Защита данных в сложных информационных системах

А. Ю. Даниленко

Рассматривается общая концепция защиты информации в клиент-серверных системах сложной архитектуры, обрабатывающих различные информационные объекты.

1. Введение

Задача защиты информации ограниченного доступа от несанкционированного использования существовала всегда. В разное время она решалась по-разному, но всегда общим в подходе к охране любого информационного объекта оставались несколько простых и очевидных принципов. В первую очередь это наличие владельца объекта, который давал разрешение на использование данных, а также наличие более или менее понятных правил, которыми он при этом руководствовался, наличие средств защиты технического характера (шифрование, тайнопись, сейфы), а также организационные меры по защите информации, например, тщательный отбор и ограничение круга лиц, подлежащих ознакомлению. Не следует исключать из рассмотрения и физическую охрану носителей информации, которая всегда присутствует в том или ином виде среди средств защиты данных. В точном соответствии с указанными принципами защиты находятся и средства несанкционированного доступа к информации: взлом сейфов, подкуп, расшифровка зашифрованных данных.

В последнее время интерес к рассматриваемой теме в части, относящейся к защите данных в информационных системах, существенно обострился. Это связано с рядом причин, являющихся логичным следствием тенденций развития вычислительной техники. Так, бурное развитие технологий, использующих Интернет (включая и электронную почту), привело к тому, что все больше людей используют Всемирную паутину не как средство для получения кем-то опубликованных данных, а как средство общения. При этом, естественно, каждый из них предполагает, что отправляемая им информация должна быть доступна только адресату — тому, кому она предназначена. Однако, сами по себе протоколы

информационного обмена, используемые в Сети, совершенно не предназначены для выполнения этой функции, что, естественно, приводит к разработке всевозможных надстроек над ними, например, SSL над Http.

Помимо проблем, связанных с обменом данными, серьезное значение приобретает то, что многие организации, как государственные, так и коммерческие, хранят в информационных системах данные ограниченного доступа. Самые вопиющие преступления в этой части — публикации баз данных МВД (прописка, водительские удостоверения, госномера автомобилей) и операторов сотовой связи. Строго говоря, закрытая информация хранится в информационных системах государственных ведомств уже десятки лет, однако именно сейчас это становится серьезной проблемой, поскольку прежде работа с этими данными, хранящимися в вычислительных комплексах на основе больших ЭВМ, таких, как ЕС, БЭСМ, IBM, Univac, существенно отличалась от современных стандартов. Доступ к хранящимся в этих системах данным был возможен только через операторов, выполнявших поиск и выдачу данных только по распоряжению руководства, что означает применение организационных мер защиты. Сейчас в связи с широким распространением персональных ЭВМ легальные пользователи закрытой информации предпочитают работать с ней так же, как они это делают с любыми другим данными, что приводит к необходимости применения специально разрабатываемых технических средств защиты.

2. Способы защиты информации и их взаимодействие между собой

Под защитой информации, как правило, понимается решение нескольких взаимосвязанных задач. Это защита данных от несанкционированного доступа, куда входит как разграничение доступа само по себе, так и средства подтверждения подлинности субъекта, обратившегося к данным. Кроме того, требуется обеспечить доступность информации, противодействуя преднамеренному выводу из строя информационных систем. Следующей задачей является обеспечение целостности (неизменности) как хранимых данных, так и программного обеспечения (в первую очередь средств защиты информации — СЗИ). К этим проблемам примыкает аудит — средства протоколирования фактов доступа к данным и других событий в информационной системе, а также средства просмотра протоколов с разграничением прав доступа к их данным.

Рассмотрим основные технические способы решения перечисленных задач [1, 2].

Идентификация и аутентификация (авторизация). Под авторизацией понимается определение субъекта (например, путем ввода им своего

имени) и проверка подлинности предъявленных идентификационных данных (например, ввод пароля). Таким образом, после выполнения этих двух процедур информационная система фиксирует, что с указанного компьютера с ней работает определенный человек, обладающий правами, зафиксированными в базе данных системы.

