41. Защита информации в локальных и глобальных компьютерных сетях

Автор: Александр
26.08.2014 15:48

Данных о потерях российских компаний от сбоев в работе локальных сетей в прессе пока не приводилось, однако можно предположить, что и для них проблема отказоустойчивости сети и защиты данных является актуальной. Ведь не секрет, что многие российские фирмы на заре своей деятельности отдавали предпочтение наиболее дешевым и, зачастую, наименее надежным сетевым решениям. По данным анкетирования 100 администраторов локальных сетей, проведенного фирмой АйТи в январе этого года, серьезные сбои в работе сетевого оборудования и программного обеспечения в большинстве российских фирм происходят не реже, чем один раз в месяц.

Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике. На сегодняшний день сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать [1].

- целостность данных - защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных;

- конфиденциальность информации и, одновременно,

- ее доступность для всех авторизованных пользователей.

Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач. В данной статье мы не будем затрагивать вопросы специальных систем безопасности, а остановимся на общих вопросах защиты информации в компьютерных сетях.

При рассмотрении проблем защиты данных в сети прежде всего возникает вопрос о

классификации сбоев и нарушений прав доступа, которые могут привести к уничтожению или нежелательной модификации данных. Среди таких потенциальных "угроз" можно выделить:

1. Сбои оборудования:

- сбои кабельной системы;

- перебои электропитания;

- сбои дисковых систем;

- сбои систем архивации данных;

- сбои работы серверов, рабочих станций, сетевых карт и т. д.;

2. Потери информации из-за некорректной работы ПО:

- потеря или изменение данных при ошибках ПО;

- потери при заражении системы компьютерными вирусами;

3. Потери, связанные с несанкционированным доступом:

- несанкционированное копирование, уничтожение или подделка информации;

- ознакомление с конфиденциальной информацией, составляющей тайну, посторонних лиц;

4. Потери информации, связанные с неправильным хранением архивных данных.

5. Ошибки обслуживающего персонала и пользователей.

- случайное уничтожение или изменение данных;

- некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных.

В зависимости от возможных видов нарушений работы сети (под нарушением работы мы также понимаем и несанкционированный доступ) многочисленные виды защиты информации объединяются в два основных класса:

- средства физической защиты, включающие средства защиты кабельной системы, систем электропитания, средства архивации, дисковые массивы и т. д.

- программные средства защиты, в том числе: антивирусные программы, системы разграничения полномочий, программные средства контроля доступа.

- административные меры защиты, включающие контроль доступа в помещения, разработку стратегии безопасности фирмы, планов действий в чрезвычайных ситуациях и т.д.

Следует отметить, что подобное деление достаточно условно, поскольку современные технологии развиваются в направлении сочетания программных и аппаратных средств защиты. Наибольшее распространение такие программно-аппаратные средства получили, в частности, в области контроля доступа, защиты от вирусов и т. д.

Системы архивирования и дублирования информации

Организация надежной и эффективной системы архивации данных является одной из важнейших задач по обеспечению сохранности информации в сети. В небольших сетях, где установлены один-два сервера, чаще всего применяется установка системы архивации непосредственно в свободные слоты серверов. В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер.

Такой сервер автоматически производит архивирование информации с жестких дисков серверов и рабочих станций в указанное администратором локальной вычислительной сети время, выдавая отчет о проведенном резервном копировании. При этом обеспечивается управление всем процессом архивации с консоли администратора, например, можно указать конкретные тома, каталоги или отдельные файлы, которые необходимо архивировать. Возможна также организация автоматического архивирования по наступлении того или иного события ("event driven backup"), например, при получении информации о том, что на жестком диске сервера или рабочей станции осталось мало свободного места, или при выходе из строя одного из "зеркальных" дисков на файловом сервере. Среди наиболее распространенных моделей архивационных серверов можно выделить Storage Express System корпорации Intel, ARCserve for Windows, производства фирмы Cheyenne и ряд других.

