4 Забезпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

УДК 681.06

ВОПРОСЫ БЕЗОПАСНОСТИ И ПУТИ ИХ РЕШЕНИЯ В СОВРЕМЕННЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Игорь Нетесин
Международный научный центр технологии программирования ТЕХНОСОФТ НАН Украины и Госкомитета по связи и информатизации, г. Киев

Анотація: **В роботі розглядаються основні питання безпеки та напрямки їх вирішення у сучаних комп'ютерних системах і мережах. Наведені фактори, що загрожують безпеці мережі, програмним об'єктам та автоматизованим і інформаційним системам обробки даних, що функціонують у мережі. Визначені основні загальносистемні засоби безпеки та захисту інформації у деяких сучасних розподілених системах.**
Summary: **This paper represents the basic problems of safety and security, the ways of their decision in modern computer systems and networks. The facts threated to safety, program objects and automatization and information systems of data processing are discussed. The general system means of the information safety and security in modern distributed systems are defined. The conclusions are given.**
Ключові слова: **Безопасность, компьютерная сеть, факторы безопасности, авторизация, аутентификация, шифрование.**

В связи с интенсивным использованием распределенных систем, локальных и глобальных компьютерных сетей (КС) одним из основных вопросов создания автоматизированных и информационных систем является обеспечение циркулирующей в них информации техническими и программными средствами безопасности и защиты [1,2]. Наиболее общими чертами, характеризующими состояние обеспеченности безопасности сети, являются:

наличие сетевых и общесистемных средств безопасности;
существование реальных угроз безопасной работы сети;
недостаточное внимание разработчиков программ и пользователей сети вопросам защиты информации.

Рассмотрению этих особенностей и других вопросов безопасности, а также путей их решения разными разработчиками общесистемных и сетевых услуг посвящена данная работа.

I Определение общих задач обеспечения безопасности сети

Обеспечением безопасности называется аспект управления, связанный с предоставлением авторизованного (санкционированного) доступа к данным, устройствам, программам и другим компонентам КС. Основными гарантиями безопасности сети является:

доступность к сетевым компонентам, информации и службам только авторизованных пользователей;

конфиденциальность одних пользователей располагать соответствующими полномочиями, которыми не располагают другие;

целостность и сохранность компонентов и информации, их защита от похищения, повреждения или уничтожения посторонними воздействиями или из-за некомпетентности обслуживающего персонала.

Гарантия безопасности достигается сетевыми и специальными компонентами программного обеспечения (ПО), средствами обработки информации и спецоборудованием сети (например, спецсредства защиты в компьютерно-телефонных сетях [3]).

Объектам сети и ее пользователям обычно угрожают некоторые факторы, вероятность возникновения и возможность предотвращения которых носит, как правило, непредвиденный характер. Например, если неавторизованное (несанкционированное) лицо похитит сетевое имя одного из объектов и соответствующий ему пароль, то вызванная этим угроза свидетельствует не только о нарушении защиты сети, но и том, что данная КС становится небезопасной. Ниже рассмотрим три основных вида угроз, которые нарушают сетевую, программную и информационную безопасность.

1.1 Угроза сетевой среде. Классифицируется по элементам сети, которым угрожает нарушение безопасности и включает ряд факторов.

Внутренний фактор. Связан с элементами сети, их неправильным функционированием или выходом из строя (например, поломка вентилятора может привести к перегреву компьютера и к возможной потере части информации).

Внешний фактор. Воздействие на КС объекта, находящегося вне ее (например, человек с магнитом).

Преднамеренный (активный) фактор. Специальное и целенаправленное действие, приводящее к потере, искажению, похищению информации или частичному повреждению объектов КС. К таким факторам относятся: шпионаж, диверсия, компьютерные вирусы, взламывание хакерами защищенных файлов или программ, а также несанкционированное извлечение информации из авторизованных данных или сообщений.

Непреднамеренный фактор. Действия, которые связаны с различными природными явлениями, угрожающими КС (авария, землетрясение, наводнение и т.п.).

