Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 4 (107)/2002

Обеспечение информационной безопасности в вычислительных комплексах на базе мэйнфреймов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Обеспечение информационной безопасности в вычислительных комплексах на базе мэйнфреймов

Сергей Симонов, Павел Колдышев

СОДЕРЖАНИЕ

1. Введение

Лет 30-40 назад информационные системы строились только на базе мэйнфреймов. Соответственно, архитектура информационной системы, как правило, была централизованной. Затем наступила эра малых машин, распределенных архитектур обработки информации. Мэйнфреймы были практически полностью вытеснены из небольших и средних информационных систем, однако, сохранили достаточно прочные позиции в крупных системах с повышенными требованиями к доступности и целостности данных.

С точки зрения информационной безопасности (ИБ), основными особенностями современных мэйнфреймов являются:

- **Надежность**. Мэйнфреймы могут изолировать и исправлять большинство аппаратных и программных ошибок. Среднее время наработки на отказ оценивается в 12-15 лет.
- **Дублирование**. Предусмотрена возможность установки резервных процессоров и микросхем памяти.
- **Альтернативные пути доступа к периферийным устройствам**. Горячая замена всех элементов вплоть до каналов, плат памяти и центральных процессоров.
- **Механизмы обеспечения целостности данных**. Ошибки не приводят к разрушению данных в памяти или данных, ожидающих ввода-вывода. Подсистемы хранения данных, построенные на основе RAID-массивов и средств резервного копирования, способны эффективно защитить от потери данных.
- **Масштабирование** может быть как вертикальным так и горизонтальным. Вертикальное масштабирование обеспечивается линейкой процессоров с производительностью от 200 до 3000 MIPS и наращиванием до 20 центральных процессоров в одном компьютере. Горизонтальное масштабирование реализуется объединением ЭВМ в Parallel Sysplex — многомашинный кластер, выглядящий с точки зрения пользователя единым компьютером. Программное масштабирование — на одном мэйнфрейме может быть сконфигурировано большое число различных серверов, изолированных друг от друга так, как будто они работают на отдельных выделенных компьютерах; в тоже время они могут совместно использовать аппаратные и программные ресурсы и данные.
- **Отработанные механизмы обеспечения информационной безопасности**. Такие средства, как криптографические сопроцессоры или средства защиты операционных систем (например, RACF или VM:SECURE), позволяют обеспечивать весьма высокий уровень защищенности информационных систем.

В России мэйнфреймы успешно работают в ряде ведомственных систем. При проектировании новых крупных информационных систем с повышенными требованиями в области ИБ, специалисты зачастую склоняются к использованию мэйнфреймов. Однако при проектировании подсистем безопасности все же возникает ряд проблем, основными из которых являются:

- Реализация криптографической защиты, соответствующей отечественным стандартам.
- Оценка «штатных» механизмов безопасности с позиции требований отечественных стандартов и РД.

Ниже рассматриваются наиболее существенные аспекты, возникающие при обеспечении режима ИБ информационных систем, построенных на вычислительной технике с архитектурой S/390.

При написании данного материала использовалась информация, доступная в интернет:

- [1], [2] — описание архитектуры безопасности и сервера безопасности;
- [3] — документация по операционным системам.
- Некоторые дополнительные материалы по теме публикации на русском языке имеются на сервере компании «УСП Компьюлинк» [4],[5].

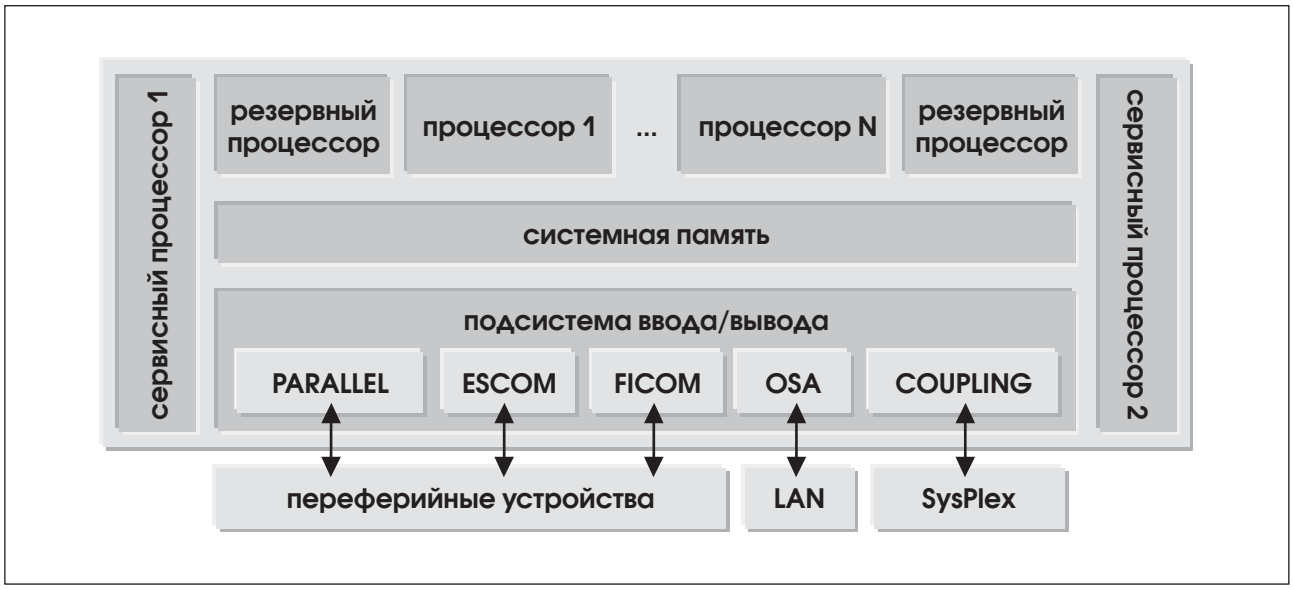

Рис.1. Упрощенная структурная схема мэйнфреймов с архитектурой S/390

2. Архитектура IBM S/390

Упрощенная структурная схема мэйнфреймов с архитектурой S/390 приведена на рис. 1.