Хранение архивной информации, представляющей особую ценность, должно быть

организовано в специальном охраняемом помещении. Специалисты рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании, на случай пожара или стихийного бедствия. Для обеспечения восстановления данных при сбоях магнитных дисков в последнее время чаще всего применяются системы дисковых массивов - группы дисков, работающих как единое устройство, соответствующих стандарту RAID (Redundant Arrays of Inexpensive Disks).

Защита от компьютерных вирусов

Вряд ли найдется хотя бы один пользователь или администратор сети, который бы ни разу не сталкивался с компьютерными вирусами. По данным исследования, проведенного фирмой Creative Strategies Research, 64% из 451 опрошенного специалиста испытали "на себе" действие вирусов [3]. На сегодняшний день дополнительно к тысячам уже известных вирусов появляется 100-150 новых штаммов ежемесячно. Наиболее распространенными методами защиты от вирусов по сей день остаются различные антивирусные программы.

Однако в качестве перспективного подхода к защите от компьютерных вирусов в последние годы все чаще применяется сочетание программных и аппаратных методов защиты. Среди аппаратных устройств такого плана можно отметить специальные антивирусные платы, которые вставляются в стандартные слоты расширения компьютера. Корпорация Intel в 1994 году предложила перспективную технологию защиты от вирусов в компьютерных сетях. Flash-память сетевых адаптеров Intel EtherExpress PRO/10 содержит антивирусную программу, сканирующую все системы компьютера еще до его загрузки.

Автор: Александр
26.08.2014 15:48

Защита от несанкционированного доступа

Проблема защиты информации от несанкционированного доступа особо обострилась с широким распространением локальных и, особенно, глобальных компьютерных сетей (рис. 2). Необходимо также отметить, что зачастую ущерб наносится не из-за "злого умысла", а из-за элементарных ошибок пользователей, которые случайно портят или удаляют жизненно важные данные. В связи с этим, помимо контроля доступа, необходимым элементом защиты информации в компьютерных сетях является разграничение полномочий пользователей.

В компьютерных сетях при организации контроля доступа и разграничения полномочий пользователей чаще всего используются встроенные средства сетевых операционных систем

Исследования практики функционирования систем обработки данных и вычислительных систем показали, что существует достаточно много возможных направлений утечки информации и путей несанкционированного доступа в системах и сетях. В их числе:

· чтение остаточной информации в памяти системы после выполнения санкционированных запросов;

· копирование носителей информации и файлов информации с преодолением мер защиты;

· маскировка под зарегистрированного пользователя;

· маскировка под запрос системы;

· использование программных ловушек;

· использование недостатков операционной системы;

· незаконное подключение к аппаратуре и линиям связи;

· злоумышленный вывод из строя механизмов защиты;

· внедрение и использование компьютерных вирусов.

Обеспечение безопасности информации в ВС и в автономно работающих ПЭВМ достигается комплексом организационных, организационно-технических, технических и программных мер.

К организационным мерам защиты информации относятся:

· ограничение доступа в помещения, в которых происходит подготовка и обработка информации;

· допуск к обработке и передаче конфиденциальной информации только проверенных должностных лиц;

· хранение магнитных носителей и регистрационных журналов в закрытых для доступа посторонних лиц сейфах;

· исключение просмотра посторонними лицами содержания обрабатываемых материалов через дисплей, принтер и т.д.;

· использование криптографических кодов при передаче по каналам связи ценной информации;

· уничтожение красящих лент, бумаги и иных материалов, содержащих фрагменты ценной информации.

Организационно-технические меры защиты информации включают:

· осуществление питания оборудования, обрабатывающего ценную информацию от независимого источника питания или через специальные сетевые фильтры;

· установку на дверях помещений кодовых замков;

· использование для отображения информации при вводе-выводе жидкокристаллических или плазменных дисплеев, а для получения твёрдых копий - струйных принтеров и термопринтеров, поскольку дисплей даёт такое высокочастотное электромагнитное излучение, что изображение с его экрана можно принимать на расстоянии нескольких сотен километров;

· уничтожение информации, хранящейся в ПЗУ и на НЖМД, при списании или отправке ПЭВМ в ремонт;

· установка клавиатуры и принтеров на мягкие прокладки с целью снижения возможности снятия информации акустическим способом;

· ограничение электромагнитного излучения путём экранирования помещений, где происходит обработка информации, листами из металла или из специальной пластмассы.

