ОБ ОДНОМ КРИПТОГРАФИЧЕСКОМ ПРОТОКОЛЕ

В.В. Койбичук
Украинская академия банковского дела
Национального банка Украины (Украина)

Description of the cryptosystems, use of Kerberos crypto protocol for the information transfer protection in the shared distributed systems.

Сейчас для любой компании, государственной организации или отдельного индивидуума, которым требуется защитить данные, транзакции, репутацию, и даже самих себя, как никогда важны безопасность и проверка идентификации. Информация – это актив, который, подобно другим активам организации, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий: конфиденциальность (доступ к информации только авторизованных пользователей), целостность (достоверность и полноту информации и методов ее обработки), доступность (доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости).

Использование криптографических протоколов – один из способов защиты информации в открытых распределенных системах. Каждая криптосистема характеризуется такими понятиями, как шифрование (расшифровка), ключ шифрования (расшифровки), аутентификация. ***Шифрование*** (***кодирование***) – процесс преобразования порции информации в непонятный вид. Исходную информацию называют ***открытым текстом***, а результат преобразования – ***зашифрованным текстом (криптограммой)***. ***Декодирование (расшифровка)*** – обратный процесс преобразования зашифрованного текста в открытый. Открытый и зашифрованный текст образуют пару взаимосвязанных понятий: открытый текст поступает на вход алгоритма шифрования, а зашифрованный текст является его результатом. В ***симметричной криптосистеме*** (***системе с общим ключом*** (shared-key system)) используются одинаковые (или практически одинаковые) ключи. В ***асимметричной криптосистеме*** (***криптосистеме с открытым ключом*** (public-key cryptosystem)) используются два разных ключа: ***ключ шифрования*** и (соответствующий) ***ключ расшифровки (секретный)***. Под понятием ***аутентификация*** понимается процедура установления соответствия параметров, характеризующих пользователя, процесс или данные задан-

ным критериям. В качестве критерия соответствия обычно используется совпадение заранее введенной в систему и поступающей в процессе аутентификации информации, например, о пароле пользователя, его отпечатке пальца или структуре сетчатки глаза.

Аутентификацию можно разделить на три вида: ***аутентификация источника данных*** (***аутентификация сообщения***), ***аутентификация сущности*** и ***генерация аутентифицированных ключей.*** Первый вид аутентификации означает проверку объявленного свойства сообщения и обязательно связан с каналами связи. Она представляет собой службу безопасности получателя, предназначенную для верификации источников сообщений. Аутентификация сущности – это процесс обмена информацией (т.е. протокол), в ходе которого пользователь устанавливает подлинность другого пользователя. Часто слово «сущность» опускают. Третий вид аутентификации предназначен для организации защищенного канала обмена секретными ключами.

В качестве примера рассмотрим один из наиболее распространенных и эффективно применяемых для защиты передающейся информации, криптографический протокол Kerberos версии 5.

Участниками безопасной связи являются клиент, сервер и центр распределения ключей (KDC – Key Distribution Center), который выступает в качестве доверенного посредника.

Когда клиенту нужно обратиться к серверу, он изначально направляет запрос в центр KDC, который в ответ направляет каждому участнику предстоящего сеанса копии уникального сеансового ключа (session key), действующие в течение короткого времени. Назначение этих ключей – проведение аутентификации клиента и сервера. Обмен сообщениями происходит следующим образом:

***Сообщение 1*:**

$$A \rightarrow S : A,B\,.$$

***Сообщение 2*:**

$$S \rightarrow A:\{T_s, L, K_{ab}, B, \{T_s, L, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}\,.$$

***Сообщение 3*:**

$$A \rightarrow B:\{T_s, L, K_{ab}, A\}_{K_{bs}}\ \{A, T_a\}_{K_{ab}}.$$

***Сообщение 4*:**

$$B \rightarrow A:\{T_a+1\}_{K_{ab}}.$$

Здесь *A*, *B* – принципалы (люди, компьютеры, устройства), *S* – доверенный по средник (сервер аутентификации), *T* – метка времени, *L* – срок годности мандата, K_{ab} – общий ключ для *A* и *B*. Как видно из сообщения 2, сервер генерирует сеансовый ключ, общий для *A* и *B*, скрытно доставляет его (спрятан внутри двух мандатов), шифруя долговременными секретными ключами, который он разделяет с *A* и *B* (K_{bs} , K_{as}).

Получив протокольные сообщения от *Сервера*, пользователи (принципалы) могут обнаружить, что их послания остались без ответа, про-

верив неравенство $|Время - T| < \Delta t_1 + \Delta t_2$. Здесь *Время* означает локальное время получателя, Δt_1 – интервал, представляющий допустимую разницу между временем Сервера и локальным временем, Δt_2 – ожидаемая временна́я задержка. Если часы всех клиентов сверены по эталону, то величина Δt_1, равная одной-двум минутам, вполне допустима. Главное допущение протокола Kerberos – это то, что часы принципалов работают синхронно с часами сервера.

Таким образом, рассмотрев основные концепции протокола сетевой аутентификации Kerberos 5, нельзя полагать, что Kerberos это централизованное решение, способное решить все проблемы сетевой безопасности. В основе данного протокола лежит принцип наследования: клиент доверяет Kerberos, если система корректно предоставляет клиенту ключ шифрования. Приложение доверяет клиенту, если клиент успешно предоставил квитанцию, зашифрованную ключом сервера. В этом доверии и кроется уязвимасть системы (Kerberos). Иначе говоря, секретные ключи должны как и полагается, храниться в секрете. Если взломщик каким-либо образом получит ключ инициатора запроса, то он сможет его сымитировать. Kerberos не защищает от атак типа «подбора пароля». Если пользователь использует несложный пароль, то атакующий может спокойно подобрать его атакой по словарю.

Не смотря на эти недостатки, следует отметить, что данный протокол отличается гибкостью и эффективностью использования, а также обеспечивает повышенный уровень безопасности. Kerberos положен в основу аутентификации пользователей операционных систем Windows 2000/XP/2003.

В заключение, следует отметить, что при разработке и реализации систем защиты, нужно руководствоваться следующими принципами.

1. Ясно формулировать все необходимы предположения. Система защиты информации взаимодействует с окружением, и следовательно, это окружение должно удовлетворять определенным условиям.
2. Явно и точно указывать все предполагаемые услуги по защите информации (обеспечение конфиденциальности, доказательство знания, аутентификация, невозможность отречения, фиксация).
3. Явно выделять частные случаи математических задач (может существовать частный случай трудноразрешимой задачи, который относительно просто решить).