Внутри процессорного модуля расположены процессоры, оперативная память и канальная подсистема. Последняя обеспечивает операции ввода/вывода и является главной отличительной чертой архитектуры мэйнфреймов, так как разгружает от этих операций внутренние шины данных. Канальная подсистема состоит из интерфейсных устройств (каналов) трёх типов — параллельного и двух последовательных: ESCON (Enterprise System CONnection) и FICON (FIber CONnection), обеспечивающих скорость передачи до 100 Мбайт/с.

Каналы соединяются с периферийными устройствами напрямую или через неблокирующий коммутатор пересечений — ESCON или FICON Director. Он может иметь до 124 портов, обеспечивая между любыми двумя портами одновременно до 62 соединений. Один порт Director может быть подключен к ЭВМ, а остальные — к периферийным устройствам, что аналогично непосредственному подключению к каналу ЭВМ. Периферийное устройство может быть подключено к множеству каналов, в том числе от разных ЭВМ. ESCON каналы обеспечивают передачу данных на расстояние до 9 километров, FICON — до 100 км и более; при использовании аппаратных удлинителей эти цифры могут быть ещё большими.

PR/SM (Processor Resource/Systems Manager) обеспечивает логическое разделение ресурсов компьютера на несколько самостоятельных машин (LPAR), обеспечивающих одновременное выполнение различных операционных систем на одной ЭВМ — от 4 до 20, в зависимости от модели. В последних моделях процессоров IBM PR/SM дополнен Intelligent Resource Director (IRD), позволяющим динамически перераспределять мощности процессорного комплекса и канальной подсистемы между LPAR. Таким образом обеспечивается максимальная загрузка каналов и практически исключается вероятность потери связи с абонентом по вине аппаратуры центральной части системы.

Для каналов ESCON возможно также совместное использование канальных путей разными LPAR с помощью компонента EMIF (ESCON Multiple Images Facility).

Канальная подсистема обеспечивает возможность «горячего подключения» кабелей. Dynamic reconfiguration management (управление динамическим переконфигурированием) позволяет вносить динамические изменения в конфигурацию ввода/вывода, избавляя от необходимости перезапуска системы, чтобы изменить «представление» процессора о конфигурации ввода/вывода. Эту возможность использует функция интерактивного определения конфигурации оборудования (Hardware Configuration Definition, HCD); она также может динамически обновлять определения конфигурации ввода/вывода в операционной системе.

В архитектуру S/390 введены специальные аппаратные средства для подключения ЭВМ непосредственно к сетям ATM, Ethernet (включая Fast и Gigabit), TokenRing и FDDI — полнодуплексный адаптер OSA (Open Systems Adapter). OSA обеспечивает взаимодействие SNA/APPN, TCP/IP и IPX — клиентов с ресурсами сервера S/390. Приложения

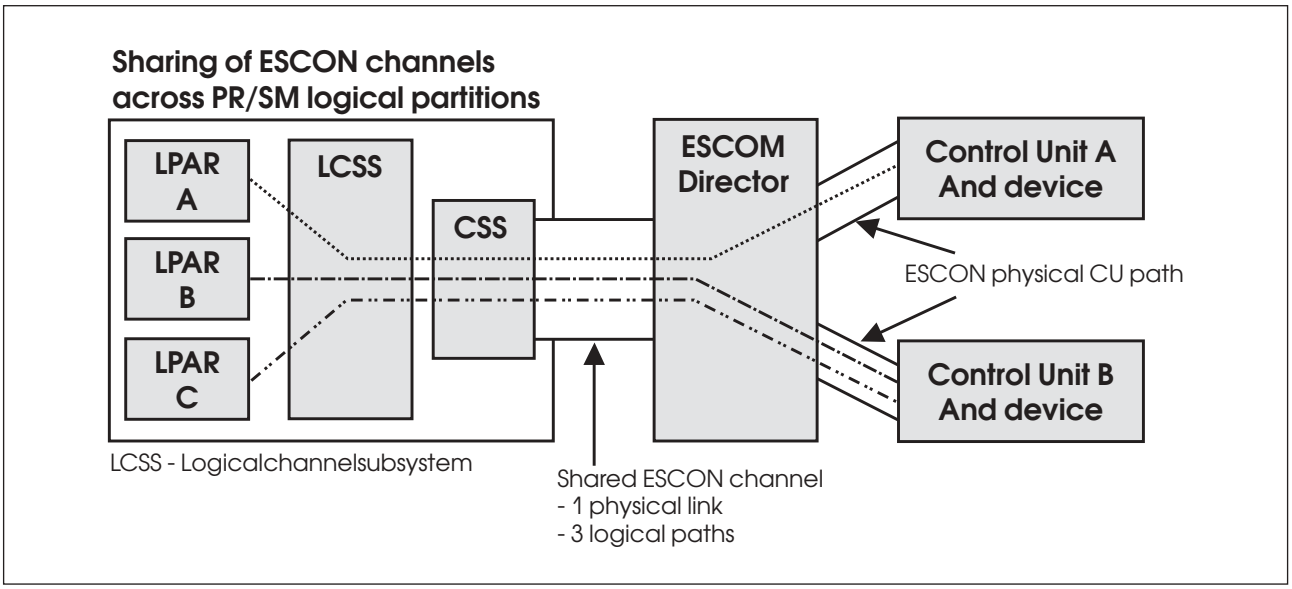

Рис. 2. Совместное использование ESCON-каналов

TCP/IP и SNA/APPN могут получать доступ к сервисным функциям через один и тот же порт адаптера OSA; также эти адаптеры могут разделяться между LPAR. Всего через OSA может быть подключено до 32 FDDI сетей, 16 сетей TokenRing и 16 — Ethernet.