Технические средства защиты информации - это системы охраны территорий и помещений с помощью экранирования машинных залов и организации контрольно-пропускных систем. Защита информации в сетях и вычислительных средствах с помощью технических средств реализуется на основе организации доступа к памяти с помощью:

· контроля доступа к различным уровням памяти компьютеров;

· блокировки данных и ввода ключей;

· выделение контрольных битов для записей с целью идентификации и др.

Архитектура программных средств защиты информации включает:

· контроль безопасности, в том числе контроль регистрации вхождения в систему, фиксацию в системном журнале, контроль действий пользователя;

· реакцию (в том числе звуковую) на нарушение системы защиты контроля доступа к ресурсам сети;

· контроль мандатов доступа;

· формальный контроль защищённости операционных систем (базовой общесистемной и сетевой);

· контроль алгоритмов защиты;

· проверку и подтверждение правильности функционирования технического и программного обеспечения.

Для надёжной защиты информации и выявления случаев неправомочных действий проводится регистрация работы системы: создаются специальные дневники и протоколы, в которых фиксируются все действия, имеющие отношение к защите информации в системе. Фиксируются время поступления заявки, её тип, имя пользователя и терминала, с которого инициализируется заявка. При отборе событий, подлежащих регистрации, необходимо иметь в виду, что с ростом количества регистрируемых событий затрудняется просмотр дневника и обнаружение попыток преодоления защиты. В этом случае можно применять программный анализ и фиксировать сомнительные события. Используются также специальные программы для тестирования системы защиты. Периодически или в случайно выбранные моменты времени они проверяют работоспособность аппаратных и программных средств защиты.

К отдельной группе мер по обеспечению сохранности информации и выявлению несанкционированных запросов относятся программы обнаружения нарушений в режиме реального времени. Программы данной группы формируют специальный сигнал при регистрации действий, которые могут привести к неправомерным действиям по отношению к защищаемой информации. Сигнал может содержать информацию о характере нарушения, месте его возникновения и другие характеристики. Кроме того, программы могут запретить доступ к защищаемой информации или симулировать такой режим работы (например, моментальная загрузка устройств ввода-вывода), который позволит выявить нарушителя и задержать его соответствующей службой.

Один из распространённых способов защиты - явное указание секретности выводимой информации. В системах, поддерживающих несколько уровней секретности, вывод на экран терминала или печатающего устройства любой единицы информации (например, файла, записи и таблицы) сопровождается специальным грифом с указанием уровня секретности. Это требование реализуется с помощью соответствующих программных средств.

Автор: Александр
26.08.2014 15:48

В отдельную группу выделены средства защиты от несанкционированного использования программного обеспечения. Они приобретают особое значение вследствие широкого распространения ПК.

Оснастив сервер или сетевые рабочие станции, например, устройством чтения смарт-карточек и специальным программным обеспечением, можно значительно повысить степень защиты от несанкционированного доступа. В этом случае для доступа к компьютеру пользователь должен вставить смарт-карту в устройство чтения и ввести свой персональный код. Программное обеспечение позволяет установить несколько уровней безопасности, которые управляются системным администратором. Возможен и комбинированный подход с вводом дополнительного пароля, при этом приняты специальные меры против "перехвата" пароля с клавиатуры. Этот подход значительно надежнее применения паролей, поскольку, если пароль подглядели, пользователь об этом может не знать, если же пропала карточка, можно принять меры немедленно.

Смарт-карты управления доступом позволяют реализовать, в частности, такие функции, как контроль входа, доступ к устройствам персонального компьютера, доступ к программам, файлам и командам. Кроме того, возможно также осуществление контрольных функций, в частности, регистрация попыток нарушения доступа к ресурсам, использования запрещенных утилит, программ, команд DOS.

Одним из удачных примеров создания комплексного решения для контроля доступа в открытых системах, основанного как на программных, так и на аппаратных средствах защиты, стала система Kerberos. В основе этой схемы авторизации лежат три компонента:

- База данных, содержащая информацию по всем сетевым ресурсам, пользователям, паролям, шифровальным ключам и т.д.

