Протокол аутентификации Kerberos
(описание и применение в операционной системе Windows)

Эссе Галановой Яны Антольевны, студентки 018 гр.

Краткое описание протокола Kerberos

Kerberos представляет собой протокол проверки подлинности с доверенной третьей стороной, разработанный для сетей TCP/IP. Установленная в сети служба Kerberos действует как доверенный посредник, обеспечивая надежную сетевую аутентификацию. Это предоставляет пользователям возможность работать на нескольких машинах сети. Kerberos создан на базе симметричной криптографии (в нем реализован алгоритм DES, но вместо него можно использовать и другие алгоритмы). При общении с каждым субъектом сети Kerberos использует различный общий секретный ключ, и знание этого секретного ключа равносильно доказательству идентичности субъекта.

Протокол Kerberos был первоначально разработан в МИТ для проекта Athena. Версии протокола с 1 по 3 представляли собой рабочие версии, предназначенные только для внутреннего использования (в пределах МИТ). Версии 4 и 5 уже являются общедоступными для внедрения протокола в различные рабочие среды.

Модель, применяемая в Kerberos. В модель Kerberos включены расположенные в сети объекты – клиенты и серверы. Клиентами могут также выступать и пользователи, и независимые программы, выполняющие такие, к примеру, действия: загрузка файлов, передача сообщений, доступ к базам данных, доступ к принтерам, получение административных привилегий и т.д.

Kerberos поддерживает базу данных клиентов и их секретных ключей. Для пользователей-людей секретный ключ представлен в виде зашифрованного пароля. Сетевые службы, требующие аутентификации, и клиенты этих служб регистрируют в Kerberos свои секретные ключи.

Так как Kerberos имеет все секретные ключи, то он может посылать сообщения, убеждающие один объект в подлинности другого. Kerberos также создает сеансовые ключи, которые выдаются клиенту и серверу (или двум клиентам) и никому больше. Сеансовый ключ используется для шифрования сообщений, которыми обмениваются две стороны, и уничтожаются после окончания сеанса.

Функционирование Kerberos. Здесь рассматривается Kerberos версии 5. Протокол Kerberos функционально прост. Клиент запрашивает у Kerberos мандат (ticket) на обращение к Службе распределения мандатов (Ticket-Granting Service, TGS). Этот мандат пересылается клиенту в зашифрованном секретным ключом клиента виде. Для использования ресурсов конкретного сервера клиент запрашивает у TGS мандат на обращение к серверу. Если все в порядке, TGS отсылает мандат клиенту. После этого клиент предъявляет этот мандат серверу вместе с аутентификатором. И если удостоверение клиента верно, сервер предоставляет клиенту доступ к службе.

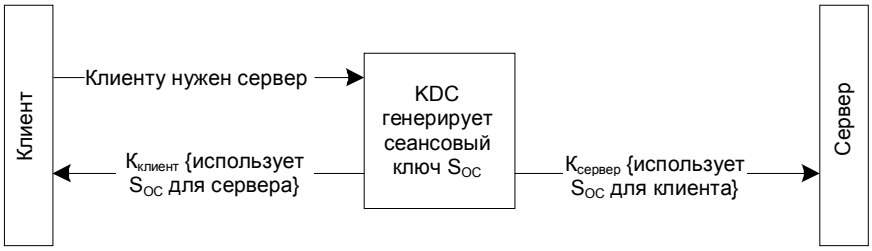

Рис. 2. Управление ключами (в теории)

Удостоверения. Kerberos использует два типа удостоверений (credentials): мандаты (tickets) и аутентификаторы (authenticators). Мандат используется для безопасной передачи серверу информации о личности клиента, которому выдан мандат. В нем также содержатся данные, которые сервер может использовать для подтверждения, что использующий данный мандат клиент, действительно тот, кому изначально был выдан мандат. Аутентификатор – это дополнительное удостоверение, предоставляемое серверу вместе с мандатом.

