4. Идентификация и аутентификция пользователей

Реализуйте систему аутентификации на основе протокола Kerberos. Предусмотрите функцию отображения всех сообщений, передаваемых между субъектами взаимодействия. Результатом успешной аутентификации является наличие общего сеансового ключа, сгенерированного сервером выдачи мандатов, у клиента и сервера ресурсов. Взаимодействие узлов системы должно осуществляться по сети.

Kerberos

Протокол Kerberos использует дополнительную аутентификацию на доверенном посреднике (рис. 1). Роль посредника здесь играет так называемый ***центр распределения ключей KDC*** (Key Distribution Center).

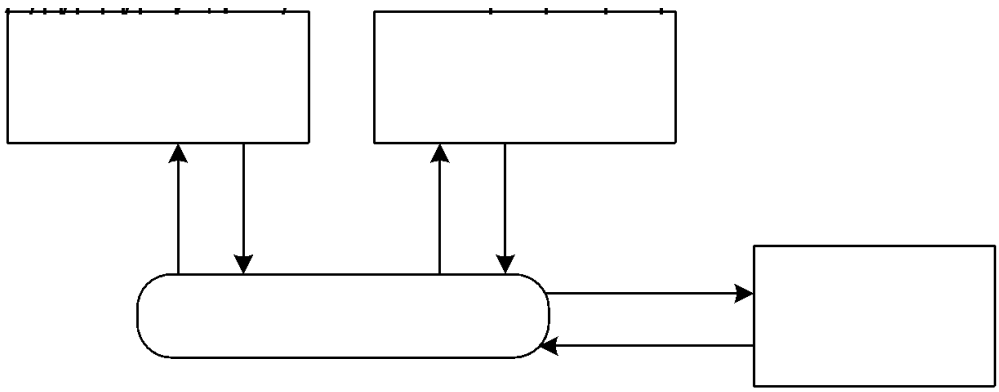

Рисунок 1 – Схема аутентификации Kerberos.

KDC представляет собой службу, работающую на физически защищенном сервере. Она ведет базу данных с информацией об учетных записях всех своих абонентов безопасности. Вместе с информацией о каждом из них в базе данных KDC сохраняется криптографический ключ, известный только этому абоненту и службе KDC. Данный ключ, который называют ***долговременным***, используется для связи пользователя системы безопасности с центром распределения ключей. В большинстве практических реализаций протокола Kerberos долговременные ключи создаются на основе пароля пользователя.

Путь клиента к ресурсу в системе Kerberos состоит из трех этапов:

1. Определение легальности клиента, осуществляющего вход в

систему (сообщения 1 и 2 на рис. 1).

2. Получение разрешения на обращение к ресурсному серверу (сообщения 3 и 4).

3. Получение доступа к ресурсу (сообщения 5 и 6).

Для решения первой и второй задач клиент обращается к серверу KDC, который соответственно делится на две вспомогательные службы. Выполнение первичной аутентификации осуществляется так называемым ***аутентификационным сервером AS*** (Authentication Server). Этот сервер хранит в своей базе данных информацию об идентификаторах и паролях пользователей. Вторую задачу, связанную с получением разрешения на обращение к ресурсному серверу, решает ***сервер мандатов TGS*** (Ticket-Granting Server). Сервер TGS для легальных клиентов выполняет дополнительную проверку и дает клиенту разрешение на доступ к нужному ему ресурсному серверу, для чего наделяет его электронной формой-мандатом. Для выполнения своих функций сервер мандатов использует копии секретных ключей всех ресурсных серверов, которые хранятся у него в базе данных. Кроме этих ключей, сервер TGS имеет еще один секретный ключ, который разделяется с сервером AS.

Протокол Kerberos описывается следующими сообщениями:

1. Клиент-AS: C, TGS.
2. AS-клиент: $\{K_{C,TGS}\}K_C$, $\{T_{C,TGS}\}K_{TGS}$.
3. Клиент-TGS: S, $\{A_{C,TGS}\}K_{C,TGS}$, $\{T_{C,TGS}\}K_{TGS}$.
4. TGS-клиент: $\{K_{C,S}\}K_{C,TGS}$, $\{T_{C,S}\}K_S$.
5. Клиент-сервер: $\{A_{C,S}\}K_{C,S}$, $\{T_{C,S}\}K_S$.
6. Сервер-клиент: $\{t+1\}K_{C,S}$.

Здесь C обозначает клиента, S – сервер, K_x – секретный ключ x, $K_{x,y}$ – сеансовый ключ для x и y, $\{m\}K_x$ – сообщение m, шифрованное секретным ключом x, $T_{x,y}$ – мандат (билет) x на использование y, $A_{x,y}$ – удостоверение (аутентификатор) x для y, t – метка времени, входящая в состав удостоверения.