1.2 Угроза программным объектам. К факторам, угрожающим программным объектам ÏÎ (приложениям, ОС, сервисным процедурам и т.п.) КС относятся:

случайное или преднамеренное уничтожение программы;

похищение программы путем копирования неавторизованным пользователем;

искажение программ вирусами или неправильной входной информацией;

возникновение программных ошибок, приводящих к искажению программ или данных.

Одним из способов борьбы с такими угрозами является использование специальных сетевых процедур, которые обеспечивают безопасность и защиту, а также обнаружение угрожающих факторов и связанных с ними ошибок. Так как работа программных объектов в сети, как правило, заключается в обработке информации, в том числе параметров конфигурации системы, файлов данных, параметров взаимодействия объектов (процедур), то для некоторых из них необходимо обеспечить защиту.

1.3 Угроза информационным объектам. Безопасности информации угрожают следующие факторы:

случайное или преднамеренное уничтожение файлов баз данных;

замена параметров запросов путем перехвата, последствия от которого могут быть обнаружены не сразу;

похищение информации с мест ее хранения специальной аппаратурой и другими устройствами;

потеря данных при сбоях в сети или ошибках в самих программных объектах;

искажение передаваемых по сети данных путем подмены другой информацией.

Некоторые из приведенных факторов обнаруживаются с помощью сетевых процедур контроля или других средств обнаружения ошибок. В настоящее время в состав сетевых процедур входят программы защиты от вирусов и от несанкционированного доступа. Кроме того, разрабататываются дополнительные меры по обеспечению безопасности современных КС:

физическая защита оборудования от угрожающих факторов (наводнений, пожаров и др.);

логическая защита информации с помощью специальных микросхем, устанавливаемых на сетевые интерфейсные платы;

хранение ключей шифрования в местах, недоступных из сети;

использование резервного сервера, который может взять на себя функции управления сетью при выходе из строя основного сервера;

копирование ценной информации с применением в узлах сети специальных сетевых интерфейсных плат и сохранение копий и паролей отдельно от основных данных;

контроль передаваемых запросов и их хранение в специальных областях;

полное протоколирование всех сетевых действий, выполняемых процессами или пользователями, а также предупреждение попыток несанкционированного подключения к сети;

ограничение доступа к определенным файлам и каталогам сети, а также к паролям и идентификаторам;

применение новых контролирующих технологий, кодов аутентификации сообщений, гарантирующих отправку сообщения и надежную ее защиту от перехватов и искажений.

В компьютерных системах и сетях в основном существует пять путей, допускающих возможность применения нелегальных действий с угрозами для ее безопасности:

доступ к данным и программам;

изменение данных;

пользование услугами и программами;

блокирование услуг;

недопустимость входа в сеть (impersonation)

От первых трех видов нелегальных действий средства защиты предусмотрены практически во всех современных сетях. Охарактеризуем остальные.

Блокирование - это действие, затрудняющее авторизованным лицам пользоваться услугами сети. Например, одновременная отправка с одного узла множества запросов ко всем принтерам КС приводит к тупиковым ситуациям (timeout) и, следовательно, к небезопасной работе сети. К этому понятию примыкает также генерация ложных (spoofing) сообщений с одного узла другим узлам сети, чтобы завести эти узлы в заблуждение, в результате чего сеть становится неработоспособной и небезопасной.

Недопустимый вход в сеть - это ложное задание подлинности автора, посылающего запрос. Одним из способов борьбы с подобными действиями является использование серверов с контрольными функциями и процедурами, предупреждающими возникновение такого рода угрозы.

II Подходы к обеспечению безопасности в современных распределенных системах общего назначения

К настоящему времени получили широкое распространение клиент-серверные системы общего назначения, предоставляющие пользователям богатый набор сервисов обслуживания запросов, хранения и ведения объектов в общих хранилищах-репозиториях, взаимодействия удаленно расположенных программных компонентов, обмена данными и т.п. Эти средства являются базисом для разработчиков компонентных и объектно-ориентированных приложений, освобождая их от создания собственных сервисных и системных средств обслуживания распределенных приложений [4].

