$$(\lambda+\sigma)F_1(x,z)=\frac{\partial F_1(x,z)}{\partial z}-\frac{\partial F_1(x,0)}{\partial z}+$$
$$+(\lambda+\sigma/x)B(z)F_0(x)+\sigma P_1(0,z)-\sigma/x\,B(z)P_0(0),$$
$$\lambda(1-x)F_2(x,z)=\frac{\partial F_2(x,z)}{\partial z}-\frac{\partial F_2(x,0)}{\partial z}+$$
$$+(\lambda x^2+\sigma x)A(z)F_1(x)-\sigma xA(z)P_1(0),$$
$$\lambda(1-x)F_3(x,z)=\frac{\partial F_3(x,z)}{\partial z}-\frac{\partial F_3(x,0)}{\partial z}+$$
$$+\frac{\partial F_1(x,0)}{\partial z}B_1(z). \qquad (12)$$

Здесь $F_k(x)=F_k(x,\infty)$.

В уравнениях системы (12) при $z\to\infty$, имеем:

$$\frac{\partial F_1(x,0)}{\partial z}=\left(\lambda+\frac{\sigma}{x}\right)F_0(x)-(\lambda+\sigma)F_1(x)+\sigma P_1(0)-\frac{\sigma}{x}P_0(0),$$
$$\frac{\partial F_2(x,0)}{\partial z}=(\lambda x^2+\sigma x)F_1(x)-\lambda(1-x)F_2(x)-\sigma xP_1(0),$$
$$\frac{\partial F_3(x,0)}{\partial z}=\frac{\partial F_1(x,0)}{\partial z}-\lambda(1-x)F_3(x). \qquad (13)$$

Решая второе уравнение системы (12), получим:

$$F_1(x,z)=\exp\{(\lambda+\sigma)z\}f_1(x,z),$$
$$f_1(x,z)=\int_0^z\exp\{-(\lambda+\sigma)t\}\left\{\frac{\partial F_1(x,0)}{\partial z}-(\lambda+\frac{\sigma}{x})\times\right.$$
$$\left.\times B(t)F_0(x)-\sigma P_1(0,t)+\sigma/x\,B(t)P_0(0)\right\}dt \qquad (14)$$

так как $\lim\limits_{z\to\infty}F_1(x,z)=F_1(x)<\infty\Rightarrow\lim\limits_{z\to\infty}f_1(x,z)=0$. Обозначим $\beta_1(x)=\lambda(1-x)\int\limits_0^\infty\exp\{-\lambda(1-x)t\}B_1(t)dt$,

$$\Pi=(\lambda+\sigma)\int_0^\infty\exp\{-(\lambda+\sigma)t\}P_1(0,t)dt,$$
$$\beta=(\lambda+\sigma)\int_0^\infty\exp\{-(\lambda+\sigma)t\}(1-B(t))dt,$$
$$\alpha(x)=\lambda(1-x)\int_0^\infty\exp\{-(\lambda+\sigma)t\}A(t)dt,$$
$$\delta=\lambda\int_0^\infty\exp\{-\lambda tt\}B(t)dt. \qquad (15)$$

Из (14) с учетом (15) получим выражение для производной в нуле:

$$\frac{\partial F_1(x,0)}{\partial z}=\left(\lambda+\sigma/x\right)(1-\beta)F_0(x)+$$
$$+\sigma\Pi-\sigma/x\,P_0(0)(1-\beta). \qquad (16)$$

Аналогично из второго и третьего уравнений системы (12) будем иметь:

$$\frac{\partial F_2(x,0)}{\partial z}=(\lambda x^2+\sigma x)\alpha(x)F_1(x)-\sigma x\alpha(x)P_1(0),$$
$$\frac{\partial F_3(x,0)}{\partial z}=\beta_1(x)\frac{\partial F_1(x,0)}{\partial z}. \qquad (17)$$

Для неизвестных констант Π и $P_1(0)$ можно найти их выражения через константу $P_0(0)$ из системы для начальных условий (11). Приравнивая выражения из (13) с (16) и (17), получаем систему неоднородных линейных уравнений относительно искомых функций $F_k(x)$. Решая эту систему, получим выражения для производящих функций через неизвестную константу $P_0(0)$, которую можно найти из условия нормировки $F_0(1)+F_1(1)+F_2(1)+F_3(1)=1$.