Мандат используется для безопасной передачи серверу личности клиента, которому выдан этот мандат. Мандат Kerberos имеет следующую форму:

$$T_{C,S} = S, \{C, a, v, K_{C,S}\}K_S.$$

Мандат пригоден для одного сервера и одного клиента. Он содержит имя клиента C, его сетевой адрес a, имя сервера S, срок действия v и сеансовый ключ $K_{C,S}$. Эта информация шифруется секретным ключом сервера K_S. Если клиент получил мандат, он может использовать его для доступа к серверу много раз – пока не истечет срок действия мандата. Клиент не может расшифровать мандат (он не знает секретного ключа сервера), но он может предъявить его серверу в зашифрованной форме. Прочитать или изменить

мандат при передаче его по сети невозможно.

Удостоверение – это дополнительный атрибут, предъявляемый вместе с мандатом, который преследует две цели. Во-первых, удостоверение содержит некоторый открытый текст, зашифрованный сеансовым ключом. Это доказывает, что клиенту известен ключ. Кроме того, зашифрованный открытый текст включает метку времени. Злоумышленник, которому удалось записать и мандат, и удостоверение, не сможет использовать их спустя два дня. Удостоверение Kerberos имеет следующую форму:

$A_{C,S} = \{C, t, ключ\}K_{C,S}$.

Клиент создает его каждый раз, когда ему нужно воспользоваться услугами сервера. Удостоверение содержит имя клиента C, метку времени t и необязательный дополнительный сеансовый ключ. Все эти данные шифруются сеансовым ключом $K_{C,S}$, общим для клиента и сервера. В отличие от мандата, удостоверение используется только один раз. Однако это не проблема, так как клиент может генерировать удостоверения по мере надобности (ему известен общий секретный ключ).

Этапы аутентификации по протоколу Kerberos:

1. Получение первоначального мандата. У клиента есть часть информации, доказывающей его личность, – его пароль. Однако он не пересылается по сети. Клиент посылает в адрес сервера аутентификации сообщение 1, содержащее только его имя и имя его сервера TGS. В случае обнаружения данных о пользователе в базе данных сервер AS генерирует сеансовый ключ, который будет использоваться для обмена данными между клиентом и TGS, и шифрует этот сеансовый ключ секретным ключом клиента. Затем он создает мандат для доступа клиента к серверу TGS (***мандат на выделение мандата*** TGT, Ticket Granting Ticket) и шифрует его секретным ключом TGS. В сообщение 2 включаются зашифрованный сеансовый ключ и мандат. Легитимный клиент может расшифровывать только первую часть сообщения. Злоумышленник не может расшифровать ни одну часть сообщения 2.

2. Получение серверных мандатов. Мандаты для получения доступа к конкретным серверам выдает центр распределения мандатов TGS при поступлении запросов от клиентов с корректными TGT и удостоверениями (сообщение 3). Сервер TGS, получив запрос, расшифровывает TGT своим секретным ключом. Затем TGS использует включенный в TGT сеансовый ключ, чтобы расшифровать удостоверение. Наконец, TGS сравнивает информацию удостоверения с информацией мандата, сетевой адрес клиента – с адресом отправителя запроса и метку времени – с текущим временем. Если все совпадает, TGS разрешает выполнение запроса. Проверка меток времени предполагает, что часы всех компьютеров синхронизированы с точностью,

по крайней мере, до нескольких минут.

В ответ на правильный запрос TGS возвращает правильный мандат, который клиент может предъявить серверу. TGS также создает новый сеансовый ключ для клиента и сервера, зашифрованный сеансовым ключом, общим для клиента и TGS. Оба этих значения отправляются клиенту (сообщение 4). Клиент расшифровывает сообщение и извлекает сеансовый ключ.

3. Запрос услуги. Теперь клиент может доказать свою подлинность серверу. Клиент создает удостоверение и вместе с полученным в TGS мандатом передает запрос на сервер ресурсов (сообщение 5). Сервер расшифровывает и проверяет мандат и удостоверение, а также проверяет адрес клиента и метку времени. Если все в порядке, то сервер уверен, что, согласно Kerberos, клиент – именно тот, за кого он себя выдает. Если приложение требует взаимной проверки подлинности, сервер посылает клиенту сообщение, состоящее из метки времени, зашифрованной сеансовым ключом (сообщение 6). Это доказывает, что серверу известен правильный секретный ключ и он может расшифровать мандат и удостоверение. При необходимости клиент и сервер могут шифровать дальнейшие сообщения общим ключом. Так как этот ключ известен только им, они оба могут быть уверены, что последнее сообщение, зашифрованное этим ключом, отправлено другой стороной.