Управление подсистемой памяти выполняет страничный супервизор ОС при поддержке аппаратных средств виртуализации адресного пространства и страничной защиты данных. Для преобразования виртуального адреса в реальный используются таблицы сегментов и таблицы страниц, а также управляющий регистр базы, содержащий указатель на адресное пространство или регистр доступа, указывающий на пространство данных. В случае, если при обращении к данному виртуальному адресу выясняется, что соответствующая строка таблицы страниц указывает на отсутствие страницы в оперативной памяти, генерируется прерывание. Подкачка этой страницы в оперативную память из области страничного обмена на дисках (paging) включает также вытеснение страниц оперативной памяти в область накопления. Благодаря этой технологии область адресации доведена до 16 Тбайт.

Еще одна особенность S/390 — схема защиты памяти подсистемы. Оперативная память имеет схемы с автоматической коррекцией одинарных ошибок и обнаружением кратных ошибок на уровне 4-х байтных слов. Для обеспечения целостности информации все страницы оперативной памяти защищены 7-битным ключом защиты памяти, так что любая программа для получения доступа к этой странице должна предъявить соответствующий ключ. Обычные прикладные программы используют ключ 8, а защита их друг от друга обеспечивается путем размещения их в различных адресных пространствах, имеющих свои таблицы страниц. «n-процессорная» параллельная архитектура — Parallel Sysplex позволяет наращивать мощность за счет параллелизма, создавать кластеры, реализующие концепцию централизованного управления распределенными системами. Все машины кластера могут разделять данные, рабочую нагрузку и системные ресурсы. Приложения передаются другому члену кластера при сбое или при запланированном выключении. Аппаратура кластера включает оборудование связывания — IBM-9674 Coupling Facility, предоставляющее общую память всем машинам кластера, IBM-9037 Sysplex Timer, — обеспечивающий синхронизацию отсчета времени на всех ЭВМ комплекса, и Coupling Link — высокоскоростные каналы связи ЭВМ.

2.1. z/Architecture – следующий шаг в развитии мэйнфреймов

Объявленная IBM в октябре 2000 года 64-разрядная архитектура z/Architecture обладает рядом дополнительных преимуществ по сравнению с S/390. Быстродействие компьютеров этой архитектуры может достигать 2,5 млн. команд в секунду (MIPS) — на целых 50% больше, чем в предшествующих моделях S/390 Generation 6. Так как 2-гигабайтное ограничение на объем памяти теперь снято (объём адресуемой памяти может достигать 16 экзабайт), отпала и необходимость в расширенной памяти (Expanded Storage, ES), применявшейся для быстрого кэширования, — в результате устранены непроизводительные издержки, возникавшие за счет

перемещения страниц памяти из Central Storage в Expanded Storage. Быстродействие процессоров z900 на 25—40% выше, чем у их предшественников — процессоров G6. Подсистема ввода-вывода z900 также была модернизирована с целью привести ее возможности в соответствие с большим числом процессоров, увеличением их быстродействия возросшим объемом физической памяти. Корпорации IBM удалось утроить максимальное число каналов ввода/вывода FICON — с 32 до 96 и улучшить их быстродействие, в результате максимальная пропускная способность каналов z900 возрасла до 24 Гб/с, по сравнению с 8 Гб/с в случае процессора G6. В состав z900 входит новый каркас для плат с 28 разъемами (nI/O), предназначенный для плат ESCON, FICON и OSA-Express. Все платы стандарта nI/O допускают «горячую» замену.

Каждая отдельная система z900 рассчитана на сведение нарушений работы к минимуму. Помимо исключительно высокой надежности компонентов оборудования (представители IBM заявляют, что среднее время наработки оборудования на отказ составляет десятилетия), сервер z900 обеспечивает правильность функционирования программного обеспечения благодаря вычислительным модулям с дублированием команд (Dual-Instruction Execution Unit). К прочим функциональным возможностям относятся резервирование микросхем памяти (Memory Chip Sparing) и динамическое резервирование ЦПУ (Dynamic CPU Sparing). Когда количество поддающихся исправлению ошибок какой-либо микросхемы памяти превышает некоторое заранее определенное число, система автоматически заменяет дефектную микросхему на запасную. Если же откажет чип ЦП и повторная попытка выполнить команду окажется безуспешной, то всегда найдется по крайней мере одна запасная микросхема, способная возобновить исполнение программы в точности с той команды, на которой произошел сбой.

Разработав платформу z900, корпорация IBM тем самым взяла на вооружение новую концепцию организации вычислительной среды, отличную от семейств Unix-серверов (E10000 производства Sun и Superdome производства HP). Поставщики Unix-систем обычно рекламируют возможности создания разделов и наращивания вычислительной мощности по запросу при использовании своих систем для задач электронной коммерции. При этом, однако, этим серверам не хватает способности z900 динамически перемещать ресурсы между приложениями в зависимости от рабочей нагрузки.

2.2. Обеспечение отказоустойчивости

Архитектура мэйнфреймов IBM содержит арсенал средств, обеспечивающих целостность данных, восстановление и поддержание восстановления вычислительного процесса в случае ошибок или сбоев как в оборудовании, так и в системном программном обеспечении. Современные дисковые подсистемы реализуют различные уровни RAID-архитектуры для защиты данных при физической порче носителя (DASD media failure).

Наивысшая отказоустойчивость достигается при использовании Parallel Sysplex — тогда процент времени доступности системы достигает 99,999%, что является наивысшим показателем среди всех компьютерных систем.