- Авторизационный сервер (authentication server), обрабатывающий все запросы пользователей на предмет получения того или иного вида сетевых услуг. Авторизационный сервер, получая запрос от пользователя, обращается к базе данных и определяет, имеет ли пользователь право на совершение данной операции. Примечательно, что пароли пользователей по сети не передаются, что также повышает

степень защиты информации.

- Ticket-granting server (сервер выдачи разрешений) получает от авторизационного сервера "пропуск", содержащий имя пользователя и его сетевой адрес, время запроса и ряд других параметров, а также уникальный сессионный ключ. Пакет, содержащий "пропуск", передается также в зашифрованном по алгоритму DES виде. После получения и расшифровки "пропуска" сервер выдачи разрешений проверяет запрос и сравнивает ключи и затем дает "добро" на использование сетевой аппаратуры или программ.

Среди других подобных комплексных схем можно отметить разработанную Европейской Ассоциацией Производителей Компьютеров (ECMA) систему Sesame. (Secure European System for Applications in Multivendor Environment), предназначенную для использования в крупных гетерогенных сетях.

защита информации, передаваемой по каналам удаленного доступа, требует особого подхода.

В частности, в мостах и маршрутизаторах удаленного доступа применяется сегментация пакетов - их разделение и передача параллельно по двум линиям, - что делает невозможным "перехват" данных при незаконном подключении "хакера" к одной из линий. К тому же используемая при передаче данных процедура сжатия передаваемых пакетов гарантирует невозможность расшифровки "перехваченных" данных. Кроме того, мосты и маршрутизаторы удаленного доступа могут быть запрограммированы таким образом, что удаленные пользователи будут ограничены в доступе к отдельным ресурсам сети главного офиса.

Разработаны и специальные устройства контроля доступа к компьютерным сетям по коммутируемым линиям. Например, фирмой AT&T предлагается модуль Remote Port Security Device (PRSD), представляющий собой два блока размером с обычный модем: RPSD Lock (замок), устанавливаемый в центральном офисе, и RPSD Key (ключ), подключаемый к модему удаленного пользователя. RPSD Key и Lock позволяют установить несколько уровней защиты и контроля доступа, в частности:

- шифрование данных, передаваемых по линии при помощи генерируемых цифровых ключей;

- контроль доступа в зависимости от дня недели или времени суток (всего 14 ограничений).

Широкое распространение радиосетей в последние годы поставило разработчиков радиосистем перед необходимостью организации защиты информации от "хакеров", вооруженных разнообразными сканирующими устройствами. Были применены разнообразные технические решения. Например, в радиосети компании RAM Mobil Data информационные пакеты передаются через разные каналы и базовые станции, что делает практически невозможным для посторонних собрать всю передаваемую информацию воедино [4]. Активно используются в радиосетях и технологии шифрования данных при помощи алгоритмов DES и RSA.

Механизмы обеспечения безопасности

1. Криптография.

Для обеспечения секретности применяется шифрование, или криптография, позволяющая трансформировать данные в зашифрованную форму, из которой извлечь исходную информацию можно только при наличии ключа.

Системам шифрования столько же лет, сколько письменному обмену информацией.

Автор: Александр
26.08.2014 15:48

“Криптография” в переводе с греческого языка означает “тайнопись”, что вполне отражает её первоначальное предназначение. Примитивные (с позиций сегодняшнего дня) криптографические методы известны с древнейших времён и очень длительное время они рассматривались скорее как некоторое ухищрение, чем строгая научная дисциплина. Классической задачей криптографии является обратимое преобразование некоторого понятного исходного текста (открытого текста) в кажущуюся случайной последовательность некоторых знаков, называемую шифртекстом или криптограммой. При этом шифр-пакет может содержать как новые, так и имеющиеся в открытом сообщении знаки. Количество знаков в криптограмме и в исходном тексте в общем случае может различаться. Непременным требованием является то, что, используя некоторые логические замены символов в шифртексте, можно однозначно и в полном объёме восстановить исходный текст. Надёжность сохранения информации в тайне определялось в далёкие времена тем, что в секрете держался сам метод преобразования.