Разграничение доступа. Для реализации разграничения доступа, т. е. алгоритмов, позволяющих предоставлять средствами системы доступ к информации выделенным субъектам, требуется выработка непротиворечивых правил доступа к хранимым информационным объектам и последующая реализация их на программном уровне. Как правило, эти правила оформляются в виде матрицы доступа, устанавливающей соответствие субъектов и их прав на выполнение действия с защищаемыми информационными объектами. При реализации алгоритмов выдачи данных существенно используются результаты выполненной авторизации пользователей.

Аудит (протоколирование). Важность этой части СЗИ обусловлена тем простым соображением, что абсолютно защищенной системой можно признать только систему, установленную на выключенный компьютер, помещенный в хорошо охраняемый сейф. В связи с этим средства аудита выполняют следующие функции: предоставление информации разработчикам СЗИ для выявления и последующего устранения уязвимостей, сбор данных для руководства и службы безопасности организации о сотрудниках, пытающихся обойти систему защиты, выдача информации о попытках взлома системы защиты для немедленного реагирования со стороны службы безопасности.

Блокировки и оповещения. С последней задачей, решаемой системой аудита, тесно связана система блокировок и оповещений. Речь в данном случае идет о том, что в случае обнаружения попыток несанкционированного доступа к данным (НСД) система автоматически оповещает администратора безопасности или других уполномоченных лиц о произошедшем. Кроме этого, она может в автоматическом режиме или по команде с АРМ аудитора заблокировать дальнейшую работу пользователя. Точно также возможна блокировка конкретных информационных объектов, если выявлено, что они были искажены (преднамеренно или в результате технических сбоев).

Использование средств защиты операционных систем и СУБД. Все современные операционные системы (ОС) и СУБД обладают встроенными средствами защиты обрабатываемых данных. Для ОС линейки Windows NT (NT, 2000, XP, Vista) это средства разграничения доступа к файлам, директориям, ключам реестра, системным журналам событий, учетным записям пользователей и другим объектам. При этом подразумевается, что объекты средствами любого программного комплекса

защищаются от попыток НСД, выполняемых средствами этого же самого комплекса. Другими словами, средствами Windows, как правило, нельзя защитить данные, если их читают напрямую с жесткого диска специально разработанными программами, работающими на уровне секторов. Исключением из этого правила можно считать шифрование самих данных, записываемых на диск. Аналогично разграничивается доступ и к объектам, хранящимся в базах данных под управлением промышленных СУБД (Oracle, MS SQL Server, Cache), причем для случая реляционных СУБД разграничивается доступ на уровне таблиц и колонок базы данных. Все указанные средства могут и должны применяться для защиты информации от НСД в информационных системах, однако здесь возникает вопрос о надежности этих средств и возможности их использования для работы с данными требуемого уровня конфиденциальности. В связи с этим вводится понятие доверенных систем, которым обозначаются системы, которые можно использовать для конкретной цели в конкретных условиях (мы доверяем этой системе свои данные). Процесс обретения системой нужной степени доверия всегда сложен и состоит из нескольких этапов, он описывается процедурой сертификации на соответствие требованиям соответствующего уровня [3–8], при которой проверяется соответствие системы требованиям как по функционалу, так и по отсутствию в ней недекларированных возможностей (например, программных закладок). Следует отметить, что упомянутые процедуры сертификации обязательны не во всех случаях, точный перечень систем, для которых это обязательно, приведен в соответствующих нормативных актах.