Использование мандата оптимально для одного сервера и одного клиента. Мандат содержит имя клиента, его сетевой адрес, имя сервера, метку времени и сеансовый ключ. Эта информация шифруется секретным ключом сервера. Если клиент получил мандат, он может использовать его неограниченное количество раз для доступа к серверу, пока не истечет срок действия мандата. Сам клиент не может расшифровать мандат (т.к. он не знает секретного ключа сервера), но он может предоставлять его серверу в зашифрованном виде. Прочитать или изменить мандат при передаче его по сети невозможно.

Клиент создает аутентификатор каждый раз, когда ему нужно получить доступ к сервисам данного сервера. Аутентификатор содержит имя клиента, метку времени и необязательный дополнительный сеансовый ключ. Все эти данные шифруются сеансовым ключом общим для клиента и сервера. В отличие от мандата аутентификатор используется только один раз, т.е. после окончания рабочего сеанса, аутентификатор уничтожается. Но это не проблема, т.к. клиент может создавать аутентификаторы по мере необходимости (ему известен общий секретный ключ).

Получение первоначального мандата. У клиента есть информация, идентифицирующая его личность – его пароль. Как известно пароль нельзя передавать по сети в открытом виде. Протокол Kerberos минимизирует вероятность компрометации пароля, но при этом не дает пользователю правильно идентифицировать себя, если он не знает пароля.

Клиент отсылает сообщение с его именем и именем сервера TGS на сервер аутентификации Kerberos. Сервер аутентификации Kerberos производит поиск данных о клиенте в своей базе данных. Если информация о клиенте найдена, Kerberos генерирует сеансовый ключ, используемый далее для обмена данными между клиентом и сервером TGS. Это действие называется мандатом на выдачу мандата.(Ticket Granting Ticket, TGT). Kerberos шифрует секретным ключом клиента этот сеансовый ключ. Затем он создает для клиента мандат TGT, доказывающий подлинность клиента TGS, и шифрует его секретным ключом TGS. Далее сервер аутентификации посылает клиенту эти два зашифрованных сообщения.

Теперь клиент расшифровывает первое сообщение и получает сеансовый ключ. Секретный ключ является однонаправленной хэш-функцией клиентского пароля, поэтому истинный пользователь без проблем сможет его расшифровать. Самозванец не знает пароля и, следовательно, не сможет расшифровать ответ сервера проверки подлинности. Клиент сохраняет мандат TGT и сеансовый ключ, удаляя пароль и хэш-значение. Эта информация уничтожается, чтобы вероятность компрометации была минимальной. Если злоумышленник попытается скопировать память клиента, он получит только мандат TGT и сеансовый ключ. Это временные данные, и действительны только на время жизни мандата TGT.

Теперь в течение времени жизни мандата TGT клиент может доказывать серверу свою подлинность.

Получение мандатов сервера. Клиенту необходимо получать отдельный мандат для каждой службы сервера. Сервер TGT предоставляет мандаты для отдельных серверов.

Когда клиенту нужен мандат, он посылает запрос TGS. Сервер TGS, получив запрос, расшифровывает мандат TGT своим секретным ключом. Затем служба TGS использует

вложенный в TGT сеансовый ключ, чтобы расшифровать аутентификатор. Наконец TGS сравнивает информацию аутентификатора с информацией в мандате, сетевой адрес клиента с адресом отправителя и метку времени с текущим временем. Если все эти данные совпадают, служба TGS разрешает выполнение запроса.

Проверка меток времени предполагает, что все часы компьютеров синхронизированы с точностью до нескольких минут. Если время в запросе на много отличается от текущего времени, служба TGS считает запрос попыткой повторения предыдущего запроса. Служба TGS должна также отслеживать все действующие аутентификаторы, т.к. повторные запросы могут иметь метки времени, которые еще действительны. Другой запрос с тем же мандатом и меткой времени будет отвергнут.

В ответ на правильный запрос сервер TGS возвращает правильный мандат, который клиент может предъявить серверу. TGS также создает новый сеансовый ключ для клиента и сервера, зашифрованный ключом, общим для клиента и службы TGS. Оба эти сообщения посылаются клиенту. Клиент расшифровывает сообщение и получает сеансовый ключ.

