Обеспечение защиты информации в компьютерных сетях

Опасность злоумышленных несанкционированных действий над информацией приняла особенно угрожающий характер с развитием компьютерных сетей. Большинство систем обработки информации создавалось как обособленные объекты: рабочие станции, ЛВС, большие универсальные компьютеры и т.д. Каждая система использует свою рабочую платформу (MS DOS, Windows, Novell), а также разные сетевые протоколы (TCP/IP, VMS, MVS). Сложная организация сетей создает благоприятные предпосылки для совершения различного рода правонарушений, связанных с несанкционированным доступом к конфиденциальной информации. Большинство операционных систем, как автономных, так и сетевых, не содержат надежных механизмов защиты информации.

Следствием опасности сетевых систем стали постоянно увеличивающиеся расходы и усилия на защиту информации, доступ к которой можно осуществить через сетевые каналы связи. Сохранить целостность данных можно только при условии принятия специальных мер контроля доступа к данным и шифрования передаваемой информации. Разные системы нуждаются в разных степенях защиты. Актуальной стала задача объединения систем с различными степенями защищенности (например, на платформах Unix и Windows).

Необходимо иметь четкое представление о возможных каналах утечки информации и путях несанкционированного доступа к защищаемой информации. Только в этом случае возможно построение эффективных механизмов защиты информации в компьютерных сетях (Локальные вычислительные сети.

Угрозы безопасности сети

Пути утечки информации и несанкционированного доступа в компьютерных сетях в основной своей массе совпадают с таковыми в автономных системах (см. выше). Дополнительные возможности возникают за счет существования каналов связи и возможности удаленного доступа к информации. К ним относятся:

- электромагнитная подсветка линий связи;
- незаконное подключение к линиям связи;
- дистанционное преодоление систем защиты;
- ошибки в коммутации каналов;
- нарушение работы линий связи и сетевого оборудования.

Вопросы безопасности сетей решаются в рамках архитектуры безопасности, в структуре которой различают:

- угрозы безопасности;
- службы (услуги) безопасности;
- механизмы обеспечения безопасности.

Под *угрозой безопасности* понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства.

Угрозы принято подразделять на непреднамеренные, или случайные, и умышленные.

Случайные угрозы возникают как результат ошибок в программном обеспечении, выхода из строя аппаратных средств, неправильных действий пользователей или администратора сети и т.п.

Умышленные угрозы преследуют цель нанесения ущерба пользователям и абонентам сети и, в свою очередь, подразделяются на активные и пассивные.

Пассивные угрозы направлены на несанкционированное использование информационных ресурсов сети, но при этом не оказывают влияния на ее функционирование. Примером пассивной угрозы является получение информации, циркулирующей в каналах сети, посредством прослушивания.

Активные угрозы имеют целью нарушение нормального процесса функционирования сети *посредством целенаправленного воздействия* на ее аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя компьютера или операционной системы, искажение сведений в пользовательских базах данных или системной информации и т.п.

К основным угрозам безопасности информации в сети относятся:

- раскрытие конфиденциальной информации;
- компрометация информации;
- несанкционированный обмен информацией;
- отказ от информации;
- отказ в обслуживании;
- несанкционированное использование ресурсов сети;
- ошибочное использование ресурсов сети.

Угрозы раскрытия конфиденциальной информации реализуются путем несанкционированного доступа к базам данных.

Компрометация информации реализуется посредством внесения несанкционированных изменений в базы данных.

Несанкционированное использование ресурсов сети является средством раскрытия или компрометации информации, а также наносит ущерб пользователям и администрации сети.

Ошибочное использование ресурсов является следствием ошибок, имеющихся в программном обеспечении ЛВС.

Несанкционированный обмен информацией между абонентами сети дает возможность получать сведения, доступ к которым запрещен, т.е., по сути, приводит к раскрытию информации.

Отказ от информации состоит в непризнании получателем или отправителем этой информации фактов ее получения или отправки.

Отказ в обслуживании представляет собой весьма распространенную угрозу, источником которой является сама сеть. Подобный отказ особенно

опасен в случаях, когда задержка с предоставлением ресурсов сети может привести к тяжелым для абонента последствиям.

Службы безопасности сети

Службы безопасности сети указывают направления нейтрализации возможных угроз безопасности. Службы безопасности находят свою практическую реализацию в различных механизмах безопасности. Одна и та же служба безопасности может быть реализована с использованием разных механизмов безопасности или их совокупности.

♦ ***Различия в составе и особенностях служб безопасности.*** Протоколы информационного обмена в сетях делятся на две большие группы: типа *виртуального соединения* и *дейтаграммные,* в соответствии с которыми сети также принято делить на *виртуальные* и *дейтаграммные.*

В *виртуальных* сетях передача информации между абонентами организуется по так называемому *виртуальному каналу* и происходит в три этапа: создание канала (соединение), собственно передача, уничтожение канала (разъединение). Сообщения разбиваются на блоки, которые передаются в порядке их следования в сообщении.