Следствие. Пропускная способность сети определяется уравнением

$$S=\frac{G(1-\beta)(b+b_1)}{b_1[1+G(1-\beta)+\beta(1+aG)]+b[1+\beta(1+aG)]},$$

где b – среднее время резервирования, b_1 – среднее время обслуживания, $a=a_1/(b+b_1)$, a – средняя длительность интервала оповещения о конфликте, $R=\lambda(b+b_1)$ – загрузка системы, $\gamma=\sigma(b+b_1)$, $G=S+\gamma$

ЛИТЕРАТУРА

1. *Назаров А.А., Пичугин С.Б.* Исследование спутниковой сети связи методом математического моделирования // Изв. вузов. Физика. 1992. № 9. С. 120–129.
2. *Шохор С.Л.* Распределение числа сообщений в спутниковой сети связи с динамическим протоколом доступа // Математическое моделирование. Кибернетика. Информатика. Томск: Изд-во Том. ун-та, 1999. С. 162–166
3. *Назаров А.А., Шохор С.Л.* Сравнение асимптотической и допредельной моделей сети связи с динамическим протоколом случайного множественного доступа // Математическое моделирование и теория вероятностей. Томск: Изд-во «Пеленг», 1998. С. 233–242
4. *Баруча-Рид А.Т.* Элементы теории марковских процессов и их приложения. М.: Наука, 1969.
5. *Клейнрок Л.* Теория массового обслуживания. М.: Машиностроение, 1979.
6. *Кениг Д., Штойян Д.* Методы теории массового обслуживания. М.: Радио и связь, 1981.

Статья предоставлена кафедрой теории вероятностей и математической статистики факультета прикладной математики и кибернетики Томского государственного университета, поступила в научную редакцию 26 мая 2000 г.

УДК 002.001

А.А. Скутин

ВОПРОСЫ АУТЕНТИФИКАЦИИ УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Дается неформальное представление о корпоративных информационных системах (КИС), обсуждаются проблемы, связанные с обеспечением целостности информации в них, – защиты, аутентификации, синхронизации. Подробно обсуждаются проблемы аутентификации удаленных пользователей КИС и защиты обмениваемой информации. Предлагается модель построения механизма доступа удаленных пользователей к КИС.

Понятие корпоративной информационной системы

Информационной системой (ИС) назовем совокупность, состоящую из базы данных (БД), системы управления базой данных (СУБД) и механизмов взаимодействия БД с пользователями ИС. КИС – это некоторое конечное множество ИС, взаимодействующих между собой по определенным правилам. Под взаимодействием ИС понимается обмен информацией между базами данных ИС.

Пользователи ИС могут производить манипуляции с информацией и ее модификацию. Под манипуляцией понимаются операции чтения (Select), записи (Insert), удаления (Delete) и изменения (Update) информации, а под модификацией информации – только операции записи (Insert), удаления (Delete) и изменения (Update) информации.

Пользователей ИС можно разделить на 3 группы по ограничениям в манипуляциях с информацией – работники (лица, которым разрешается производить все виды манипуляций с некоторой строго определенной информацией в ИС), клиенты (лица, которым разрешено производить чтение части также строго определенной информации и запрещено производить модификацию информации) и сторонние лица (им запрещено манипулировать со всякой информацией). Под манипуляцией с объектом ИС подразумевается манипуляция с информацией, входящей в этот объект.

Проблемы синтеза КИС

КИС предназначается для сбора информации (по договорам, по коммерческому учету товаров и т.п.) и последующего анализа для принятия решений, способствующих эффективному управлению организацией. Организация может состоять из подразделений, расположенных на больших расстояниях друг от друга и имеющих свои ИС. Эти ИС и образуют КИС.