Прошли многие века, в течении которых криптография являлась предметом избранных - жрецов, правителей, крупных военачальников и дипломатов. Несмотря на малую распространённость использование криптографических методов и способов преодоления шифров противника оказывало существенное воздействие на исход важных исторических событий. Известен не один пример того, как переоценка используемых шифров приводила к военным и дипломатическим поражениям. Несмотря на применение криптографических методов в важных областях, эпизодическое использование криптографии не могло даже близко подвести её к той роли и значению, которые она имеет в современном обществе. Своим превращением в научную дисциплину криптография обязана потребностям практики, порождённым электронной информационной технологией.

Пробуждение значительного интереса к криптографии и её развитие началось с XIX века, что связано с зарождением электросвязи. В XX столетии секретные службы большинства развитых стран стали относится к этой дисциплине как к обязательному инструменту своей деятельности.

В основе шифрования лежат два основных понятия: алгоритм и ключ. Алгоритм - это способ закодировать исходный текст, в результате чего получается зашифрованное послание. Зашифрованное послание может быть интерпретировано только с помощью ключа.

Очевидно, чтобы зашифровать послание, достаточно алгоритма.

Автор: Александр
26.08.2014 15:48

Голландский криптограф Керкхофф (1835 - 1903) впервые сформулировал правило: стойкость шифра, т.е. криптосистемы - набора процедур, управляемых некоторой секретной информацией небольшого объёма, должна быть обеспечена в том случае, когда криптоаналитику противника известен весь механизм шифрования за исключением секретного ключа - информации, управляющей процессом криптографических преобразований. Видимо, одной из задач этого требования было осознание необходимости испытания разрабатываемых криптосхем в условиях более жёстких по сравнению с условиями, в которых мог бы действовать потенциальный нарушитель. Это правило стимулировало появление более качественных шифрующих алгоритмов. Можно сказать, что в нём содержится первый элемент стандартизации в области криптографии, поскольку предполагается разработка открытых способов преобразований. В настоящее время это правило интерпретируется более широко: все долговременные элементы системы защиты должны предполагаться известными потенциальному злоумышленнику. В последнюю формулировку криптосистемы входят как частный случай систем защиты. В этой формулировке предполагается, что все элементы систем защиты подразделяются на две категории - долговременные и легко сменяемые. К долговременным элементам относятся те элементы, которые относятся к разработке систем защиты и для изменения требуют вмешательства специалистов или разработчиков. К легко сменяемым элементам относятся элементы системы, которые предназначены для произвольного модифицирования или модифицирования по заранее заданному правилу, исходя из случайно выбираемых начальных параметров. К легко сменяемым элементам относятся, например, ключ, пароль, идентификация и т.п. Рассматриваемое правило отражает тот факт, надлежащий уровень секретности может быть обеспечен только по отношению к легко сменяемым элементам.

Несмотря на то, что согласно современным требованиям к криптосистемам они должны выдерживать криптоанализ на основе известного алгоритма, большого объёма известного открытого текста и соответствующего ему шифртекста, шифры, используемые специальными службами, сохраняются в секрете. Это обусловлено необходимостью иметь дополнительный запас прочности, поскольку в настоящее время создание криптосистем с доказуемой стойкостью является предметом развивающейся теории и представляет собой достаточно сложную проблему. Чтобы избежать возможных слабостей, алгоритм шифрования может быть построен на основе хорошо изученных и апробированных принципах и механизмах преобразования. Ни один серьёзный современный пользователь не будет полагаться только на надёжность сохранения в секрете своего алгоритма, поскольку крайне сложно гарантировать низкую вероятность того, что информация об алгоритме станет известной злоумышленнику.

Секретность информации обеспечивается введением в алгоритмы специальных ключей

(кодов). Использование ключа при шифровании предоставляет два существенных преимущества. Во-первых, можно использовать один алгоритм с разными ключами для отправки посланий разным адресатам. Во-вторых, если секретность ключа будет нарушена, его можно легко заменить, не меняя при этом алгоритм шифрования. Таким образом, безопасность систем шифрования зависит от секретности используемого ключа, а не от секретности алгоритма шифрования. Многие алгоритмы шифрования являются общедоступными.

