УДК 004

Е.С. Калинина, А.В. Чернышова
Донецкий национальный технический университет
Кафедра прикладной математики и информатики
E-mail: lena00777@gmail.com, alla@pmi.dgtu.donetsk.ua

АНАЛИЗ ПРОТОКОЛА БЕЗОПАСНОСТИ KERBEROS

Аннотация

Калинина Е.С., Чернышова А.В., Анализ протокола безопасности Kerberos. *В тексте данной статьи описан принцип работы протокола Kerberos и возможность его использования в корпоративных системах и сетях. Служба Kerberos, работающая в сети, действует как доверенный посредник, обеспечивая безопасную сетевую проверку подлинности, которая позволяет пользователю работать на нескольких машинах. При общении с каждым объектом сети Kerberos использует сгенерированный общий секретный ключ. На сегодняшний день протокол Kerberos самый безопасный механизм аутентификации, поддерживаемый AD.*

Актуальность

На сегодняшний день универсальные системы аутентификации получили широкое распространение в информационно-вычислительных сетях. Причиной этому послужил активный рост требований к защищённости информационно-телекоммуникационных систем. В течение длительного времени основными проблемами были организация масштабируемости системы аутентификации и организация кроссистемного взаимодействия. Однако сейчас существует достаточное количество протоколов, которые решают подобного рода задачи.

Протокол Kerberos был специально разработан для того, чтобы обеспечить надежную аутентификацию пользователей, и

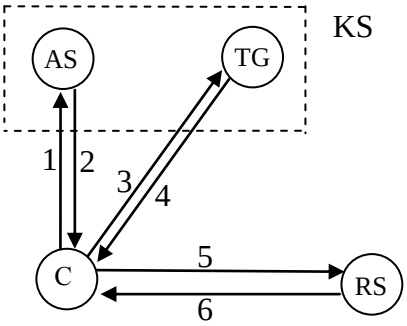
был создан более десяти лет назад в Массачусетском технологическом институте в рамках проекта «Афина». Kerberos – единственный протокол аутентификации Windows, который обеспечивает ограниченное делегирование. [1]

Основная концепция протокола Kerberos

Основу Kerberos составляет протокол аутентификации и распределения ключей Нидхэма-Шредера с третьей доверенной стороной. В протоколе Kerberos участвуют две взаимодействующие стороны и доверенный сервер, который выполняет роль центра распределения ключей. Этот протокол успешно работает при условии, что часы каждого участника синхронизированы с часами сервера. Система Kerberos имеет структуру типа клиент-сервер и состоит из клиентских частей и сервера Kerberos. Клиентами могут быть пользователи, а также различного рода независимые программы, выполняющие такие действия, как загрузка удаленных файлов, отправка сообщений, доступ к БД, доступ к принтерам, получение привилегий у администратора и т.п. Сервер Kerberos KS делится на две части: сервер аутентификации AS (Authentication Server) и сервер службы выдачи мандатов TGS (Ticket Granting Service), которые физически могут быть совмещены. Информационными ресурсами управляет сервер RS. Секретные службы, которые требуют проверку подлинности, и клиенты, которые хотят использовать эти службы, регистрируют в Kerberos свои секретные ключи. Kerberos хранит БД о клиентах и их секретных ключах, наличие которых позволяет создавать зашифрованные сообщения, которые направляются клиенту или серверу. Успешное расшифрование этих сообщений является гарантией прохождения аутентификации всеми участниками протокола. Также Kerberos создаёт сеансовые ключи (session key), которые выдаются клиенту и серверу. Этот ключ используется для шифрования сообщений и уничтожается после окончания сеанса. [2]

Работа системы Kerberos

Процесс идентификации и аутентификации пользователя в системе Kerberos 5 можно описать следующим образом (рис.1) [2]:



Обозначения:
KS – сервер системы Kerberos
AS – сервер аутентификации
TGS – сервер службы выделения мандатов
RS – сервер информационных ресурсов

Рис.1. Процесс идентификации и аутентификации пользователя в системе Kerberos 5.

Основные шаги работы Kerberos:

1. Клиент вводит имя пользователя, пароль и домен для получения доступа к ресурсу сети и отправляет запрос серверу аутентификации (AS). Причём, имя клиента передаётся в открытом виде, а текущее время на рабочей станции клиента передаётся в зашифрованном виде и является аутентификатором.

2. Сервер AS проверяет, есть ли такой клиент, выявляет мастер ключ клиента, который основан на пароле и расшифровывает аутентификатор (получает время отправки запроса). Разница текущего времени и времени отправки запроса от клиента не должно превышать определённого значения, которое указано в политике протокола Kerberos. После этого, Сервер AS высылает клиенту билет на получение билета (TGT), формирует ключ сессии (обеспечивает шифрование данных при обмене между AS и клиентом), идентификатор на доступ к

серверу службы выделения мандатов TGS (Ticket-Granting Service) и время жизни билета.

3. Клиент получает данные от сервера AS, расшифровывает свою часть для получения сессионного ключа Клиент/TGS и отправляет запрос TGS мандат на обращение к серверу AS. Запрос содержит полученный ранее TGT, идентификатор сервиса и аутентификатор, зашифрованный на сессионном ключе Клиент/TGS.