В дейтаграммных сетях пакеты *(дейтаграммы)* сообщения передаются от отправителя к получателю независимо друг от друга по различным маршрутам, в связи с чем порядок доставки пакетов может не соответствовать порядку их следования в сообщении. Виртуальная сеть в концептуальном плане реализует принцип организации телефонной связи, тогда как дейтаграммная – почтовой.

Международная организация стандартизации (МОС) определяет следующие службы безопасности:

1) аутентификация (подтверждение подлинности);
2) обеспечение целостности;
3) засекречивание данных;
4) контроль доступа;
5) защита от отказов.

Две последние службы едины для дейтаграммных и виртуальных сетей. Первые три характеризуются определенными отличиями, обусловленными особенностями используемых в сетях протоколов.

♦ ***Служба аутентификации.*** Данная служба применительно к виртуальным сетям называется *службой аутентификации объекта (одноуровневого)* и обеспечивает подтверждение того факта, что отправитель информации является именно тем, за кого он себя выдает. Применительно к дейтаграммным сетям служба аутентификации называется *службой аутентификации источника данных.*

♦ ***Службы целостности.*** Под *целостностью* понимается точное соответствие отправленных и полученных данных между собой. Службы целостности для рассматриваемых сетей выглядят следующим образом:

виртуальные сети:

• служба целостности соединения с восстановлением;

• служба целостности соединения без восстановления;

• служба целостности выборочных полей соединения;

дейтаграммные сети:

• служба целостности без соединения;

• служба целостности выборочных полей без соединения.

Под *полями* понимаются отдельные определенные элементы блоков или пакетов передаваемых данных. Под *восстановлением* понимаются процедуры восстановления данных, уничтоженных или потерянных в результате обнаружения искажений, вставок или повторов в блоках или дейтаграммах. В службах целостности дейтаграммных сетей наличие процедур восстановления не предусматривается.

♦ ***Службы засекречивания данных:***

• *служба засекречивания соединения* – обеспечивает секретность всех данных, пересылаемых объектами по виртуальному каналу;

• *служба засекречивания без соединения* – обеспечивает секретность данных, содержащихся в каждой отдельной дейтаграмме;

• *служба засекречивания отдельных полей соединения;*

• *служба засекречивания трафика* – нейтрализует возможность получения сведений об абонентах сети и характере использования сети.

Механизмы безопасности

Среди механизмов безопасности сетей, предусмотренных МОС, обычно выделяют следующие *основные:*

• шифрование;

• контроль доступа;

• цифровая подпись.

♦ ***Шифрование*** применяется для реализации служб засекречивания и используется в ряде других служб.

♦ ***Механизмы контроля доступа*** обеспечивают реализацию одноименной службы безопасности, осуществляют проверку полномочий объектов сети, т.е. программ и пользователей, на доступ к ресурсам сети. При доступе к ресурсу через соединение контроль выполняется в точке инициализации связи, в промежуточных точках, а также в конечной точке.

Механизмы контроля доступа делятся на *две основные группы:*

• *аутентификация объектов,* требующих ресурса, с последующей проверкой допустимости доступа, для которой используется специальная информационная база контроля доступа;

• *использование меток безопасности,* связываемых с объектами; наличие у объекта соответствующего мандата дает право на доступ к ресурсу.

Самым распространенным и одновременно самым ненадежным методом аутентификации является *парольный доступ.* Более совершенными являются пластиковые карточки и электронные жетоны. Наиболее надежными считаются методы аутентификации по особым приметам личности, так называемые *биометрические методы.*

♦ ***Цифровая подпись*** *используется для реализации служб аутентификации и защиты от отказов.* По своей сути она призвана служить электронным аналогом реквизита “подпись”, используемого на бумажных документах. Механизм цифровой подписи базируется на использовании способа шифрования с открытым ключом. Знание соответствующего открытого ключа дает возможность получателю электронного сообщения однозначно опознать его отправителя.

Дополнительными механизмами безопасности, предусмотренными МОС, являются следующие:

- обеспечение целостности данных;
- аутентификация;
- подстановка трафика;
- управление маршрутизацией;
- арбитраж.

♦ ***Механизмы обеспечения целостности данных*** направлены на реализацию одноименной службы как применительно к отдельному блоку данных, так и к потоку данных. Целостность блока обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Возможны и более простые методы контроля целостности потока данных, например нумерация блоков, дополнение их меткой времени и т.д.

♦ ***Механизмы обеспечения аутентификации*** используются для реализации одноименной службы, различают одностороннюю и взаимную аутентификацию. В первом случае один из взаимодействующих объектов одного уровня проверяет подлинность другого, тогда как во втором проверка является взаимной. На практике механизмы аутентификации, как правило, совмещаются с контролем доступа, шифрованием, цифровой подписью и арбитражем.

