МЕТОД АУТЕНТИФИКАЦИИ ОБЪЕКТОВ ИНФО-КОММУНИКАЦИОННЫХ СИСТЕМ

М.М.КАРИМОВ, Ж.Т.АРЗИЕВА

Ушбу маколада ахборот-коммуникация тизимлари объектларини ўзаро аутентификациялаш асосида ҳақиқийлигини тасдиқлаш усули таклиф этилган.

In the given article are considered the questions of the authentication of objects of information-communication systems on the basis of mutual authenticate.

В компьютерных системах аутентификация и управления доступом обычно реализуются как две совершенно разные вещи. Хотя иногда имеет смысл проводить различие между задвижкой, которая удерживает дверь закрытой, и замком, который управляет задвижкой, такие вещи часто встроены в один механизм. В компьютерах же процесс аутентификации просто устанавливает правильное имя пользователя для дальнейшего использования, а управление доступом осуществляется отдельно. Компьютерные системы, как правило, управляют доступом путем сравнения имени пользователя с правилами доступа, привязанными к конкретному файлу или другому ресурсу. Если правила разрешают доступ пользователю с этим именем, то он получает возможность использовать ресурс. Современные системы аутентификации эволюционировали в результате десятилетий атак, многие из которых были успешными. Это привело к попыткам перехвата паролей, что, в свою очередь,- к возникновению других защитных мер.

Обычно стороны, вступающие в информационный обмен, нуждаются во взаимной аутентификации. Этот процесс выполняется в начале сеанса связи.

Для проверки подлинности применяют следующие способы:

- механизм запроса-ответа;
- механизм отметки времени ("временной штемпель").

Механизм запроса-ответа. Если пользователь А хочет быть уверен, что сообщения, получаемые им от пользователя В, не являются ложными, он включает в посылаемое для В сообщение непредсказуемый элемент - запрос X (например, некоторое случайное число). При ответе пользователь В должен выполнить над этим числом некоторую заранее оговоренную операцию (например, вычислить некоторую функцию f(X)). Это невозможно осуществить заранее, так как пользователю В неизвестно, какое случайное число X придет в запросе. Получив ответ с результатом действий В, пользователь А может быть уверен, что В - подлинный. Недостаток этого метода - возможность установления закономерности между запросом и ответом.

Механизм отметки времени подразумевает регистрацию времени для каждого сообщения. В этом случае каждый пользователь сети может определить насколько "устарело" пришедшее сообщение и не принимать его, поскольку оно может быть ложным.

В обоих случаях для защиты механизма контроля следует применять шифрование, чтобы быть уверенным, что ответ послан не злоумышленником.

При использовании отметок времени возникает проблема *допустимого временного интервала задержки* для подтверждения подлинности сеанса. Ведь сообщение с "временным штемпелем" в принципе не может быть передано мгновенно. Кроме того, компьютерные часы получателя и отправителя не могут быть абсолютно синхронизированы.

Для взаимной проверки подлинности обычно используют ***процедуру "рукопожатия"***, которая базируется на указанных выше механизмах и заключается во взаимной проверке ключей, используемых сторонами. Иначе говоря, стороны признают друг друга законными партнерами, если докажут друг другу, что обладают правильными ключами. Процедуру "рукопожатия" применяют в компьютерных сетях при организации связи между пользователями, пользователем и хост-компьютером, между хост-компьютерами и т.д.

В качестве примера рассмотрим процедуру "рукопожатия" для двух пользователей А и В. Пусть применяется симметричная криптосистема. Пользователи А и В разделяют один и тот же секретный ключ K_{AB}.

– Пользователь А инициирует "рукопожатие", отправляя пользователю В свой идентификатор ID_A в открытой форме.

– Пользователь В, получив идентификатор ID_A, находит в базе данных секретный ключ K_{AB} и вводит его в свою криптосистему.

– Тем временем пользователь А генерирует случайную последовательность S с помощью псевдослучайного генератора PG и отправляет ее пользователю В в виде криптограммы $E_{KAB}(S)$.

– Пользователь B расшифровывает эту криптограмму и раскрывает исходный вид последовательности S.
– Затем оба пользователя преобразуют последовательность S, используя одностороннюю функцию f.
– Пользователь B шифрует сообщение f(S) и отправляет криптограмму $E_{KAB}(f(S))$ пользователю A.
– Наконец, пользователь A расшифровывает эту криптограмму и сравнивает полученное сообщение f'(S) с исходным f(S). Если эти сообщения равны, то пользователь A признает подлинность пользователя B.