Количество возможных ключей для данного алгоритма зависит от числа бит в ключе. Например, 8-битный ключ допускает 256 (2^8) комбинаций ключей. Чем больше возможных комбинаций ключей, тем труднее подобрать ключ, тем надёжнее зашифровано послание. Так, например, если использовать 128-битный ключ, то необходимо будет перебрать 2^{128} ключей, что в настоящее время не под силу даже самым мощным компьютерам. Важно отметить, что возрастающая производительность техники приводит к уменьшению времени, требующегося для вскрытия ключей, и системам обеспечения безопасности приходится использовать всё более длинные ключи, что, в свою очередь, ведёт к увеличению затрат на шифрование.

Поскольку столь важное место в системах шифрования уделяется секретности ключа, то основной проблемой подобных систем является генерация и передача ключа. Существуют две основные схемы шифрования: симметричное шифрование (его также иногда называют традиционным или шифрованием с секретным ключом) и шифрование с открытым ключом (иногда этот тип шифрования называют асимметричным).

При симметричном шифровании отправитель и получатель владеют одним и тем же ключом (секретным), с помощью которого они могут зашифровывать и расшифровывать данные.При симметричном шифровании используются ключи небольшой длины, поэтому можно быстро шифровать большие объёмы данных. Симметричное шифрование используется, например, некоторыми банками в сетях банкоматов. Однако симметричное шифрование обладает несколькими недостатками. Во-первых, очень сложно найти безопасный механизм, при помощи которого отправитель и получатель смогут тайно от других выбрать ключ. Возникает проблема безопасного распространения секретных ключей. Во-вторых, для каждого адресата необходимо хранить отдельный секретный ключ. В третьих, в схеме симметричного шифрования невозможно гарантировать личность отправителя, поскольку два пользователя владеют одним ключом.

В схеме шифрования с открытым ключом для шифрования послания используются два

различных ключа. При помощи одного из них послание зашифровывается, а при помощи второго - расшифровывается. Таким образом, требуемой безопасности можно добиваться, сделав первый ключ общедоступным (открытым), а второй ключ хранить только у получателя (закрытый, личный ключ). В таком случае любой пользователь может зашифровать послание при помощи открытого ключа, но расшифровать послание способен только обладатель личного ключа. При этом нет необходимости заботиться о безопасности передачи открытого ключа, а для того чтобы пользователи могли обмениваться секретными сообщениями, достаточно наличия у них открытых ключей друг друга.

Недостатком асимметричного шифрования является необходимость использования более длинных, чем при симметричном шифровании, ключей для обеспечения эквивалентного уровня безопасности, что сказывается на вычислительных ресурсах, требуемых для организации процесса шифрования.

Электронная подпись

Если послание, безопасность которого мы хотим обеспечить, должным образом зашифровано, всё равно остаётся возможность модификации исходного сообщения или подмены этого сообщения другим. Одним из путей решения этой проблемы является передача пользователем получателю краткого представления передаваемого сообщения. Подобное краткое представление называют контрольной суммой, или дайджестом сообщения.

Контрольные суммы используются при создании резюме фиксированной длины для представления длинных сообщений. Алгоритмы расчёта контрольных сумм разработаны так, чтобы они были по возможности уникальны для каждого сообщения. Таким образом, устраняется возможность подмены одного сообщения другим с сохранением того же самого значения контрольной суммы.

Однако при использовании контрольных сумм возникает проблема передачи их получателю. Одним из возможных путей её решения является включение контрольной суммы в так называемую электронную подпись.

При помощи электронной подписи получатель может убедиться в том, что полученное им сообщение послано не сторонним лицом, а имеющим определённые права отправителем. Электронные подписи создаются шифрованием контрольной суммы и дополнительной информации при помощи личного ключа отправителя. Таким образом, кто угодно может расшифровать подпись, используя открытый ключ, но корректно создать подпись может только владелец личного ключа. Для защиты от перехвата и повторного использования подпись включает в себя уникальное число - порядковый номер.