Запрос службы. Теперь клиент может доказать свою подлинность серверу. Он создает сообщение, очень похожее на то, которое посылалось серверу TGS.

Клиент создает аутентификатор, состоящий из его имени, сетевого адреса и метки времени, зашифрованный сеансовым ключом, который был сгенерирован службой TGS для сеанса клиента и сервера. Запрос состоит из мандата, полученного от Kerberos (уже зашифрованного секретным ключом сервера), и зашифрованного аутентификатора.

Сервер расшифровывает и проверяет мандат и аутентификатор, а также проверяет адрес клиента и метку времени. Если все в порядке, то сервер убеждается, что, согласно Kerberos, клиент – именно тот, за кого себя выдает.

Если приложение требует взаимной проверки подлинности, сервер посылает клиенту сообщение, состоящее из метки времени, зашифрованной сеансовым ключом. Это доказывает, клиенту, что серверу известен правильный сеансовый ключ, и он может расшифровать мандат и аутентификатор.

При необходимости клиент и сервер могут шифровать дальнейшие сообщения общим ключом. Так как этот ключ известен только им, они могут быть уверены, что сообщение отправляется противоположной стороной.

Протокол аутентификации Kerberos для Windows

Kerberos и служба каталогов Active Directory

Каждый контроллер домена Windows выступает как в роли агента службы каталогов Active Directory, так и в качестве Kerberos KDC. Благодаря этому вся информация об учетных данных пользователей хранится в одном каталоге. Средние и крупные организации, вероятно, будут использовать несколько контроллеров домена для обеспечения требуемой доступности и производительности. Это не повлияет на возможность использования аутентификации по протоколу Kerberos, так как везде, где есть экземпляр службы каталогов Active Directory, также имеется экземпляр службы аутентификации Kerberos.

Аутентификация в Windows

Windows использует несколько протоколов, которые удостоверяют, что входящий в систему пользователь имеет здесь свою учетную запись. Это протоколы аутентификации удаленных подключений и протоколы аутентификации пользователей, входящих в сеть через Интернет. Среди этих протоков внутри доменов Windows для проверки

пользовательских данных используется протокол Kerberos версии 5. Kerberos 5 является средством аутентификации сетевых пользователей в домене Active Directory на всех компьютерах с операционной системой Windows.

Делегирование аутентификации

Во многих случаях приложения при выполнении задачи обращаются к нескольким серверам. Например, для предоставления данных клиенту на основе обозревателя веб-приложение может использовать как веб-сервер, так и сервер базы данных. В операционной системе Windows клиенту не нужно отдельно проходить аутентификацию для доступа к каждому используемому серверу.
Вместо этого безопасность обеспечивается за счет применения многоуровневых приложений.

Транзитивные доверительные отношения между доменами Windows значительно расширяют набор ресурсов, к которым клиент, работающий под управлением операционной системы Windows или Windows NT Workstation, может получить доступ после входа в домен Windows. Такой вид доступа, называемый единым входом в систему, стал возможен благодаря объединению механизмов доверия Windows и протокола Kerberos со службой каталогов Active Directory.

Операционная система предоставляет единую модель безопасности и инфраструктуру для определения учетных данных пользователей и управления разрешениями на доступ. Это означает, что можно один раз задать настройки в службе каталогов Active Directory, и они будут согласованно использоваться всеми серверами приложений организации. Такой метод, применяемый для поддержки трехуровневой модели, называется *делегированием аутентификации* (*delegation of authentication*).

Такая модель позволяет клиенту делегировать аутентификацию серверам, вовлеченным в работу приложения. Серверы выдают себя за клиента и выполняют запросы на доступ от его имени. Это значит, что все передачи учетных данных и мандатов, необходимых для проверки подлинности, происходят без участия пользователя. Несмотря на то, что сервер выдает себя за клиента, журнал аудита для исходного клиента сохраняется. Когда сервер обрабатывает запрос, переданный другим сервером, в его журнал записывается имя клиента, а не промежуточного сервера.

