Протокол Kerberos

Саргсян Арам Грачьяевич

Содержание

1 Введение **5**

2 История создания **6**

3 Основные особенности **8**
3.1 Kerberos 4 8
3.2 Kerberos 5 9

4 Поддержка разных ОС **11**

5 Недостатки **13**

Список литературы **15**

Список иллюстраций

Список таблиц

1 Введение

В современном мире использование корпоративных сетей для осуществления деятельности предприятий имеет огромное значение. Решение проблемы администрирования доступа пользователей к сетевым ресурсам является актуальной задачей, в рамках которой необходимо использовать различные сетевые протоколы для достижения соответствующих целей. Kerberos — это сетевой протокол централизованной аутентификации клиентов компьютерных сетей на основе архитектуры клиент-сервер [1]

2 История создания

Массачусетский технологический институт (MIT) разработал протокол Kerberos в 1988 году для защиты сетевых служб, предоставляемых проектом Athena. Его первую версию в основном разработали Стив Миллер и Клиффорд Нейман на основе ранее использованного симметричного протокола Нидхэма-Шрёдера. Версии Kerberos с 1 по 3 были экспериментальными и не распространялись за пределами MIT.

Kerberos версии 4, первая общедоступная версия, была выпущена 24 января 1989 года. Поскольку Kerberos 4 был разработан в Соединенных Штатах и использовал алгоритм шифрования Data Encryption Standard (DES), ограничения на экспорт, связанные с США, мешали его распространению в другие страны. MIT создал экспортируемую версию Kerberos 4, из которой был удален весь код шифрования, названную “Bones”. Эрик Янг из австралийского университета Бонда внедрил DES в “Bones” и создал версию под названием “eBones”, которую можно было свободно использовать в любой стране. Королевский институт технологии Швеции выпустил еще одну версию под названием KTH-KRB.

Нейман и Джон Коуль опубликовали версию 5 в 1993 году с целью преодоления существующих ограничений и проблем безопасности. Версия 5 была опубликована как RFC 1510 и затем была признана устаревшей в RFC 4120 в 2005 году [2].

В 2005 году рабочая группа Kerberos Internet Engineering Task Force (IETF) обновила спецификации. Обновления включали:

- Спецификации шифрования и контрольных сумм (RFC 3961).

- Шифрование по стандарту Advanced Encryption Standard (AES) для Kerberos 5 (RFC 3962).
- Новую версию спецификации Kerberos V5 “Службы сетевой аутентификации Kerberos (V5)” (RFC 4120). Эта версия устраняла недоразумения в протоколе и предоставляла более детальное и ясное объяснение предполагаемого использования.
- Новую версию спецификации Generic Security Services Application Program Interface (GSS-API) “Механизм общей службы аутентификации Kerberos Version 5 (GSS-API): Версия 2” (RFC 4121).

MIT предоставляет реализацию Kerberos бесплатно, с разрешениями, аналогичными тем, которые используются для BSD. В 2007 году MIT создал Консорциум Kerberos для поддержки дальнейшего развития. Среди учредителей Консорциума были такие компании-спонсоры, как Oracle, Apple Inc., Google, Microsoft, Centrify Corporation и TeamF1 Inc., а также академические учреждения, такие как Королевский институт технологии Швеции, Стэнфордский университет, MIT, и компании, такие как CyberSafe, предлагающие коммерчески поддерживаемые версии.

3 Основные особенности

3.1 Kerberos 4

Kerberos 4 имел два существенних изменения по сравнению с протоколом Нидхема-Шрёдера.

1. Уменьшало количество сообщений, пересылаемых между клиентом и сервером аутентификации.
2. Введении TGT (англ. ticket granting ticket — мандат для получения мандата) концепции, позволяющей пользователям аутентифицироваться в нескольких сервисах, используя свои доверительные данные только один раз.

Как результат, протокол Kerberos 4 содержит два логических компонента: сервер аутентификации и сервер выдачи мандатов или разрешений.

Принцип работы:

1. Аутентификация по паролю: Пользователь вводит свой логин и пароль на клиентском компьютере. Клиент отправляет запрос на аутентификацию Key Distribution Center (KDC).

2. KDC: KDC - это центр распределения ключей, который состоит из двух частей: Authentication Server (AS) и Ticket Granting Server (TGS). AS проверяет логин и пароль пользователя и, если они верны, создает временный ключ (TGT - Ticket Granting Ticket).

3. TGT: TGT - это зашифрованный билет, который выдается пользователю. Он используется для получения билетов TGS для доступа к другим ресурсам.

4. Запрос TGS: Пользователь отправляет TGT на TGS и запрос на доступ к конкретному ресурсу.

5. Билет TGS: TGS проверяет TGT и создает билет TGS, который предоставляет доступ к запрошенному ресурсу.

6. Доступ к ресурсу: Пользователь отправляет билет TGS на сервер ресурса. Сервер ресурса проверяет билет TGS и, если он действителен, предоставляет доступ к ресурсу.