Аутентификация

Аутентификация является одним из самых важных компонентов организации защиты информации в сети. Прежде чем пользователю будет предоставлено право получить тот или иной ресурс, необходимо убедиться, что он действительно тот, за кого себя выдаёт.

При получении запроса на использование ресурса от имени какого-либо пользователя сервер, предоставляющий данный ресурс, передаёт управление серверу аутентификации. После получения положительного ответа сервера аутентификации пользователю предоставляется запрашиваемый ресурс.

При аутентификации используется, как правило, принцип, получивший название “что он знает”, - пользователь знает некоторое секретное слово, которое он посылает серверу

аутентификации в ответ на его запрос. Одной из схем аутентификации является использование стандартных паролей. Пароль - совокупность символов, известных подключенному к сети абоненту, - вводится им в начале сеанса взаимодействия с сетью, а иногда и в конце сеанса (в особо ответственных случаях пароль нормального выхода из сети может отличаться от входного). Эта схема является наиболее уязвимой с точки зрения безопасности - пароль может быть перехвачен и использован другим лицом. Чаще всего используются схемы с применением одноразовых паролей. Даже будучи перехваченным, этот пароль будет бесполезен при следующей регистрации, а получить следующий пароль из предыдущего является крайне трудной задачей. Для генерации одноразовых паролей используются как программные, так и аппаратные генераторы, представляющие собой устройства, вставляемые в слот компьютера. Знание секретного слова необходимо пользователю для приведения этого устройства в действие.

Одной из наиболее простых систем, не требующих дополнительных затрат на оборудование, но в то же время обеспечивающих хороший уровень защиты, является S/Key, на примере которой можно продемонстрировать порядок представления одноразовых паролей.

В процессе аутентификации с использованием S/Key участвуют две стороны - клиент и сервер. При регистрации в системе, использующей схему аутентификации S/Key, сервер присылает на клиентскую машину приглашение, содержащее зерно, передаваемое по сети в открытом виде, текущее значение счётчика итераций и запрос на ввод одноразового пароля, который должен соответствовать текущему значению счётчика итерации. Получив ответ, сервер проверяет его и передаёт управление серверу требуемого пользователю сервиса.

Защита сетей

В последнее время корпоративные сети всё чаще включаются в Интернет или даже используют его в качестве своей основы. Учитывая то, какой урон может принести

незаконное вторжение в корпоративную сеть, необходимо выработать методы защиты. Для защиты корпоративных информационных сетей используются брандмауэры. Брандмауэры - это система или комбинация систем, позволяющие разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую. Как правило, эта граница проводится между локальной сетью предприятия и INTERNETOM, хотя её можно провести и внутри. Однако защищать отдельные компьютеры невыгодно, поэтому обычно защищают всю сеть. Брандмауэр пропускает через себя весь трафик и для каждого проходящего пакета принимает решение - пропускать его или отбросить. Для того чтобы брандмауэр мог принимать эти решения, для него определяется набор правил.

Брандмауэр может быть реализован как аппаратными средствами (то есть как отдельное физическое устройство), так и в виде специальной программы, запущенной на компьютере.

Как правило, в операционную систему, под управлением которой работает брандмауэр, вносятся изменения, цель которых - повышение защиты самого брандмауэра. Эти изменения затрагивают как ядро ОС, так и соответствующие файлы конфигурации. На самом брандмауэре не разрешается иметь разделов пользователей, а следовательно, и потенциальных дыр - только раздел администратора. Некоторые брандмауэры работают только в однопользовательском режиме, а многие имеют систему проверки целостности программных кодов.

Брандмауэр обычно состоит из нескольких различных компонентов, включая фильтры или экраны, которые блокируют передачу части трафика.

Все брандмауэры можно разделить на два типа:

· пакетные фильтры, которые осуществляют фильтрацию IP-пакетов средствами фильтрующих маршрутизаторов;

· серверы прикладного уровня, которые блокируют доступ к определённым сервисам в сети.