Защита объектов информационных систем. Как отмечалось выше, ОС и СУБД предоставляют возможность для защиты (в первую очередь разграничения доступа) своих объектов — файлов и записей в таблицах баз данных. Однако, сложные информационные системы (ИС) оперируют другими объектами, которые хранятся в объектах ОС и СУБД, например, системы электронного документооборота оперируют с документами, каждый из которых представляет собой совокупность ряда файлов и записей в базе данных. Это приводит к тому, что средствами ОС и СУБД нельзя разграничить доступ к таким документам, эту задачу решает прикладная система, в базе данных которой хранится информация о матрице доступа к объектам, в соответствии с этими данными ИС сама разрешает или запрещает выдачу и модификацию данных. При этом средствами ОС и СУБД доступ к файлам и базе данных предоставляется учетным записям пользователей, от имени которых работает прикладная ИС.

Контроль целостности программного обеспечения (ПО) и объектов ИС. Под контролем целостности ПО понимается периодический или по специальной команде обслуживающего персонала контроль соответствия установленного на данном компьютере ПО исходному, уста-

новленному с инсталляционного комплекта доверенному ПО. Важность этой работы обусловлена возможностью установки специально разработанных вредоносных программ, в первую очередь предназначенных для обхода СЗИ. Такой контроль выполняется путем вычисления и хранения уникальных характеристик файлов, ключей реестра и других подобных данных сразу после установки. В качестве уникальных характеристик могут использоваться контрольные суммы файлов или вычисляемые по особым алгоритмам хэш-значения (см. следующий раздел). Точно также требуется контроль целостности обрабатываемых данных, что позволит гарантировать их неизменность при хранении и передаче, а также отследить, что модификация данных выполняется только в установленном порядке. При этом контролироваться должны объекты ИС, а не объекты ОС, т. е. для контроля целостности документа необходимо вычислять хэш-значения всех файлов документа и соответствующих ему записей в базе данных. Проверка целостности объектов ИС может выполняться при выдаче пользователям или по отдельным командам в режиме регламентных работ.

Криптозащита. В СЗИ используются несколько видов криптографических алгоритмов: симметричное шифрование, при котором для шифрования и расшифровки используется один и тот же ключ; несимметричное шифрование. Когда данные шифруются одним ключом, а расшифровываются другим, не равным первому, но составляющим с ним пару (при этом один из ключей — «открытый ключ» — доступен всем желающим, а другой — «закрытый» — сохраняется в тайне и доступен только его владельцу); вычисление хэш-значений для контроля целостности, под хэш-значением понимается результат преобразования исходного текста, при котором получается последовательность символов фиксированной длины (например, 128 байт для любого исходного набора данных). При этом алгоритм преобразования составляется таким образом, чтобы гарантировать получение одного и того же результата при одинаковых исходных данных, существенное отличие результата при незначительных изменениях исходного набора, а также невозможность (либо принципиальную, либо за разумное время) восстановления исходного текста по хэш-значению.

Шифрование сетевого трафика. Наиболее очевидное применение криптографии для защиты данных в информационной системе — шифрование их при передаче по каналам связи. Наличие такого шифрования предотвращает утечку информации в случае, если злоумышленник имеет возможность перехвата сетевого трафика. Такое шифрование осуществляется, как правило, с помощью симметричных алгоритмов, что позволяет выполнять это за разумное время. Алгоритм формирования ключа для шифрования разрабатывается таким образом, чтобы

свести к минимуму вероятность самостоятельного вычисления ключа злоумышленником.

Электронно-цифровая подпись (ЭЦП). Применяется для контроля неизменности данных при передаче или при хранении. ЭЦП представляет собой хэш-значение подписываемых данных (например, содержимого файла), зашифрованное закрытым ключом пользователя. Для проверки подписи она расшифровывается открытым ключом, при этом получается хэш-значение исходных данных, а затем выполняется хэширование полученного массива. Если хэш-значения равны, это означает, что, во-первых, данные с момента подписания не поменялись и, во-вторых, они были подписаны именно тем пользователем системы, подпись которого мы проверяли.