Эта модель играет важную роль в операционной системе Windows, поскольку благодаря ей поддерживается единый вход в систему и упрощается (но не за счет снижения качества) система безопасности. В настоящее время многие приложения требуют отдельную базу данных учетных записей для обеспечения безопасности. Но приложения, использующие службу каталогов Active Directory в качестве центрального хранилища данных для системы безопасности, позволяют создать сеть, намного более простую в управлении и масштабировании.

Преимущества использования протокола Kerberos

Протокол Kerberos выгодно отличается от других протоколов аутентификации большей гибкостью и эффективностью использования. Также он обеспечивает повышенный уровень безопасности. Перечислим некоторые его преимущества:

• Более эффективная аутентификация на серверах. У Kerberos при аутентификации необходимость в подключении серверу приложений к контроллеру домена для проверки каждого клиента (как у NTLM) отпадает – здесь аутентификация производится за счет проверки удостоверения, представленного клиентом. Индивидуальное удостоверение

клиент получает от контроллера один раз, после этого может неоднократно использовать его на протяжении всего сеанса работы в сети.

- Взаимная аутентификация. Протокол NTLM позволяет серверу идентифицировать своих клиентов, однако не предусматривает верификации сервера ни клиентами, ни другими серверами. В отличие от него, Kerberos такого допущения не делает, поэтому проверяет обоих участников сетевого подключения, каждый из которых в результате может точно узнать, с кем поддерживает связь.
- Делегированная аутентификация. Когда клиент сети Windows обращается к ресурсам, службы операционной системы, прежде всего, производят его идентификацию. Во многих случаях для выполнения этой операции службе достаточно информации на локальном компьютере. Как NTLM, так и Kerberos обеспечивают все данные, необходимые для идентификации пользователя на месте, однако иногда их бывает недостаточно. Некоторые распределенные приложения требуют, чтобы при подключении к серверным службам на других компьютерах идентификация клиента производилась локально службой самого этого клиента. Решить проблему помогает Kerberos, где предусмотрен специальный механизм представительских мандатов, который позволяет на месте идентифицировать клиента при его подключении к другим системам. В протоколе NTLM такая возможность отсутствует.
- Упрощенное управление доверительными отношениями. Одно из важных достоинств взаимной аутентификации по протоколу Kerberos состоит в том, что доверительные отношения между доменами Windows по умолчанию являются двусторонними и транзитивными. Благодаря этому в сетях с множеством доменов не придется устанавливать много явных доверительных отношений. Вместо этого все домены большой сети можно свести в дерево транзитивных отношений взаимного доверия. Удостоверение, выданное системой безопасности для любого домена, может приниматься во всех ветвях дерева. Если же сеть содержит несколько деревьев, то удостоверение любого из них будет приниматься по всему «лесу».

Компоненты протокола Kerberos в Windows

В операционной системе Windows Центр распределения ключей (Key Distribution Center, KDC) реализован как служба домена. В качестве базы данных учетных записей он использует Active Directory.

В протоколе Kerberos, центр KDC Windows представляет собой единый процесс, объединяющий две службы:

- Служба аутентификации Authentication Service (AS). Эта служба выдает мандаты на выдачу мандатов (мандаты TGT). Прежде, чем получить мандат, клиент должен запросить первоначальный мандат TGT, обратившись для этого к службе аутентификации того домена, где находится учетная запись пользователя.
- Служба выдачи мандатов Ticket-Granting Service (TGS). Эта служба выдает мандаты на доступ к другим службам своего домена или к службе выдачи мандатов доверяемого домена. Чтобы обратиться в службу TGS, клиенту нужно сначала войти в контакт со службой выдачи мандатов того домена, где находится учетная запись службы, представить свой мандат TGT и запросить нужный мандат. Если у клиента нет мандата TGT, который открывает доступ к данной службе выдачи мандатов, он может воспользоваться процессом переадресации (referral process). Начальной точкой этого процесса является служба того домена, где находится учетная запись пользователя, а конечной – служба выдачи мандатов домена, где находится учетная запись требуемой службы.