3.2 Kerberos 5

Kerberos 5 является усовершенствованной версией протокола. Общий принцип работы Kerberos 5 схож с Kerberos 4, но он предоставляет более широкие возможности аутентификации и дополнительные меры безопасности, что делает его более современным и безопасным протоколом для обеспечения безопасности сетевых ресурсов.

Отличия от Kerberos 4:

1. Поддержка различных методов аутентификации: Kerberos 5 позволяет использовать не только пароли, но и другие методы аутентификации, такие как общие секреты или смарт-карты.

2. Поддержка цифровых сертификатов: Kerberos 5 позволяет использовать цифровые сертификаты для аутентификации.

3. Поддержка прокси-серверов: Клиенты могут использовать прокси-серверы для аутентификации и получения билетов.

4. Улучшенная защита от атак: Kerberos 5 включает дополнительные меры безопасности, такие как защита от атак на отказ в обслуживании и защита от атак с перебором паролей.

5. Сжатие и шифрование сообщений: Kerberos 5 поддерживает сжатие и шифрование сообщений между клиентом, KDC и серверами ресурсов.

4 Поддержка разных ОС

Windows 2000 и более поздние версии используют Kerberos в качестве метода аутентификации по умолчанию. Некоторые дополнения Microsoft к набору протоколов Kerberos описаны в RFC 3244 “Протоколы изменения пароля и установки пароля Kerberos для Microsoft Windows 2000”. RFC 4757 документирует использование Microsoft шифра RC4. Несмотря на то, что Microsoft использует и расширяет протокол Kerberos, она не использует программное обеспечение MIT.

Kerberos используется в качестве предпочтительного метода аутентификации: в общем случае, присоединение клиента к домену Windows означает включение Kerberos в качестве протокола аутентификации по умолчанию для запросов от этого клиента к службам в домене Windows и всех доменах с доверительными отношениями к этому домену.

В отличие от этого, когда клиент, сервер или оба не присоединены к домену (или не являются частью той же доверительной среды домена), Windows вместо этого использует NTLM для аутентификации между клиентом и сервером.

Интернет-веб-приложения могут настраивать использование Kerberos в качестве метода аутентификации для клиентов, присоединенных к домену, с использованием API, предоставляемых в рамках SSPI.

Microsoft Windows и Windows Server включают setspn, утилиту командной строки, которую можно использовать для чтения, модификации или удаления учетных имен службы (SPN) для учетной записи службы Active Directory.

Многие операционные системы, подобные Unix, включая FreeBSD, OpenBSD, macOS от Apple, Red Hat Enterprise Linux, Solaris от Oracle, AIX от IBM, HP-UX и

другие, предоставляют программное обеспечение для аутентификации пользователей или служб с использованием Kerberos. Поддержка Kerberos также доступна на различных операционных системах, не похожих на Unix, таких как z/OS, IBM i и OpenVMS. Компании также предоставляют встраиваемую реализацию протокола аутентификации Kerberos V для клиентских агентов и сетевых служб, работающих на встраиваемых платформах[3]

5 Недостатки

Данный протокол имеет также некоторые недостатки:

- Единая точка отказа: требуется постоянное наличие центрального сервера. Когда сервер Kerberos падает, новые пользователи не могут войти. Это может быть устранено с помощью нескольких серверов Kerberos и резервных механизмов аутентификации.
- Kerberos имеет строгие требования к времени, что означает, что часы участников должны быть синхронизированы в заданных пределах. Мандаты имеют время жизни и, если часы клиента не синхронизированы с часами сервера Kerberos, аутентификация не будет выполнена. Конфигурация по умолчанию требует, чтобы часы расходились не более чем на пять минут друг от друга. На практике, как правило, используются демоны Network Time Protocol для синхронизации часов у клиентов.
- Протокол администрирования не стандартизирован и зависит от конкретной реализации сервера. Смена пароля описана в RFC 3244.
- В случае использования симметричной криптографии (Kerberos может работать с использованием как симметричной, так и асимметричной (с открытым ключом) криптографии), так как все способы аутентификации управляются централизованно центром распределения ключей (KDC), эта особенность инфраструктуры аутентификации позволит злоумышленнику выдавать себя за пользователя.
- Каждый сетевой сервис, требующий смены имени хоста, должен будет обновить собственный набор ключей Kerberos. Это усложняет использование

виртуального хостинга и кластеров.

- Kerberos требует, чтобы учетные записи пользователей, клиенты и пользователи услуг на сервере, все доверяли серверу Kerberos (все должны быть в одном и том же домене с Kerberos или в доменах, имеющих доверительные отношения друг с другом). Kerberos не может использоваться в случаях, когда пользователи хотят подключаться к службам от неизвестных / ненадежных клиентов, как в обычном интернете.

Список литературы

1. Fan K., Li H., Wang Y. Security Analysis of the Kerberos Protocol Using BAN Logic // 2009 Fifth International Conference on Information Assurance and Security. IEEE, 2009.
2. Kohl J., Neuman C. The Kerberos Network Authentication Service (V5). RFC Editor, 1993.
3. Vilhuber J. и др. Kerberized Internet Negotiation of Keys (KINK): 4430. RFC 4430; RFC Editor, 2006. 40 с.