Рассматриваемые здесь КИС должны удовлетворять следующим условиям:

1) связь между ИС, входящими в КИС, осуществляется по сети Internet;

2) обмен информацией между ИС осуществляется в режимах On-Line (рабочий режим), Off-Line (резервный режим);

3) доступ клиентов к КИС осуществляется средствами Internet;

4) разграничение прав между работниками ИС на возможность манипулирования с тем или иным объектом ИС;

5) целостность ИС обеспечивается на уровне объектов ИС;

6) масштабируемость КИС.

В связи с этими условиями, наложенными на КИС, возникает ряд проблем, связанных с обеспечением целостности и защищенности КИС, выходящих за стандартные механизмы, заложенные в СУБД, а именно:

1) ИС обмениваются информацией (по крайне мере, в рабочем режиме) через Internet, и возникает проблема защиты КИС от различных атак со стороны пользователей Internet для перехвата, подмены, повторного использования информации (проблема защиты);

2) пользователи могут осуществлять доступ к КИС средствами Internet, и должен существовать механизм аутентификации пользователя (проблема аутентификации);

3) при обеспечении целостности ИС требуется механизм определения, какие объекты необходимо привести в информационное соответствие и в каких таблицах этих объектов были произведены модификации информации (проблема синхронизации).

Остановимся на рассмотрении проблем аутентификации пользователей и защиты обмениваемой информацией между удаленными пользователями КИС и самой КИС, т.е. затрагиваются первая и вторая проблемы. Проблема синхронизации рассмотрена в [1].

Проблемы аутентификации и защиты обмениваемой информации

Обеспечение защиты информации при обмене ею между пользователем и КИС может быть двух типов. Первый – защита обеспечивается только для информации, исходящей со стороны пользователя, второй – защита обеспечивается как пользователю, так и КИС. Первый тип возникает, когда пользователь передает конфиденциальную информацию для КИС (личный пароль, номер кредитной карточки,...), а со стороны КИС передается информация, не являющаяся конфиденциальной (чек, отчет, ...). Разделение на типы происходит вследствие того, что для решения задач защиты и аутентификации используются криптографические протоколы с открытым ключом. Для таких протоколов необходимы механизмы генерации, распределения и обслуживания открытых и закрытых ключей, поэтому в первом типе эти проблемы ложатся на КИС, а во втором – на обе стороны. Для решения проблем защиты и аутентификации необходимо рассматривать тот или иной тип, а также оценить следующие факторы:

1) важность передаваемой информации и время, в течение которого информация является конфиденциальной;

2) возможность применения дополнительных средств защиты, не заложенных в стандартные средства операционных систем (ОС) и программных продуктов (ПП).

Первый фактор отвечает за уровень защиты информации, т.е. выбор криптосистемы, размерности ключей, возможности и гибкости манипулирования с параметрами криптосистемы; второй – за то, что есть в распоряжении из криптосредств для достижения поставленной задачи.

Рассмотрим, что имеется из криптогафичиских средств в ОС фирмы Microsoft и программных продуктах, предназначенных для доступа в Internet. Существует множество технологий, но наиболее стандартизованными и известными на данный момент являются две технологии: Secure Sockets Layer (SSL) и Secure Hypertext Transport Protocol (S-HTTP) [2,3]. SSL технология разработана Netscape Communications Corporation совместно с RSA Data Security Inc и предназначена больше для решения задач первого типа. Вторая разработана Enterprise Integration Technologies (EIT) и может быть применена для задач обоих типов.

SSL технология использует криптографические протоколы RC2, RC4, DES и 3-DES с длиной ключа 128 бит для RC2 и RC4, 56 – для DES и 192 – для 3-DES. S-HTTP технология использует RC2 и DES протоколы с длинами ключей 128 и 56 бит соответственно.