♦ ***Механизмы подстановки трафика*** используются для реализации службы засекречивания потока данных. Они основываются на генерации объектами сети фиктивных блоков, их шифровании и организации их передачи по каналам сети.

♦ ***Механизмы управления маршрутизацией*** используются для реализации служб засекречивания. Эти механизмы обеспечивают выбор маршрутов движения информации по сети.

♦ ***Механизмы арбитража*** обеспечивают подтверждение характеристик данных, передаваемых между объектами сети, третьей стороной. Для этого вся информация, отправляемая или получаемая объектами, проходит и через арбитра, что позволяет ему впоследствии подтвердить упомянутые характеристики.

В общем случае *для реализации одной службы безопасности может использоваться комбинация нескольких механизмов безопасности.*

Защита сетевых операционных систем

Операционная система и аппаратные средства сети обеспечивают защиту ресурсов сети, одним из которых является сама ОС, т.е. входящие в нее программы и системная информация. Поэтому в сетевой ОС ЛВС должны быть так или иначе реализованы механизмы безопасности.

Принято различать:

• пассивные объекты защиты (файлы, прикладные программы, терминалы, области оперативной памяти и т.п.);

• активные субъекты (процессы), которые могут выполнять над объектами определенные операции.

Защита объектов реализуется операционной системой посредством контроля за выполнением субъектами совокупности правил, регламентирующих указанные операции. Указанную совокупность иногда называют *статусом защиты.* Операции, которые могут выполняться над защищенными объектами, принято называть *правами доступа,* а права доступа субъекта по отношению к конкретному объекту – *возможностями.* В качестве *формальной модели статуса защиты* в ОС чаще всего используется так называемая *матрица контроля доступа.*

Достаточно простым в реализации средством разграничения доступа к защищаемым объектам является *механизм колец безопасности.*

Защита файлов в ОС организована следующим образом. С каждым файлом связывается множество *прав доступа:* чтение, обновление и (или) выполнение (для исполняемых файлов). Владелец файла, т.е. создавшее его лицо, пользуется но отношению к файлу всеми правами. Часть этих прав он может передать членам группы – лицам, которым он доверяет сведения, имеющиеся в файле.

Доступ к ресурсам ОС чаще всего ограничен средствами защиты по паролям. Пароль может быть использован и в качестве ключа для шифрования-дешифрования информации в пользовательских файлах. Сами пароли также хранятся в зашифрованном виде, что затрудняет их выявление и использование злоумышленниками. Пароль может быть изменен пользователем, администратором системы либо самой системой по истечении установленного интервала времени.

Защита распределенных баз данных

Обеспечение безопасности распределенных баз данных (РБД) косвенно реализуется сетевой ОС. Однако все указанные механизмы и средства инвариантны конкретным способам представления информации в БД. Подобная инвариантность приводит к тому, что в случае непринятия специальных мер все пользователи СУБД имеют равные права по

использованию и обновлению всей информации, имеющейся в базе данных. В то же время указанная информация, как и при ее неавтоматизированном накоплении и использовании, должна быть разбита на категории по грифу секретности, группам пользователей, которым она доступна, а также по операциям над нею, которые разрешены указанным группам. Реализация этого процесса требует разработки и включения в состав СУБД специальных механизмов защиты.

Принятие решения о доступе к той или иной информации, имеющейся в РБД, может зависеть от следующих факторов:

1) времени и точки доступа;
2) наличия в БД определенных сведений;
3) текучести состояния СУБД;
4) полномочий пользователя;
5) предыстории обращения к данным.

В первом случае доступ к БД с каждого терминала ЛВС может быть ограничен некоторым фиксированным отрезком времени.

Во втором случае пользователь может получить из БД интересующие его сведения только при условии, что база данных содержит некоторую взаимосвязанную с ними информацию определенного содержания.

В третьем случае обновление информации в некоторой БД может быть разрешено пользователю только в те моменты времени, когда она не обновляется другими пользователями.

В четвертом случае для каждого пользователя прикладной программы устанавливаются индивидуальные права на доступ к различным элементам базы данных. Эти права регламентируют операции, которые пользователь может выполнять над указанными элементами. Например, пользователю может быть разрешен отбор элементов БД, содержащих информацию о товарах, предлагаемых на бирже, но запрещено обновление этих сведений.

В основе *пятого* из перечисленных факторов лежит то обстоятельство, что интересующую его информацию пользователь может получить не непосредственным отбором тех или иных элементов БД, а косвенным путем, т.е. посредством анализа и сопоставления ответов СУБД на последовательно вводимые запросы (команды на обновление данных). В связи с этим для обеспечения безопасности информации в БД в общем случае необходимо учитывать предысторию обращения к данным.