Центральные процессоры имеют двойной набор исполнительных устройств, которые выполняют одну и ту же операцию, после чего результаты сравниваются и, в случае их несовпадения, операция повторяется. ЭВМ могут комплектоваться специальным резервным процессором, подхватывающим рабочую нагрузку «на лету» при выходе из строя одного из основных процессоров.

2.3. Операционные системы мэйнфреймов IBM

На мэйнфреймах IBM развивается несколько линий операционных систем. Линия ОС в настоящее время представлена такими системами, как OS/390 и z/OS. Эти операционные системы отличает высочайшая надежность, использование всех возможностей аппаратной среды. Основное бизнес-предназначение этих систем — сервера больших и сверхбольших СУБД и связанные с ними системы онлайновых транзакций (OLTP).

Набирающая все большую популярность линия операционных систем Linux также нашла свое место на мэйнфреймах IBM — существует уже ряд дистрибутивов Linux для этой платформы. Эта система предназначена для выполнения серверных задач среднего уровня — серверов приложений, электронной почты, Web. Благодаря использованию архитектуры мэйнфреймов, на одном физическом процессорном устройстве могут одновременно работать до десятки тысяч образов Linux, что является мощнейшим средством консолидации серверов. Один мэйнфрейм может заменить огромное количество отдельно стоящих компьютеров, например Sun или HP, резко уменьшая накладные расходы на их поддержку и упрощая администрирование.

Линия Систем Виртуальных Машин VM представлена операционными системами VM/ESA

и z/VM. Эти системы позволяют организовывать так называемые виртуальные машины, независимые друг от друга, на которых можно запускать другие, «гостевые», операционные системы. VM в настоящее время используется, в основном, для поддержания работы большого количества образов Linux на одном процессорном устройстве.

Поскольку линия VM в настоящее время рассматривается как вспомогательная, а Linux не обеспечивает многих необходимых функций безопасности, в дальнейшем будет рассматриваться защита информации на примере OS/390 — флагмана операционных систем для мэйнфреймов.

3. Особенности обеспечения информационной безопасности на платформе S/390

Для информационных систем, построенных на вычислительной технике с архитектурой S/390, имеется возможность разделения ресурсов процессора на логические части — LPAR, позволяющие работать независимым операционным системам даже на однопроцессорной машине. Сертифицированно по европейскому стандарту безопасности OS/390 по уровню E4 — аналог B2 в США, что соответствует выполнению требования на «отдельно стоящие устройства».

Одним из основных компонентов операционной системы OS/390 является Сервер безопасности (Security Server), базирующийся на RACF — Resource Access Control Facility. Вследствие интеграции Unix-оболочки в OS/390, ряд стандартных компонентов Unix, обладающих своими элементами обеспечения информационной безопасности, был перенесен в OS/390 (например, LDAP, DCE), и элементы безопасности этих компонентов стали частью Сервера безопасности.

Ряд компонентов подсистемы безопасности реализован в других системных компонентах. Это связано, во-первых, с историческим наследием операционной системы OS/390, во-вторых, с многообразием задач обеспечения безопасности. Все эти компоненты взаимодействуют с RACF.

Рассмотрим основные элементы подсистемы безопасности в OS/390.

4. RACF– базовая составляющая подсистемы безопасности

RACF (*Resourse Access Control Facility*) обеспечивает защиту информационных ресурсов системы и администрирование средств защиты. Каждому пользователю системы присваивается идентификатор **RACF** (*RACF user ID*) и пароль — (*RACF user password*) или его эквивалент, при помощи которого проверяется достоверность идентификатора пользователя, в том числе обеспечивается поддержка пользователей и групп пользователей среды Unix.

Объекты системы, такие как команды, наборы данных, тома магнитной ленты, терминалы и другие объекты, в том числе определённые администратором, могут быть защищены от несанкционированного доступа при помощи средств **RACF**.

4.1. Задачи и принципы работы

Задачами RACF являются:

- идентификация и аутентификация пользователей;
- интеграция управления безопасностью системы и всех приложений;
- обеспечение возможности централизации управления информационной безопасностью для комплексов машин, как расположенных локально, так и удаленных друг от друга;
- обеспечение возможности доступа к защищенным ресурсам только авторизованным пользователям;