К *программным средствам* относятся специальные сетевые процедуры и функции безопасности, выполняющие: проверку параметров аутентификации в запросах, их принадлежность зарегистрированным пользователям; контроль паролей, ассоциированных с подлинными именами пользователей системы; анализ доступа к программам и данным авторизованными и неавторизованными пользователями; проверка паролей и частоты их использования и изменения.

Разные категории пользователей с помощью этих средств могут провести анализ их вхождений в сеть и сформировать ограничения, которых необходимо придерживаться при работе в сети.

К *организационным средствам* относятся службы, занимающиеся внедрением технических средств защиты в сетевые инфраструктуры, определением новых способов шифрования и формированием разговорных ключей, наблюдением за системными таблицами, фиксирующими все циркулирующие сообщения с целью обнаружения разного рода нарушений, угрожающих безопасности КС.

Под *административными средствами* понимаются мероприятия специалистов (администраторов) сферы обслуживания КС по проведению политики и мер безопасности. Им предоставляются специальные серверы, с помощью которых проверяются:

пароли пользователей, их минимальная и максимальная длина;

частота изменения паролей;

списки использованных паролей;

типы доступов (в том числе удаленных и гостевых) и предоставляемых пользователям паролей.

К классу систем с приведенными средствами и мероприятиями по организации безопасности относятся: OSF DCE [5], Sun RPC [6], CORBA [7], COM [8] и др.

Дадим краткую характеристику особенностей организации служб безопасности и защиты в этих системах.

2.1 Распределенная система OSF DCE (Open Software Foundation Distributed Computing Environment). В этой системе имеется служба безопасности, которая располагается на одном из серверов, защищенном физически и программно от подключения к нему произвольных пользователей. Основные требования в данной службе к обеспечению безопасности следующие:

пароль является единственным средством проверки подлинности пользователя, который ассоциируется с регистрационным именем;

пользователь регистрируется только один раз, после чего имеет доступ к службам сети;

доступ к сетевому сервису основывается на гибкой системе проверки личности пользователя с правом на защиту информации;

ключ для шифрования и расшифровки единственен для каждого пользователя.

Служба безопасности DCE состоит из трех подсистем (подслужб): аутентификации, авторизации и контроля доступа.

Служба аутентификации обеспечивает установку подлинности личности пользователя. Основу аутентификации составляет метод шифрования информации с секретным ключом. При регистрации пользователя одновременно генерируется соответствующий ему разговорный ключ (Conversation key). Специальная система (Private Attribute Certificate) выдает сертификат, в котором указывается авторизованная информация, категория пользователя и билет (ticket), позволяющий запрашивать услугу у сервера.

Важное место занимают средства передачи протоколов путем совершенствования средств ведения списков контроля доступа, а также передачи поручений другим серверам. Предпринимаются также шаги по реализации задач шифрования с применением публичного ключа с помощью программных и технических средств (например, устройство Clipper Chip для аппаратного шифрования).

Служба авторизации базируется на информации, содержащейся в сертификате атрибутов привилегий, которая включает сообщение для обращения к некоторому ресурсу сети, например к распределенной БД.

Последняя содержит описание входов для зарегистрированных категорий пользователей, имен групп (совокупности пользователей) и организаций. Каждое зарегистрированное имя и пользователь принадлежат некоторой организации, где они работают. Существуют системы протоколирования изменений авторизованной информации с целью отслеживания причин разных инцидентов в сети.

Служба контроля доступа реализована с помощью системного списка контроля доступа, который определяется для каждого узла сети и для системы в целом. В нем указываются категории зарегистрированных пользователей и допустимые для них операции. Как правило, эти списки первоначально создают разработчики приложений, погружаемых в среду распределенной системы, после чего их список передается менеджеру в системный список контроля доступа.

В целом система безопасности OSF DCE предоставляет надежные механизмы защиты и обладает большей степенью безопасности, чем другие распределенные системы обработки данных.