Шифрование хранимых данных. Может быть применено для защиты данных от НСД в месте постоянного хранения. Реализовано может быть путем шифрования данных при их получении одним и тем же ключом с использованием симметричного алгоритма. Применение одного ключа, конечно, не является обязательным, он может формироваться, исходя из каких-либо свойств документа (или иного шифруемого объекта), однако это не служит надежной защитой от подбора ключа с помощью специально написанных программ. Рассматриваемый способ защиты обычно применяется с целью замены физической охраны серверного компьютера, однако он нам представляется неэффективным. Это связано с тем, что в случае похищения всего жесткого диска с зашифрованными данными у специалиста будет неограниченное время для расшифровки путем подбора ключей, а также и неограниченный массив зашифрованных данных, что позволит решить задачу расшифровки за вполне приемлемое время. Кроме того, для большей сохранности данных желательно периодически обновлять ключ шифрования, что ведет к необходимости перешифровки всего накопленного массива данных.

Вычисление хэш-значений для контроля целостности. Применяется для контроля целостности программного обеспечения и хранимых данных.

3. Проектирование системы защиты

Проектирование системы защиты является одной из задач, решаемых при проектировании всей информационной системы. Начинаться оно должно с самого начала, при формулировании функциональных требований к системе и проведении обследования. Одной из основных задач, решаемых в этот момент, является формирование политики или модели безопасности.

3.1. Формирование модели безопасности

Модель безопасности призвана ответить на несколько простых вопросов, от ответов на которые зависит архитектура всей системы и, в особенности, ее части, связанной с защитой информации. Правильно и точно сформулированная модель безопасности позволяет достаточно точно оценить необходимые средства защиты, а также после реализации СЗИ проверить корректность выполненной работы. Обычно некоторые фрагменты модели безопасности включаются в Техническое задание на систему или в отдельное ТЗ на СЗИ, в то время как полное ее изложение является частью Технического или Эскизного проекта системы. Основные разделы модели безопасности перечислены ниже.

Субъекты защиты. Этот раздел характеризует тех, от кого, собственно, защищается информация. Например, это могут быть легальные пользователи системы, которые пытаются получить привилегии, превосходящие их собственные. Кроме того, возможна постановка задачи, когда система защищается от обслуживающего персонала или случайно зашедших в офис организации посетителей. Здесь же целесообразно определить некоторые привилегии пользователей системы, например, привилегия супервизора, который может читать все данные системы, но не может их изменять. Целесообразно определить полномочия администраторов системы, рассмотреть возможность и целесообразность выделения в отдельную системную роль администраторов безопасности.

Объекты защиты. Это — полный перечень защищаемых информационных объектов. Например, для системы электронного документооборота это могут быть документы, сообщения почтовой системы, информация о поручениях, исполняемых пользователями, личные расписания пользователей, информация о подготавливаемых ими совещаниях и других мероприятиях. Однако, некоторые информационные объекты могут и не входить в перечень объектов защиты, если утечка или искажение информации о них не существенна для заказчика системы (например, график отпусков или перечень выходных и праздничных дней в организации). Естественно, отсутствие объекта в списке объектов защиты не означает, что он может искажаться или уничтожаться произвольным образом. Работа с ним идет по обычным правилам работы в системе, что обеспечивает его сохранность, но специальных мер по линии СЗИ для его защиты не применяется, поскольку его искажение или получение данных по нему посторонними лицами не ведет к существенному ущербу для организации-заказчика информационной системы.

Допустимые действия субъектов с объектами. Представляет собой список действий с объектами защиты. Обычно это создание, уничтожение, чтение и модификация объекта. Часто отдельно выделяется измене-

ние прав доступа к объекту, например, изменение списка пользователей, которые могут редактировать содержимое объекта.