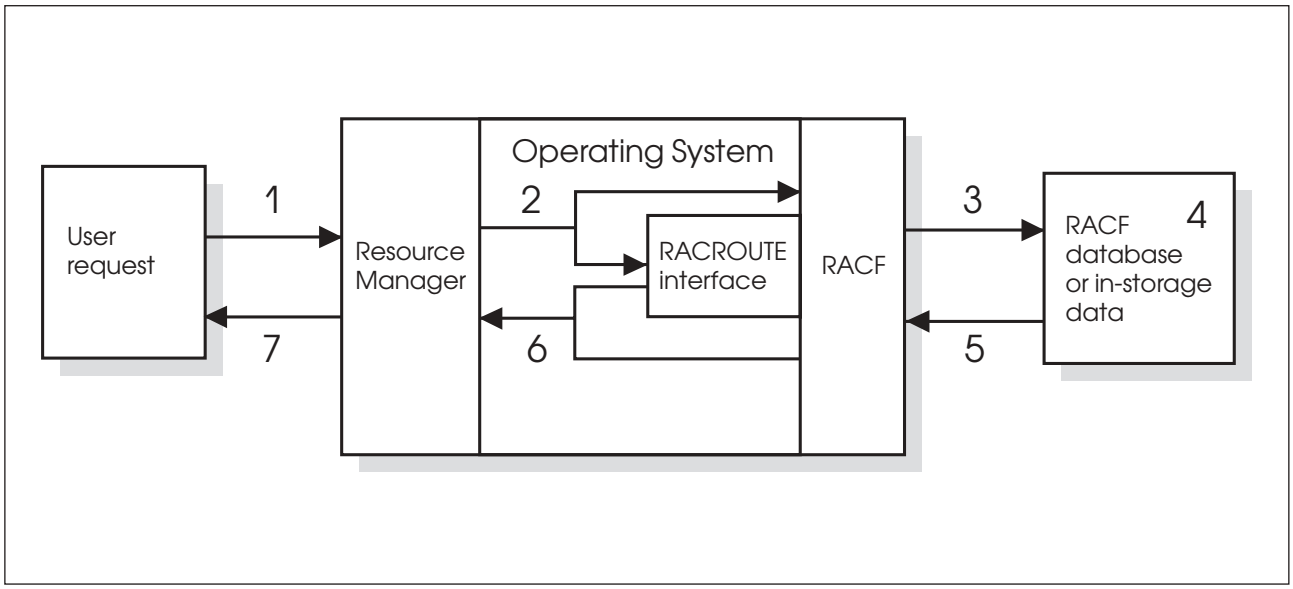

Рис. 3. Взаимодействие RACF с операционной системой

- обеспечение возможности определения прав пользователей и защищенных ресурсов одним или несколькими администраторами, примеры приведены ниже;
  - обеспечение автоматической защиты ресурса при его создании;
  - обеспечение возможности создания интерфейса к программным продуктам других производителей;
  - хранение информации о защищенных ресурсах и правах пользователей в зашифрованном виде, а также обеспечение надежности хранения этой информации;
  - протоколирование и аудит доступа к защищенным ресурсам;
  - обеспечение возможности просмотра списка защищенных ресурсов, уровней их защиты, списка и прав пользователей для администраторов.

RACF выполняет эти задачи следующим образом (рис. 3). Запрос на доступ к определенному ресурсу от пользователя поступает к приложению-менеджеру ресурсов (например, TSO или JES) (1). Менеджер ресурсов выдает запрос RAC на авторизацию пользователя на доступ к ресурсу (2). RACF обращается к своей базе данных (3). База данных RACF организована таким образом, что часть ее хранится на томе прямого доступа, а часть (более часто используемая) непосредственно в памяти (4). После проверки соответствующего профиля и авторизации пользователя на доступ (5), RACF возвращает менеджеру ресурсов код завершения (6), который обрабатывается менеджером ресурсов, и последний разрешает или запрещает доступ (7).

Права доступа RACF разграничивает так, что, после того как пользователь (или группа пользователей) зарегистрирован в системе, только он один имеет доступ к своим данным (если политика прав доступа не определена как-то иначе). Даже администратор не имеет возможности получения чужой информации, если не оговорено соответствующих прав. Конечно, он может попытаться это сделать, удалив пользователя или его пароль, а потом восстановив эту информацию, но такие действия будут обнаружены либо самим пользователем, либо через аудит.

RACF является ядром реализованной в OS/390 концепции политики защиты данных в масштабе предприятия и интегрируется в различное окружение. Например, если на платформе OS/390 реализован сервер Web, то RACF обеспечивает взаимодействие с протоколом SSL. Сертификат SSL будет обработан, отождествлен с записями в базе данных, после чего сервер безопасности даст или не даст разрешение на передачу данных по пользовательскому запросу.

Таким образом, для обеспечения защиты информации необходимо, чтобы менеджер ресурсов мог взаимодействовать с RACF — формировать запросы, обрабатывать ответы и предпринимать в соответствии с полученными ответами некоторые действия. Все приложения, входящие в OS/390 способны взаимодействовать с RACF. Программные продукты сторонних производителей должны либо поддерживать интерфейс с RACF, либо обеспечивать свои способы защиты информации. Многие из

подобных программных продуктов обеспечивают оба перечисленных варианта защиты. Это относится и к ряду компонентов OS/390. Например, Web-сервер для OS/390 позволяет ограничивать права доступа пользователей к определенным разделам сайта как с использованием RACF, так и с использованием классической системы аутентификации, используемой в Web-серверах для Unix (файл паролей).

Вся информация по защите RACF хранится в его базе данных. По умолчанию, пароли в базе RACF хранятся в зашифрованном виде в соответствии с алгоритмом DES. Обращение к этой базе происходит всякий раз, когда пользователь RACF входит в систему либо когда появляется запрос на доступ к защищенному ресурсу. При инициализации подсистемы RACF наиболее часто используемая информация переносится из базы данных в память. Для перезаписи информации в памяти существуют специальные функции. База данных RACF может содержаться как в одном, так и в нескольких дисковых наборах, может быть общей для нескольких систем и может иметь backup-копию для горячего переключения в случае неисправности основной базы данных. С использованием средства RACF Remote Sharing Facility (RRSF) возможно управление и синхронизация удаленных друг от друга баз данных RACF. Связь между системами при этом осуществляется по протоколу APPC архитектуры SNA. Записи базы данных RACF, касающиеся наборов данных и ресурсов, содержат также специальные поля, указывающие правила аудита, поэтому отследить все обращения (в первую очередь, попытки со стороны лиц или процессов, не имеющих на то права) к особо важным объектам не составляет никакого труда.

Существует возможность изменения алгоритма шифрования паролей, хранящихся в базе данных RACF. Для этого используются программы выхода. Вместо алгоритма DES можно использовать алгоритм маскирования паролей (использовавшийся в более ранних версиях RACF) либо подключить собственный уникальный алгоритм.

Посредством программ выхода можно также наложить дополнительные ограничения на пароль пользователя, например, по длине или содержанию.