2.2 Распределенная система RPC (Remote Procedure Call) Sun Microsystems. В системе реализованы механизмы аутентификации (установка подлинности личности), которые базируются на стандарте кодирования данных DES (Data Encryption Standard). Эти механизмы поддерживаются специальной системной службой безопасности.

Тип аутентификации идентифицируется уникальным именем (номером), присваиваемым при входе в систему для регистрации. С каждым типом связываются верительные данные, которые идентифицируют личность пользователя (фамилия, адрес, место проживания и др.) и верификатор этих данных (например, фото личности, задавшей верительные данные).

В качестве верительных данных используются также: имя машины, идентификатор пользователя (группы), список групп. При загрузке системы с указанием имени машины пользователь становится привилегированным, а имя - уникальным сетевым именем для всех машин сети. Никто другой не может воспользоваться этим именем.

В качестве верификатора используется и штамп времени (время таймера при отправке клиентом запроса серверу). Сервер раскодирует этот штамп, сравнивает его с ключом переговоров и проверяет, чтобы значение штампа времени было больше, чем в предыдущем запросе, и чтобы это время не истекло (не вышло за интервал действия верительных данных клиента). Верительные данные не признаются системой, если указанные условия не выполнены.

Для обеспечения большей безопасности (секретности) в системе поддерживается DES-аутентификация с публичными ключами, которые присваиваются администратором сети. Секретные ключи дешифруются при регистрации пароля автоматически. С целью гарантии использования этих ключей к сетевому имени добавляется еще имя ОС, в которой пользователь работает и посылает запросы в сеть.

Все основные функции по обеспечению безопасности приложения выполняет специально создаваемый монитор безопасности, размещаемый на сервере системы. Последний взаимодействует с общей службой безопасности системы.

2.3 Система брокера объектных запросов - CORBA (Common Object Request Broker Architecture). Система поддерживает объектный подход к проектированию приложений и предоставляет мощный набор средств по защите объектов и запросов, посылаемых по сети друг другу. В основу этих средств положена стандартная модель защиты, определяющая базовую политику безопасности и которая включает:

условия, при которых объектам разрешается взаимодействовать или иметь доступ к ресурсам;

идентификацию пользователей, подтверждающую личность пользователя и его права;

безопасность взаимосвязей между объектами, включая доверие между ними и качество защиты передаваемых данных объектам, распределенным по сетевым узлам;

виды деятельности, способствующие обеспечению безопасности.

Согласно этой модели брокер объектных запросов анализирует параметры аутентификации в запросах к объектам и обращается к соответствующим функциям системы защиты для контроля доступа и проверки условий безопасности параметров взаимодействия. Если запрос правильный, то вызывается соответствующая подслужба безопасности, которая обеспечивает защищенную передачу запроса серверу.

Стратегия защиты. Включает авторизованную модель и модель контроля доступа вызываемых объектов, которые распределены в разных узлах сети. Этот вызов осуществляется через интерфейс объектов, содержащий описание всех методов и операций объектов.

За установку прав доступа одного объекта к другому отвечает администратор сети, от имени которого может выступать и клиент. Он проверяет такие параметры объекта: подлинность псевдонимов, доступ к контролируемому списку зарегистрированных пользователей, полномочия авторизованного пользователя и др. Выделяется несколько привилегированных атрибутов, которые известны системе и администратору, осуществляющему их выборку и изменение. Для обеспечения взаимного доверия между клиентом и объектом используются такие механизмы защиты, как аутентификация и использование разговорных или публичных ключей защиты.

Стратегия контроля доступа. Базируется на модели контроля доступа и системных функциях проверки: разрешения доступа; текущих привилегий и атрибутов целевых объектов, определенных администратором или

объектом; времени отправки вызова; выполнения операций над объектами и др. При этих проверках используются авторизованная модель и контрольный список схем доступа, отображающие зарегистрированных авторизованных пользователей системы. Эта модель содержит описание привилегированных атрибутов, переменных для контроля доступа и релевантной информации об операциях, данных и их контекстах. Именно эта информация дает возможность контролировать имена привилегированных атрибутов и операций над ними.