Правила определения допустимости действий. Формулировка правил в этом разделе должна быть достаточно ясной для того, чтобы проверка из выполнения не приводила к разночтениям в трактовке. Например, право чтения документа имеют те пользователи, которые занесены в список «Читатели» для этого документа. Право создания документов и писем имеют все пользователи системы. При этом положения модели безопасности могут отличаться от деловой логики системы, например, право создания документов может быть ограничено для некоторых их категорий (входящие документы могут регистрировать только работники секретариата). Также с точки зрения СЗИ любой пользователь может отправить письмо любому пользователю системы, тогда как с точки зрения алгоритма работы всей системы в целом отправлять письма директору имеют право только руководители структурных подразделений. Это различие не снижает защищенности данных, поскольку реального несанкционированного доступа к ни мне происходит, однако простота правил позволяет точно оценить корректность их реализации.

Перечень протоколируемых событий в системе. Как уже говорилось выше, протоколировании является одним из способов защиты информации, поэтому перечень событий и определение объема протоколируемых данных — одна из существенных частей проектирования СЗИ. Обычно протоколируются события, связанные с входом пользователей в систему и выходом из нее, изменения в базе данных пользователей (регистрация новых пользователей, помещение их в системные группы). Также протоколируются события, связанные с доступом к объектам защиты: их создание и уничтожение, просмотр пользователями, изменение самих объектов и отдельно прав доступа к ним. Для обеспечения нормальной работы системы необходимо протоколировать и внутрисистемные события — аппаратные сбои, искажения или потерю данных. В протоколы заносятся обычно время события, пользователь, выполняющий действие, определение действия.

Модель нарушителя, т. е. характеристика потенциального нарушителя, включающая в себя его уровень квалификации, должностное положение, имеющиеся возможности в плане воздействия на систему. Этот пункт важен тем, что для нарушителей разной квалификации и с разными техническими возможностями средства защиты могут радикально отличаться. Так, для недобросовестного коллеги, компьютерная грамотность которого ограничивается умением копировать файлы на дискету, достаточно блокировать рабочую станцию и закрыть сетевой доступ к дискам; для профессионала, занимающегося промышленным шпионажем, нужен хороший замок на дверях серверной и шифрование сетевого

трафика средней стойкости. Ну а защиту от спецслужб мы вообще не рассматриваем.

Модель угроз, т. е. угрозы защищаемым данным и способы их преодоления. С предыдущим пунктом тесно связано описание предполагаемых угроз защищаемым данным [2]. Полный список угроз должен включать не только перехват сетевых пакетов и похищение компьютера, но и вирусные атаки, атаки типа «Отказ в обслуживании», стихийные бедствия. Следует отметить, что способы преодоления могут быть не только программные, но и организационно-административные меры, а также подбор и обучение персонала.

3.2. Особенности защиты готовых систем

Проектирование системы защиты в идеальном случае должно вестись одновременно с проектированием самой информационной системы, однако возможна ситуация, когда заказчик системы пожелает использовать уже готовую и хорошо ему знакомую систему для работы с конфиденциальными данными. При этом потребуется встроить систему защиты в уже готовую систему, совершенно на это не рассчитанную. В этой ситуации можете оказаться полезным локализовать максимальную часть функционала, связанного с информационной безопасностью, в отдельном модуле — Диспетчере доступа. Такой модуль может, находясь на сервере, анализировать весь информационный обмен между клиентом и сервером, реализуя политику безопасности, отличную от заложенной в исходную систему.

4. Заключение

Рассмотренная задача защиты информации в сложных системах не представляется неразрешимой, однако ее решение оказывается индивидуальным в случае каждой конкретной системы и каждого конкретного заказчика.

Литература

1. *Вихорев С.*, *Кобцев Р.* Как определить источники угроз // Открытые системы. 2002. № 7–8.
2. *Галатенко В.* Информационная безопасность // Открытые системы. 1995. № 4–6.
3. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М., 1992.

4. Гостехкомиссия России. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. М., 2002.
5. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. М., 1992.
6. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. М., 1992.
7. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. М., 1992.
8. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. М., 1992.