4.1.1. Пользователи и группы

Пользователи RACF объединены в группы. При этом пользователь может быть определен в нескольких группах; многие системные приложения при идентификации пользователя позволяют ввести также и идентификатор группы, к которой пользователь будет относиться при работе с данным приложением.

Среди групп пользователей существует изначальная группа SYS1, создаваемая на этапе инсталляции RACF. Все остальные группы имеют вышестоящую группу, образуя, таким образом, иерархическое дерево. Авторизация на доступ к ресурсу для пользователя, входящего в группу, при отсутствии специальных назначений для пользователя, равна авторизации группы. Для каждой группы можно определить так называемые сегменты приложений (для DFP, OMVS, OVM и TME), определяющие характеристики по умолчанию по работе с данным приложением для пользователей, входящих в группу.

Каждая группа имеет своего владельца, указываемого при создании группы. Владелец имеет наивысшие права по управлению группой: может создавать, присоединять или удалять из группы пользователей, менять параметры группы, управлять подчиненными группами и предоставлять пользователям группы авторизацию по отношению к группе. Вариантов такой авторизации четыре: USE, CREATE, CONNECT и JOIN, каждая последующая является более «сильной», чем предыдущая и включает все возможности предыдущей. С помощью распределения авторизации по отношению к группе, владелец группы может разделять между пользователями группы задачи администрирования группы.

Группам пользователей можно сопоставлять физические терминалы или рабочие станции с тем, чтобы пользователи, входящие в группу, могли входить в систему только с определенных рабочих мест.

Подобно группам, каждый пользователь имеет своего владельца и, кроме того, для него могут быть определены сегменты приложений. Для пользователя таких сегментов может быть определено 12 — для CICS, DCE, DFP, OMVS, TSO и других приложений. Кроме этого, пользователь может иметь следующие атрибуты:

- SPECIAL — авторизация на управление всеми профилями RACF;
- AUDITOR — авторизация на команды и утилиты, обеспечивающие протоколирование и аудит;
- OPERATIONS — авторизация на полный доступ к защищенным ресурсам определенных типов, в частности, к защищенным RACF наборам данных;
- CLAUTH — авторизация на создание профилей в определенном классе защиты;
- REVOKE — запрет пользователю на вход в систему;
- GRPACC — обеспечение доступности всех профилей защиты наборов данных, созданных пользователем, для членов его группы;

- ADSP — обеспечение автоматической защиты RACF всех создаваемых пользователем наборов данных.

Для доступа к защищенному ресурсу пользователь, в общем случае, должен указать пароль. Возможно использование идентификационных карт (OIDCARD) при работе со специального терминала. В целях обеспечения дополнительной защиты, доступ пользователя к системе может быть ограничен по времени и дням недели. В случае использования суррогатных пользователей (если активен класс защиты SURROGAT), возможно выполнение определенных функций одним пользователем «от имени» другого без указания пароля (это необходимо для некоторых системных и прикладных задач).

4.1.2. Классы и профили защиты ресурсов

Ресурсы, защищаемые RACF, объединены в классы защиты. Класс объединяет однотипные ресурсы. Для каждого защищенного ресурса внутри класса создается профиль защиты. Каждый класс защиты может быть активизирован и деактивизирован, позволяя таким образом включить или выключить защиту ресурсов определенного типа. При инсталляции системы ряд классов предопределен, кроме этого, существует возможность добавления новых классов. Посредством предопределенных классов можно определить для RACF ресурсы следующих типов:

- набор данных;
- команда операционной системы;
- имя Logical Unit (LU) для соединений APPC;
- операторская консоль;
- периферийное устройство;
- определенная функция определенной задачи, утилиты, подсистемы;
- том прямого доступа или магнитной ленты;
- файл спула;
- программа (загрузочный модуль);
- терминал

и многие другие.

При определении профилей защиты RACF для них указывается, в частности, параметр UACC (Universal Access). Этот параметр определяет уровень авторизации на использование ресурса для пользователей и групп по умолчанию, а также для пользователей, не определенных в RACF, или задач, не имеющих владельца. Кроме этого, для пользователей и групп можно определить специальные уровни авторизации, отличающиеся от UACC; совокупность этих специальных уровней авторизации для ресурса называют списком доступа (Access List). Вообще, уровней авторизации в RACF шесть: NONE, READ, EXECUTE, UPDATE, CONTROL, ALTER; при этом для каждого класса защиты эти уровни авторизации могут иметь различные толкования, что естественным образом вытекает из многообразия ресурсов, защищаемых RACF.

В результате для каждого пользователя RACF существует уровень авторизации на доступ к каждому защищенному ресурсу, который определяется либо посредством UACC, либо через Access List.

Профили защиты могут быть «общими» (generic). Такой профиль может одновременно определять несколько ресурсов.

При защите набора данных может быть выставлен бит защиты набора в оглавлении тома. В этом случае доступ любого типа к набору данных в любом случае будет осуществляться через запрос к RACF, в частности, доступ из другой операционной системы будет разрешен лишь в том случае, если в ее системе безопасности для этого набора данных существует профиль защиты, позволяющий доступ. Эта возможность, безусловно, повышает защищенность дисковых наборов данных, однако, может создать серьезные проблемы при переходе к другой операционной системе или при обобщении дисковых данных, поэтому в настоящее время она реализуется как опция, в то время как в ранних версиях RACF защита дисковых наборов осуществлялась только через установку бита защиты в оглавлении тома.

Для определения авторизации задач (процедур, пакетных заданий) используются механизмы сопоставления имени задачи с именем пользователя, авторизацией которого на использование тех или иных ресурсов будет пользоваться задача. Обычно такой пользователь называется владельцем (owner) задачи. Для пакетных заданий владельцем является по умолчанию пользователь, запустивший задание, однако, существует возможность явного указания пользователя в операторе JOB с помощью параметров USER, GROUP и PASSWORD. При этом, правда, серьезным недостатком является необходимость явного указания пароля. Для процедур владелец определяется с помощью класса защиты STARTED, ресурсы в котором определяются по именам процедур, и при определении профиля, в котором можно напрямую указать пользователя, являющегося владельцем данной процедуры.