Технология SSL построена на уровне TCP/IP, а S-HTTP – на уровне HTTP, поэтому S-HTTP более гибок в выборе алгоритма и его параметров. Стоит отметить также, что для обеспечения работы с использованием SSL технологии достаточно, чтобы только КИС имела сертификат, а для S-HTTP необходимо, чтобы сертификаты были и у КИС и у пользователя. Под сертификатом понимается совокупность данных, включающая: открытий ключ владельца сертификата, персональную информацию о владельце (имя, адрес,...), цифровую подпись центра сертификации (центра доверия), информацию об ограничении сертификата. Стоит отметить, что в настоящее время размерности ключей криптографических протоколов, используемых в этих технологиях, являются малыми для применения в ряде задач защиты и аутентификации, а перечень самих криптографических протоколов и невозможность их замены является дополнительным ограничением на использование предложенных технологий. Выходом из такого положения может быть создание собственной библиотеки криптографических функций и построение собственной технологии аутентификации и защиты обмениваемой информации.

Нами предлагается модель построения механизма аутентификации удаленных пользователей и защиты обмениваемой информации между пользователями и КИС.

Структура обеспечения аутентификации и защиты КИС

Предлагается следующая структура доступа удаленных пользователей к КИС (см. рис. 1).

Доступ пользователей к КИС осуществляется через сеть Internet при обращении к соответствующему www серверу. Между КИС и пользователями находится *аутентификатор КИС*, который служит для решения задачи аутентификации пользователей в КИС и ограничения прав пользователей на манипуляции с информацией в КИС. Решение задачи защиты обмениваемой информации при использовании технологии SSL и S-HTTP ложится на плечи www сервера, а при использовании собственных разработок может быть возложена на аутентификатор КИС.

Протокол взаимодействия пользователя и КИС:

1. Пользователь заходит на www сервер компании.
2. Пользователь открывает страницу аутентификации.
3. Включается протокол защиты (SSL, S-HTTP и т.д.) в зависимости от выбора, т.е.:

а) сервер отправляет пользователю сертификат и, если используется защита второго типа, то запрашивает сертификат от пользователя;

б) стороны, получившие сертификат, проверяют его на пригодность и доверие;

в) если проверка проходит успешно, устанавливается защищенное соединение, иначе выдается сообщение об отказе в доступе на страницу аутентификации.

Рис. 1

4. Пользователь вводит аутентификационные данные (имя, пароль, номер карточки, ...).
5. Аутентификатор КИС получает аутентификационные данные и проверяет их в базе пользователей КИС.
6. Если аутентификация прошла успешно, то пользователь может работать с КИС, иначе происходит отказ.

Организация механизмов ввода аутентификационных данных пользователями на страницу www сервера изложена в [4].

При решении задач аутентификации и защиты обмениваемой информации следует использовать *рабочие сертификаты*, т.е. сертификаты, которым КИС доверяет. В связи с этим необходим механизм управления сертификатами, т.е. оперативной выдачи, замены и отзыва сертификатов. Для этого целесообразно иметь собственный сервер сертификации, например, на основе Microsoft Certificate Server 2.0. Применяя технологии, использующие сертификаты пользователей, можно упростить механизм аутентификации, исключив четвертый пункт, в базе пользователей хранить вместо паролей или хеш-значений паролей открытые ключи или хеш-значения открытых ключей, взятых из сертификатов пользователей.

В данной модели вся работа пользователя с данными КИС осуществляется через аутентификатор КИС, который, в свою очередь, имеет доступ к КИС с определенными правами на манипулирование с данными в КИС. Соответственно если необходимо разделение пользователей по правам доступа к информации в КИС, то необходимо в базе пользователей вести учет их по группам прав на выполнение манипуляций с данными в КИС.

ЛИТЕРАТУРА

1. *Скутин А.А.* Вопросы защиты в корпоративных информационных системах // Доклады к международной конференции «Информационные системы и технологии». Новосибирск: НГТУ, 1999. Т. 2.
2. Rescola E., *Shiffman A.* The Secure HyperText Transfer Protocol // RFC 2660, www.kiarchive.ru/pub/internet/rfc.
3. Internet Connection Server Webmaster's Guide // lsx20r.nsls.bnl.gov.
4. *Леонов Д.* Ставим пароль на страницу // www.hackzone.ru/articles/password.html.

Статья представлена кафедрой математической логики и проектирования радиофизического факультета Томского государственного университета, поступила в научную редакцию 15 мая 2000 г.