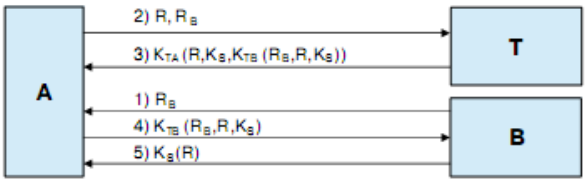
Пользователь A проверяет подлинность пользователя B таким же способом. Обе эти процедуры образуют процедуру "рукопожатия", которая обычно выполняется в самом начале любого сеанса связи между любыми двумя сторонами в компьютерных сетях.

Достоинством модели "рукопожатия" является то, что ни один из участников связи не получает никакой секретной информации во время процедуры подтверждения подлинности.

Иногда пользователи хотят иметь непрерывную проверку подлинности отправителей в течение всего сеанса связи. Рассмотрим один из простейших способов непрерывной проверки подлинности.

Чтобы отправить сообщение M, пользователь A передает криптограмму $E_K(ID_A, M)$. Получатель расшифровывает ее и раскрывает пару (ID_A, M). Если принятый идентификатор ID_A совпадает с хранимым, получатель принимает во внимание это сообщение.

Взаимная аутентификация пользователя и сети, кроме проверки подлинности пользователя, предусматривает и проверку подлинности сети. В последнем случае аутентифицирующим объектом является пользователь сети. На рисунке приведена пятиэтапная схема взаимной аутентификации системы (B) и гостевого пользователя системы (A) услуги инфокоммуникацион-ной системы.



T – мобильный пользователь. В сообщении 1 система B услуги инфокоммуникационной системы отправляет случайное число R_B в гостевому пользователю систему A. Гостевая система транслирует в мобильный пользователь T этот число, а также передает сгенерированный число R (сообщение 2).

Из мобильного пользователя T в гостевую передается сообщение 3 $K_{TA}(R, K_S, K_{TB}(R_B, R, K_S))$. Сообщение 3 зашифровано общим ключом K_{TA} мобильной и гостевой пользовательской систем UPT. Это сообщение включает:

– квитанцию $K_{TB}(R_B, R, K_S)$ доступа к системе B. Здесь K_S — сеансовый ключ, сгенерированный в мобильной системе;
– случайное число R;
– сеансовый ключ K_S.

Сообщение 3 расшифровывается в гостевой пользовательской системе A ключом K_{TB}. Полученное случайное число R подтверждает подлинность мобильной системы T. Гостевая пользовательская система транслирует квитанцию системы (сообщение 4).

Система расшифровывает полученную квитанцию, получает R_B и сравнивает с R_B, отправленным в сообщении 1. Совпадение этих значений подтверждает подлинность гостевой пользовательской системы.

Система B отправляет случайное число R, зашифрованное ключом K_S (ключ K_S расшифровывается при приеме сообщения 4) в гостевую пользовательскую систему A (сообщение 5). Расшифрованное сеансовым ключом K_S значение R позволяет убедиться в подлинности инфокоммуникационной системы.

Литература:

1. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах, ДМК Пресс, 656 стр., 2002 г.
2. Остерлох Х. TCP/IP. Семейство протоколов передачи данных в сетях компьютеров.- «ДиаСофтЮП», 2002.- 576 с.
3. Зима В., Молдовян А., Молдовян Н. Безопасность глобальных сетевых технологий, БХВ. - Санкт-Петербург, 2002.- 368 с.
4. Лукацкий А.В. Обнаружение атак. БХВ. - Санкт-Петербург, 2003.- 596 с.
5. Медведковский И.Д., Семьянов Б.В., Леонов Д.Г., Лукацкий А.В. Атака из Internet, 368 стр., 2002 г.
6. Конев И., Беляев А. Информационная безопасность предприятия.БХВ.- Санкт-Петербург, 2003 – 752 с.
7. Скляров Д. Искусство защиты и взлома информации. БХВ.- Санкт-Петербург, 2004.- 288 с.

Тошкент ахборот технологиялари университети
2011 йил 15 сентябрда қабул қилинган