Используя программы выхода, можно ужесточить либо смягчить права доступа к ресурсам. В частности, можно определять эти права когда RACF неактивен. В этом случае, если программа выхода не определяет прав пользователя на использование ресурса, выдается запрос на операторскую консоль.

Другой возможностью, предоставляемой программами выхода, является ограничение доступа владельца к своим ресурсам.

4.1.3. Security Classification

Для упрощения администрирования и большей гибкости настройки, RACF может использовать так называемую классификацию безопасности (Security Classification), определяемую как для пользователей, так и для профилей защиты. Классификация безопасности подразумевает указание следующих параметров:

- Security Level (SECLEVEL) — некоторое число (сопоставленное для удобства с символьным именем), определяющее уровень авторизации. Чем выше SECLEVEL, тем выше уровень авторизации. SECLEVEL удобно использовать по аналогии с многоуровневой системой защиты (multilevel security — MLS), традиционно используемой в государственных учреждениях и подразумевающей пометку документов грифами секретности.
- Security Category (CATEGORY) — некоторое имя, связанное с отделом или другой частью организации, внутри которой пользователи имеют схожие права.
- Security Label (SECLABEL) — некоторое имя, соответствующее одному SECLEVEL и нескольким (начиная с нуля) CATEGORY; использование SECLABEL является альтернативой использованию SECLEVEL и CATEGORY.

Проверка с использованием классификации безопасности осуществляется после проверки Universal Access, но перед проверкой Access Lists. Если Universal Access не разрешил доступ к ресурсу, то выполняется дальнейшая проверка (по классификации безопасности, по Access Lists и т.д.), если же UACC позволил доступ к ресурсу, то дальнейшей проверки не производится и доступ к ресурсу разрешается.

В случае, если механизм Security Classification активен, проверка авторизации выполняется в два этапа:

1. Сравнение SECLEVEL ресурса и пользователя. Если уровень авторизации ресурса выше, чем у пользователя, запрос отвергается.
2. Сравнение списков категорий защиты (CATEGORY) для пользователя и ресурса. Если в профиле защиты ресурса есть хоть одна категория, которой нет в профиле пользователя, запрос отвергается. Если в профиле защиты ресурса нет категорий защиты, этот шаг проверки пропускается.

Метки защиты (security labels) являются развитием механизма security level и security category. Обладая той же функциональностью, они обеспечивают следующие усовершенствования:

- Метки защиты могут быть у ресурсов, не имеющих профиля защиты RACF (например, у файлов спула);
- Пользователь может входить в систему с одним и тем же идентификатором, но с разными security labels (параметр SECLABEL можно указать, например, при входе в TSO или в операторе JOB JCL);
- Упрощается классификация безопасности пользователей и ресурсов.

При активизации класса SECLABEL автоматически создаются три метки защиты: SYSHIGH, SYSLOW и SYSNONE. Первая подразумевает максимальный уровень защиты и права на все категории, остальные — минимальный уровень защиты и отсутствие прав на категории.

4.1.4. Secured Signon

Еще одним дополнительным средством защиты данных, используемым в RACF, является Secured Signon. Эта функция позволяет для аутентификации пользователя вместо пароля применять так называемый PassTicket, генерируемый RACF и используемый однократно; срок действия PassTicket ограничен 10 минутами. Использовать Secured Signon-авторизацию можно как для локальных, так и для удаленных (в частности, клиент-серверных) приложений, что предотвращает передачу пароля по сети. Среди локальных приложений Secured Signon поддерживается, в частности, APPC, CICS, IMS, TSO и пакетными заданиями.

Идентификация происходит следующим образом. В классе защиты PTKTDATA описываются профили защиты, названия которых строятся из имени прикладной программы и, возможно, имени пользователя RACF, и/или имени группы пользователей. Каждому из профилей сопоставляется 64-битный ключ защиты, который хранится в базе данных RACF, либо в замаскированном по специальному алгоритму, либо в зашифрованном виде (при наличии криптографического программного обеспечения). При установке соединения клиентское приложение (естественно, поддерживающее функцию Secured Signon) получает идентификатор пользователя и на основании него, ключа защиты, текущего времени и других данных по специальному алгоритму генерирует PassTicket, передаваемый RACF. RACF осуществляет соответствующую проверку и разрешает или запрещает установку сессии или выполнение некоторых действий.

На основании PassTicket может быть также сгенерирован ключ маскировки данных сессии,