Центр KDC, как и служба каталогов Active Directory, имеется в каждом домене. Обе службы автоматически запускаются подсистемой LSA (Local Security Authority –

распорядитель локальной безопасности), которая установлена на контроллере домена. Ни одну из этих служб остановить невозможно.

В доменах Windows служба KDC является абонентом безопасности. Учетная запись абонента безопасности для нее создается автоматически при организации нового домена; эту запись нельзя ни изменить, ни переименовать. Пароль учетной записи KDC также присваивается автоматически, а затем регулярно меняется вместе с паролями доверенных учетных записей домена (domain trust account). Пароль учетной записи KDC используется при вычислении секретного ключа, необходимого для шифрования и расшифрования генерируемых этой службой мандатов TGT. Пароль же доверенной учетной записи домена необходим для расчета междоменных (межобластных) ключей, которые используются для шифрования мандатов переадресации.

База данных учетных записей

База данных, которая необходима службе KDC для получения информации относительно абонентов безопасности, хранится в каталоге Active Directory. Каждый абонент здесь представлен в виде учетной записи. Криптографические ключи, применяемые для связи с пользователем, компьютером или службой, хранятся в виде атрибутов объекта учетной записи конкретного абонента безопасности.

Серверами службы каталога Active Directory являются только контроллеры доменов. На каждом из них хранится копия каталога, в которую можно вносить изменения. Это позволяет создавать новые учетные записи, изменять пароли и корректировать состав групп, обратившись на любой контроллер домена. Изменения, внесенные в одну реплику каталога, автоматически переносятся на все другие его реплики. Правда, Windows не использует для этой цели протокол репликации Kerberos. Копирование и распространение информации, хранящейся в Active Directory, производится посредством собственного протокола децентрализованной репликации (multi-master replication protocol), разработанного корпорацией Microsoft , причем пересылка ее осуществляется по защищенным каналам между контроллерами доменов.

Запросы на доступ к объектам или атрибутам каталога подлежат проверке в системе управления доступом Windows. Подобно объектам файлов и папок в файловой системе NTFS, объекты Active Directory защищаются посредством ACL (Access Control List – список контроля доступа), где содержится информация о том, кто и каким способом имеет право обращаться к объектам. Правда, в объектах Active Directory, в отличие от файлов и папок, список контроля доступа имеется для каждого атрибута. Самым секретным элементом любой учетной записи, конечно же, является пароль. В объекте учетной записи атрибут пароля хранит не сам пароль, а криптографический ключ, полученный на его основе, однако этот ключ представляет для взломщика не меньшую ценность. По этой причине доступ к атрибуту пароля предоставляется исключительно владельцу учетной записи. Такого права не имеет никто другой, даже администратор.

В Windows приняты меры и против возможного взлома учетной записи изнутри, то есть, злоумышленником с доступом к резервным копиям доменного контроллера. Чтобы помешать этому, атрибут пароля в объекте учетной записи подвергается второму шифрованию с использованием *системного ключа*. Этот криптографический ключ может храниться на сменном носителе, для которого нетрудно предусмотреть дополнительные меры защиты.

Политика Kerberos

В среде Windows политика Kerberos определяется на уровне домена и реализуется службой KDC домена. Она сохраняется в каталоге Active Directory как подмножество

атрибутов политики безопасности домена. По умолчанию вносить изменения в политику Kerberos имеют право только члены группы администраторов домена.

В политике Kerberos предусматриваются:

• Максимальный срок действия пользовательского мандата (Maximum user ticket lifetime). Под «пользовательским мандатом» здесь имеется в виду мандат на выдачу мандатов (мандат TGT). Значение задается в часах и по умолчанию равно 10 час.

• Максимальное время, в течение которого допускается обновление пользовательского мандата (Maximum lifetime that a user ticket can be renewed). Задается в сутках; по умолчанию составляет 7 суток.

• Максимальный срок действия служебного мандата (Maximum service ticket lifetime). Под «служебным мандатом» здесь имеется в виду сеансовый мандат. Значение этого параметра должно быть более 10 минут, но менее значения *Maximum user ticket lifetime*. По умолчанию оно равно 10 час.