4. TGS получает и извлекает TGT, расшифровывает его с использованием секретного ключа TGS. В результате TGS получает сессионный ключ Клиент/TGS, которым расшифровывает аутентификатор. После этого он генерирует сессионный ключ клиент/сервис и посылает ответ клиенту. Ответ содержит:

- билет сервиса, который содержит ID клиента, его сетевой адрес, время действия билета и сессионный ключ клиент/сервис, зашифрованные секретным ключом сервиса.
- идентификатор сервиса, сессионный ключ клиент/сервис и время жизни билета, зашифрованные на сессионном ключе клиент/TGS.[3]

5. Клиент получает ответ и соединяется с сервером RS, посылая ему зашифрованный ранее билет сервиса, новый аутентификатор, зашифрованный на сессионном ключе клиент/сервис, включающий метку времени и ID клиента.

6. Сервер RS получает данные от клиента, расшифровывает билет, используя свой секретный ключ, и получает сессионный ключ клиент/сервис. Этим новым ключом он расшифровывает аутентификатор и посылает сообщение о готовности обслужить клиента. Метка времени, указанная клиентом, обновляется (метка + 1) и высылается клиенту. Клиент проверяет корректность обновления метки, и если всё верно, то клиент начинает посылать запросы на сервер. [4]

Приведенная модель может полноценно функционировать в том случае, если обеспечена полная целостность и конфиденциальность передаваемой информации. Без строгого обеспечения информационной безопасности клиент С не может

отправлять серверам AS, TGS и RS свои запросы и получать доступ к обслуживанию сети.

Использование протокола Kerberos в корпоративных системах и сетях

В настоящее время множество ОС поддерживают данный протокол, в число которых входят:

- ОС семейства Windows, которые используют Kerberos как метод аутентификации в домене между участниками.
- UNIX и UNIX подобные ОС (Apple Mac OS X, Red Hat Enterprise Linux 4, FreeBSD, Solaris, AIX, OpenVMS). [4]

Системы аутентификации, которые базируются или реализуются на основе протокола Kerberos, являются распространёнными, но большая часть из них – дорогие закрытые программные продукты. Наиболее важные реализации протокола:

- KTH Kerberos;
- Heimdal Kerberos;
- MIT Kerberos;
- GNU Shishi;
- Microsoft Kerberos;
- Реализация в составе Apple Mac OS X;
- Реализация в составе Red Hat Linux 4;
- Solaris Kerberos Service;
- FreeBSD.
-

Достоинства и недостатки работы протокола

В реализации протокола Kerberos существуют потенциально уязвимые места:

- возможно кеширование и повторное использование старых удостоверений. Хотя метки должны предотвратить такую возможность, удостоверения могут использоваться повторно в течение времени жизни мандата. Использование удостоверений основано на том, что все часы сети синхронизированы. В случае

если время компьютера будет установлено неправильно, то старое удостоверение может снова быть использовано. Большинство сетевых протоколов поддержки единого времени небезопасны, поэтому такая возможность несёт в себе серьёзную опасность;

- чувствительность к вскрытиям с угадыванием пароля. Злоумышленник может записать мандаты, а затем попытаться их расшифровать. В большинстве случаев пользователь редко выбирает хороший пароль, поэтому, если у злоумышленника будет достаточное количество мандатов, у него появятся все шансы на то, чтобы раскрыть пароль. [5]

К достоинствам протокола можно отнести:

- эффективный доступ к ресурсам и проверка подлинности, которые заключаются в том, что не требуется постоянный переход от сервера с ресурсами к контроллеру домена. Клиент получает «билет», который использует на протяжении всего сеанса или до истечения его срока, для получения доступа к ресурсам; [5]

- эффективное взаимодействие с доменами в лесу. Так как протокол Kerberos основан на спецификациях отслеживания, то все доверительные связи конфигурируются автоматически и являются двухсторонними и поддерживаются между всеми доменами данного леса;

− пользователь вводит пароль один раз за сессию, что позволяет ему иметь доступ ко всем сервисам без повторного ввода пароля. Данное свойство называется Single Sign-On;

− высокий уровень безопасности. При любых взаимодействиях не осуществляется передача паролей, значений хеша паролей в открытом виде.

Выводы

Таким образом, протокол проверки подлинности Kerberos отличается гибкостью и эффективностью использования, а также гарантирует повышенный уровень безопасности. С активным

развитием интернета, электронной коммерции и виртуальных частных сетей, этот протокол является одним из тех, которые удовлетворяют всем необходимым требованиям безопасности на сегодняшний день. Также протокол может использоваться в сочетании с различными криптографическими схемами. В настоящее время ведутся работы над улучшением протокола Kerberos, включая модернизацию управления ключами с помощью криптографии с открытыми ключами и интерфейса интеллектуальных карточек.

Список литературы

1. Технология Kerberos для обеспечения безопасности MOSS 2007 [электронный ресурс]. – Режим доступа: http://www.osp.ru/win2000/2008/05/5528562/

2. Протокол Kerberos [электронный ресурс]. – Режим доступа: http://ypn.ru/427/kerberos-protocol/

3. Kerberos [электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Kerberos

4. Принципы аутентификации по протоколу Kerberos [электронный ресурс]. – Режим доступа: http://itband.ru/2010/12/kerberos1/

5. Брюс шнайер. Прикладная криптография 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С. – 1994 – 816 с.