Особенностью обеспечения безопасности в системе CORBA является применение:

стратегии, критериев и правил авторизованной защиты;

доверительных данных и информации об объектах, которые не могут вмешиваться в другие объекты и сами должны быть защищены от них;

секретной технологии со специальными механизмами защиты.

Эти средства могут использоваться при необходимости организовать секретность и защищенность объектов и данных распределенных приложений сети.

2.4 Модель распределенных объектов - DCOM (Distributed Component Object Model) фирмы Microsoft. Данная модель лежит в основе большинства новых средств, создаваемых из компонентов известными фирмами: Digital Equipment Corporation, Siemens, Silicon Graphic, Sap и др. Существенным достижением в развитии этой модели является подсистема MTS (Microsoft Transaction Server), предоставляющая разные виды услуг по прохождению транзакций в сетевой среде, средств их защиты и обеспечения безопасности объектных приложений. Данные средства безопасности базируются на понятии роли (role-based security), которой пользуются разработчики приложений при определении различных классов полномочий на прикладном уровне вместо существующих средств на низком уровне. Разработка начинается с авторизации, т.е. с описания ролей и разрешенных им действий с определенными компонентами, интерфейсами и методами в пределах приложения. Доступ к таким объектам управляется системой MTS.

III Выводы

Проведенный анализ возможностей создания разного рода угроз безопасной работы распределенных систем и способов их предупреждения с помощью сетевых и общесистемных средств поддержки разработки ПО (фирм Microsoft, Sun Microsystems, OSF DCE и др.) позволяет сделать вывод о том, что полной гарантии безопасного выполнения ПО пока достичь не удается. В основном эти средства реализуют такие способы обеспечения безопасности, как авторизация, аутентификация и шифрование. Несмотря на то, что эти средства реализованы по-разному и в некоторой степени затрудняют интероперабельности ПО, имеются и общие способы поддержки защиты - единство структуры системных списков доступа и семантики процедур формирования разговорных ключей. Сходство некоторых задач безопасности и защиты информации создает основу для переноса разрабатываемых приложений в другие современные среды с гарантией защиты от несанкционированного доступа к данным и передаваемым сообщениям. Существенный вклад в рассматриваемую проблематику вносят и новые технические и программные средства защиты данных серверов баз данных.

Литература: 1. Гроувер А. Защита программного обеспечения. - М: Мир, 1992. 2. Герасименко В.А. Комплексная защита информации в современных системах обработки информации. - Зарубежная радиоэлектроника, 1993.- N2. - с. 35-38. 3. Байгер В.М., Готовский А.В., Коляда С.В. Методы и средства эффективной защиты информации в корпоративных системах связи, построенных на базе цифровых УПАТС CORAL.- Труды Ювілейної науково-технічної конференції « Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні».- Київ, 9 - 11 червня 1998р.- с.168 -172. 4. Вельбицкий И.В., Ершов С.В., Нетесин И.Е., Голубь С.В. Технология программирования распределенных объектно-ориентированных систем. - Киев, 1996.-Препринт 96-15. - НАН Украины, МНЦТП ТЕХНОСОФТ.- ИК НАН Украины, 21с. 5. Open Software Foundation. Introduce to Open Software Foundation. Distributed Computer Environments.- Englewood Cliffs, N.J.: Prentice Hall, 1992. -437 p. 6. Corbin J. The art of distributed applications. Programming Tech. for Remote Procedure Calls. - Berlin. - Springer Verlag. - 1992. - 305 c. 7. Siegel J. CORBA Fundamentals and Programming, Wiley Co. Publ. Group, John Wiley & Sons, Inc. -USA.-1996.- 694p. 8. Роджерсон Д. Основы COM. - Microsoft Press. - Русский перевод. - Microsoft Corporation, 1997. - 350с.