• Максимально допустимое отклонение в синхронизации компьютерных часов (Maximum tolerance for synchronization of computer clocks). Указывается в минутах; по умолчанию равно 5 мин.

• Проверка ограничений при входе пользователя в систему (Enforce user logon restrictions). Если этот пункт помечен флажком, служба KDC анализирует каждый запрос на сеансовый мандат и проверяет, имеет ли данный пользователь право на локальный вход в систему (привилегия *Log on Locally*) или на доступ к запрашиваемому компьютеру через сеть (привилегия *Access this computer from network*). Такая проверка занимает дополнительное время и может замедлить предоставление сетевых услуг, поэтому администратору предоставляется право ее отключения. По умолчанию она включена.

О совместимости Microsoft Kerberos с MIT Kerberos.

С выпуском Windows 2000 компания Microsoft начала использование протокола Kerberos V5 как основного протокола аутентификации. Многие восхваляли принятие протокола Kerberos компанией Microsoft, т.к. этот протокол зарекомендовал себя как надежный и эффективный алгоритм аутентификации на других платформах. Также принятие протокола Kerberos вселило надежды, что архитектура аутентификации Windows все-таки будет взаимодействовать с другими операционными системами, позволяя системным администраторам более простое обслуживание учетных записей, которыми ранее приходилось управлять по отдельности.

Стандарты шифрования. Microsoft официально поддерживает 128 bit RC4-HMAC как основной стандарт шифрования для мандатов Kerberos. Но также имеется поддержка таких стандартов, как DES-CBC-CRC и DES-CBC-MD5, чтобы иметь возможность взаимодействовать с MIT Kerberos.

Стандарты шифрования	Аутентификация (длина ключа в битах)	Подпись (длина ключа в битах)	Конфиденциальность (длина ключа в битах)
DES-CBC-CRC	56	56	56
DES-CBC-CRC	56	56	56
RC4-HMAC	128	128	56 (возможно 128)

Типы мандатов. Microsoft не поддерживает использование мандатов, датированных передним числом (post-dated), и, так называемых, proxy tickets (по доверенности). Зато

Microsoft предоставляет использование безадресных мандатов TGT, что для многих сред более удобно, но может иметь некоторую степень риска.

Имена пользователей. Существует одна несовместимость, которая сильно отличается от стандарта RFC 1510. В Microsoft нет различия в способе написания (использование заглавных или прописных букв) названий имен пользователей. Все возможные алфавитные регистры при написании имен пользователей (например, username@realm или USERNAME@realm) эквивалентны Microsoft Active Directory, и все они могут отображаться в одну учетную запись.

Некоторые сценарии взаимодействия.

1) Microsoft Active Directory может доверять MIT Kerberos KDC (ЦРК). Для того, чтобы установить доверительные отношения, адрес MIT Kerberos KDC и его область (realm) должны быть зарегистрированы в контроллере домена.
2) Для того, чтобы рабочая станция с операционной системой Windows могла получить доступ к сервисам MIT Kerberos в какой-то области, каждая рабочая стация должна знать расположение ЦРК для этой области.
3) Для того, чтобы пользователь MIT Kerberos мог получить доступ к ресурсам сети Microsoft, должны существовать доверительные отношения между пользователем MIT Kerberos KDC и Microsoft Active Directory, а также возможность отображения имени пользователя MIT Kerberos в учетной запись пользователя в Active Directory. Это отображение необходимо, чтобы Microsoft могла добавить необходимую информацию в пользовательский мандат для использования в сети Windows 2000.
4) Если пользователь Windows 2000 захочет аутентифицировать себя для сервиса MIT Kerberos, этот сервис должен быть зарегистрирован в Active Directory.

Список используемой литературы:

1) “KERBEROS”, Брюс Шнайер, “Прикладная криптография”, 2002.
2) http://www.giac.org/practical/GSEC/Christopher_Nebergall_GSEC.pdf.
3) Jennifer G. Steiner “Kerberos: An Authentication Service for Open Network Systems”,march30, 1988.