Таким образом, брандмауэр можно определить как набор компонентов или систему, которая располагается между двумя сетями и обладает следующими свойствами:

· весь трафик из внутренней сети во внешнюю и из внешней сети во внутреннюю должен пройти через эту систему;

· только трафик, определённый локальной стратегией защиты, может пройти через эту систему;

· система надёжно защищена от проникновения.

4. Требования к современным средствам защиты информации.

Согласно требованиям гостехкомиссии России средства защиты информации от несанкционированного доступа(СЗИ НСД), отвечающие высокому уровню защиты, должны обеспечивать:

· дискреционный и мандатный принцип контроля доступа;

· очистку памяти;

· изоляцию модулей;

· маркировку документов;

· защиту ввода и вывода на отчуждаемый физический носитель информации;

· сопоставление пользователя с устройством;

· идентификацию и аутентификацию;

· гарантии проектирования;

· регистрацию;

· взаимодействие пользователя с комплексом средств защиты;

· надёжное восстановление;

· целостность комплекса средств защиты;

· контроль модификации;

· контроль дистрибуции;

· гарантии архитектуры;

Комплексные СЗИ НСД должны сопровождаться пакетом следующих документов:

· руководство по СЗИ;

· руководство пользователя;

· тестовая документация;

· конструкторская (проектная) документация.

Таким образом, в соответствии с требованиями гостехкомиссии России комплексные СЗИ НСД должны включать базовый набор подсистем. Конкретные возможности этих подсистем по реализации функций защиты информации определяют уровень защищённости средств вычислительной техники. Реальная эффективность СЗИ НСД определяется функциональными возможностями не только базовых, но и дополнительных подсистем, а также качеством их реализации.

Компьютерные системы и сети подвержены широкому спектру потенциальных угроз информации, что обуславливает необходимость предусмотреть большой перечень функций и подсистем защиты. Целесообразно в первую очередь обеспечить защиту наиболее информативных каналов утечки информации, каковыми являются следующие:

· возможность копирования данных с машинных носителей;

· каналы передачи данных;

· хищение ЭВМ или встроенных накопителей.

Проблема перекрытия этих каналов усложняется тем, что процедуры защиты данных не должны приводить к заметному снижению производительности вычислительных систем. Эта задача может быть эффективно решена на основе технологии глобального шифрования информации, рассмотренной в предыдущем разделе.

Современная массовая система защиты должна быть эргономичной и обладать такими свойствами, благоприятствующими широкому её применению, как:

· комплексность - возможность установки разнообразных режимов защищённой обработки данных с учётом специфических требований различных пользователей и предусматривать широкий перечень возможных действий предполагаемого нарушителя;

· совместимость - система должна быть совместимой со всеми программами, написанными для данной операционной системы, и должна обеспечивать защищённый режим работы компьютера в вычислительной сети;

· переносимость - возможность установки системы на различные типы компьютерных систем, включая портативные;

· удобство в работе - система должна быть проста в эксплуатации и не должна менять привычную технологию работы пользователей;

· работа в масштабе реального времени - процессы преобразования информации, включая шифрование, должны выполняться с большой скоростью;

· высокий уровень защиты информации;

· минимальная стоимость системы.

Автор: Александр
26.08.2014 15:48

Вслед за массовым применением современных информационных технологий криптография вторгается в жизнь современного человека. На криптографических методах основано применение электронных платежей, возможность передачи секретной информации по открытым сетям связи, а также решение большого числа других задач защиты информации в компьютерных системах и информационных сетях. Потребности практики привели к необходимости массового применения криптографических методов, а следовательно к необходимости расширения открытых исследований и разработок в этой области. Владение основами криптографии становится важным для учёных и инженеров, специализирующихся в области разработки современных средств защиты информации, а также в областях эксплуатации и проектирования информационных и телекоммуникационных систем.

Одной из актуальных проблем современной прикладной криптографии является разработка скоростных программных шифров блочного типа, а также скоростных устройств шифрования.

В настоящее время предложен ряд способов шифрования, защищённых патентами Российской Федерации и основанных на идеях использования:

· гибкого расписания выборки подключений;

· генерирования алгоритма шифрования по секретному ключу;

· подстановок, зависящих от преобразуемых данных.