ для шифрования еще одной электронной формы, называемой *аутентификатором* $\{A\}K_S$. Аутентификатор A содержит идентификатор и сетевой адрес пользователя, а также собственную временную отметку. В отличие от квитанции $\{T_{TGS}\}K$, которая в течение сеанса требуется многократно, аутентификатор предназначен для одноразового применения и имеет очень короткое время жизни — обычно несколько минут. Kerberos-клиент посылает серверу квитанций сообщение-запрос, содержащее квитанцию и аутентификатор: $\{T_{TGS}\}K$, $\{A\}K_S$.

Сервер квитанций расшифровывает квитанцию имеющимся у него ключом K, проверяет, не истек ли срок действия квитанции, и извлекает из нее идентификатор пользователя.

Затем TGS-сервер расшифровывает аутентификатор, применяя ключ сеанса пользователя K_S, который он извлек из квитанции. Сервер квитанций сравнивает идентификатор пользователя и его сетевой адрес с аналогичными параметрами в квитанции и сообщении. Если они совпадают, сервер квитанций удостоверяется, что данная квитанция действительно представлена ее законным владельцем. Применение ключа сеанса из зашифрованной квитанции говорит TGS-серверу, что квитанция действительно была выдана AS-сервером, так как она была расшифрована мастер-ключом, который известен только паре AS-TGS.

Заметим, что простое обладание квитанцией на получение доступа к серверу квитанций не доказывает идентичности пользователя. Так как аутентификатор действителен только в течение короткого промежутка времени, то маловероятно украсть одновременно и квитанцию, и аутентификатор и применить их в течение этого времени.

Каждый раз, когда пользователь обращается к серверу квитанций для получения новой квитанции на доступ к ресурсу, он посылает многоразовую квитанцию и новый аутентификатор.

Клиент обращается к серверу квитанций за разрешением на доступ к ресурсному серверу, который здесь обозначен как RS1. Сервер квитанций, удостоверившись в легальности запроса и личности пользователя, отсылает ему ответ, содержащий две электронных формы: многоразовую квитанцию на получение доступа к запрашиваемому ресурсному серверу T_{RS1} и новый ключ сеанса K_{S1}.

Квитанция на получение доступа шифруется секретным ключом K_{RS1}, общим только для сервера квитанций и того сервера, к которому предоставляется доступ, в данном случае — RS1. Сервер квитанций разделяет уникальные секретные ключи с каждым сервером сети. Эти ключи распределяются между серверами сети физическим способом или каким-либо иным секретным способом при установке системы Kerberos. Когда сервер квитанций передает квитанцию на доступ к какому-либо ресурсному серверу, то он шифрует ее, так что только этот сервер сможет расшифровать ее с помощью своего уникального ключа.

Новый ключ сеанса K_{S1} содержится не только в самом сообщении, посылаемом клиенту, но и внутри квитанции T_{RS1}. Все сообщение шифруется старым ключом сеанса клиента K_S, так что его может прочитать только этот клиент. Учитывая введенные обозначения, ответ TGS-сервера клиенту можно представить в следующем виде: $\{\{T_{RS1}\}K_{RS1}, K_{S1}\}K_S$.

Получение доступа к ресурсу

Когда клиент расшифровывает поступившее сообщение, то он отсылает серверу, к которому он хочет получить доступ, запрос, содержащий квитанцию на получение доступа и аутентификатор, зашифрованный новым ключом сеанса: $\{T_{RS1}\}K_{RS1}, \{A\}K_{S1}$.

Это сообщение обрабатывается аналогично тому, как обрабатывался запрос клиента TGS-сервером. Сначала расшифровывается квитанция ключом K_{RS1}, затем извлекается ключ сеанса K_{S1} и расшифровывается аутентификатор. Далее сравниваются данные о пользователе, содержащиеся в квитанции и аутентификаторе. Если проверка проходит успешно, то доступ к сетевому ресурсу разрешается.

На этом этапе клиент тоже может захотеть проверить аутентичность сервера перед тем, как начать с ним работать. *Взаимная процедура аутентификации* предотвращает любую возможность попытки получения неавторизованным пользователем доступа к секретной информации от клиента путем подмены сервера.

Аутентификация ресурсного сервера в системе Kerberos выполняется в соответствии со следующей процедурой. Клиент обращается к серверу с предложением, чтобы тот прислал ему сообщение, в котором повторил временну*ю* отметку из аутентификатора клиента, увеличенную на единицу. Кроме того, требуется, чтобы данное сообщение было зашифровано ключом сеанса K_{S1}. Чтобы выполнить такой запрос клиента, сервер извлекает копию ключа сеанса из квитанции на доступ, применяет этот ключ для расшифровки аутентификатора, наращивает значение временно*й* отметки на единицу, заново зашифровывает сообщение с помощью ключа сеанса и возвращает сообщение клиенту. Клиент расшифровывает это сообщение, чтобы получить увеличенную на единицу временну*ю* отметку.

При успешном завершении описанного процесса клиент и сервер удостоверяются в секретности своих транзакций. Кроме того, они получают ключ сеанса, который могут использовать для шифрования будущих сообщений.

Достоинства и недостатки

Изучая довольно сложный механизм системы Kerberos, нельзя не задаться вопросом: какое влияние оказывают все эти многочисленные процедуры шифрования и обмена ключами на производительность сети, какую часть ресурсов сети они потребляют, как это сказывается на ее пропускной способности?

Ответ весьма оптимистичный — если система Kerberos реализована и сконфигурирована правильно, ее работа сказывается на производительности сети незначительно. Так как квитанции используются многократно, сетевые ресурсы, затрачиваемые на запросы предоставления квитанций, невелики. Хотя передача квитанции при аутентификации логического входа несколько снижает пропускную способность, такой обмен требуется в любых других системах и для любых методов аутентификации. Дополнительные

же издержки незначительны. Опыт внедрения системы Kerberos показал, что время отклика при установленной системе Kerberos существенно не отличается от времени отклика без нее — даже в очень больших сетях с десятками тысяч узлов. Такая эффективность делает систему Kerberos весьма перспективной.

Среди уязвимых мест системы Kerberos можно назвать централизованное хранение всех секретных ключей системы. Успешная атака на Kerberos-сервер, в котором сосредоточена вся информация, критическая для системы безопасности, приводит к краху информационной защиты всей сети. Поэтому хранилище мастер-ключей должно быть хорошо защищено.

Для защиты секретных мастер-ключей в процессе первоначального создания (заведении новых учетных записей пользователей и ресурсных серверов в хранилище KDC) необходимо создавать защищенный канал между компьютером пользователя или ресурсным сервером и Kerberos KDC.

Возможен также полный отказ от паролей пользователя за счет цифровых сертификатов пользователя на первом этапе аутентификации, когда пользователь обращается к AS-серверу квитанцией T_{TGS}. Это расширение протокола Kerberos описано в документе RFC 4556, Public Key Cryptography for Initial Authentication in Kerberos (PKINIT). Предполагается, что пользователь применяет для логического входа смарт-карту, на которой хранится цифровой сертификат, выпущенный доверенным сертификационным центром. После того как пользователь локально аутентифицирует себя как легальный владелец смарт-карты, его компьютер передает запрос на логический вход AS-серверу системы Kerberos, в котором содержится цифровой сертификат пользователя с его открытым ключом, а также стандартный для Kerberos аутентификатор (идентификатор пользователя, его сетевой адрес и временная отметка), зашифрованный закрытым ключом пользователя, хранящимся на смарт-карте.

AS-сервер проверяет подлинность сертификата путем обращения к серверу сертификатов (корпоративному или публичному), затем расшифровывает аутентификатор с помощью открытого ключа пользователя и извлекает из него идентификатор пользователя. Если этот идентификатор имеется в базе идентификаторов пользователей AS-сервера, то сервер отвечает стандартным образом, то есть посылает пользователю квитанцию T_{TGS}, зашифрованную ключом K, а также ключ сеанса K_S — однако ответ шифруется открытым ключом пользователя, а не его паролем. Пользователь расшифровывает ответ с помощью своего закрытого ключа, и на этом работа расширения PKINIT заканчивается.

Еще одной слабостью системы Kerberos является то, что исходные коды приложений, доступ к которым осуществляется через Kerberos, должны быть соответствующим образом модифицированы. Такая модификация называется «кербиризацией» приложения. Некоторые поставщики продают «кербиризованные» версии своих приложений. Однако если такой версии нет и нет исходного текста, то Kerberos не может обслуживать доступ к такому приложению.

В заключение хочется еще раз подчеркнуть, что стандартная версия Kerberos (соответствующая документу RFC 4210 и некоторым другим документам RFC, разработанным в IETF рабочей группой Kerberos) выполняет только аутентификацию пользователей. Авторизация оставлена ресурсным серверам, которые должны, например, задействовать списки доступа при принятии решения о том, что может делать конкретный пользователь, представленный своим идентификатором в квитанции Kerberos, и что ему делать запрещено.