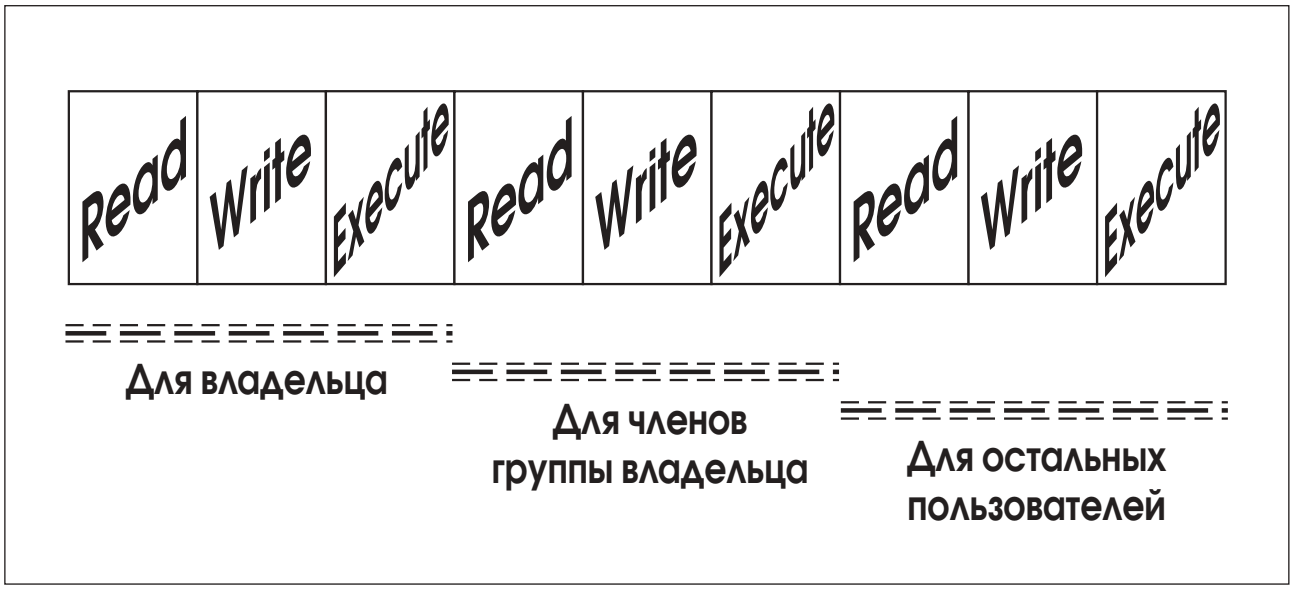

Рис.4. Защита файла Unix

обеспечивая дополнительную защиту информации при передаче данных по сети путем их шифрования.

В случае получения пользователем сообщения о неверном пароле, RACF также посылает соответствующее сообщение в системный журнал и на консоль.

Технология PassTickets разработана и запатентована IBM.

4.1.5. Взаимодействие RACF с Unix System Services

При работе с Unix System Services for OS/390 (USS) возникает проблема взаимодействия классической Unix структуры защиты данных и RACF. В Unix все пользователи имеют идентификаторы, но, в отличие от RACF, не алфавитно-цифровые, а цифровые (User Identifier — UID). Пользователи объединены в группы, которые также имеют цифровые идентификаторы (Group Identifier — GID). В Unix описывается однозначное соответствие между цифровым и символьным идентификатором пользователя (используемым для удобства), то же самое для групп. Каждый файл или директория в Unix имеют своего владельца; права доступа к ним характеризуются девятибитным словом, структура которого приведена на рисунке 4. При попытке доступа к файлу, Unix определяет тип желаемого доступа, а также категорию пользователя, пытающегося осуществить подобный доступ — владелец файла, член той же группы, что и владелец файла либо не подходящий под указанные категории, после чего разрешает или запрещает доступ. Существует также пользователь, обладающий правами superuser, имеющий доступ любого уровня ко всем файлам, а также право на изменение защиты или владельца любого файла. Superuser имеет UID 0.

Противоречие между защитой данных RACF и Unix System Services заключается в том, что в USS владелец файла обладает полными правами доступа к файлу. Даже если для владельца указан запрет на Read, Write и Execute одновременно, он всегда может выдать команду chmod и изменить права доступа к этому файлу. Никакой администратор этого запретить не может, поэтому и оказывается, что уровень защиты USS ниже уровня защиты RACF для остальных ресурсов.

Для пользователей и групп RACF, имеющих право пользоваться сервисами и доступом к файловой системе USS, должен быть определен сегмент OMVS, в котором как раз и указывается UID пользователя или GID группы. Для кэширования UID и GID, позволяющего, в частности, повысить производительность ряда команд оболочки USS, используется подсистема Virtual Lookaside Facility (VLF). Рекомендуется, чтобы каждый пользователь имел уникальный UID, однако, строгого запрета на дублирование UID нет, в связи с чем возможен эффект подмены имени владельца файла на имя другого пользователя с тем же UID, так как в кэше VLF хранится только одно имя пользователя или группы, соответствующее конкретному UID или GID.

RACF также обеспечивает авторизацию и аудит при взаимодействии между процессами в USS с использованием функций XPG4 Base Branding. Такое взаимодействие позволяет процессам, в част-

ности, совместно использовать области памяти и очереди сообщений.

4.1.6. Протоколирование и аудит

Для контроля доступа к ресурсам RACF используются три механизма: оповещение, сбор статистики и протоколирование посредством SMF. Под оповещением подразумевается немедленная передача сообщения указанному при создании профиля защиты пользователю о попытке неавторизованного доступа к ресурсу. По умолчанию сообщение дублируется на операторскую консоль и в системный журнал. В нем содержится информация об имени пользователя, сделавшего попытку несанкционированного доступа, а также о профиле защиты, описывающем ресурс, к которому пытался получить доступ пользователь.

Сбор статистики подразумевает подсчет количества обращений разных типов к защищенному ресурсу. Опция включения сбора статистики устанавливается для класса защиты, после чего для всех профилей защиты, входящих в этот класс начинается сбор статистики. Статистика собирается по двум категориям доступа: для доступа всех пользователей (посредством Universal Access) и для доступа конкретных пользователей, имеющих специальные права на использование данного ресурса. Статистика накапливается в базе RACF и может просматриваться посредством стандартных интерфейсов RACF.

System management facilities (SMF) является системным средством, позволяющим накапливать различную информацию, относящуюся к системе в целом и к отдельным задачам. Эта информация затем может анализироваться для составления отчетов, анализа событий и т.п.

Протоколирование посредством SMF является наиболее совершенным. Данные о некоторых событиях протоколируются всегда, например, обо всех случаях выдачи команд RVARY или SETROPTS, позволяющих изменить основные настройки RACF. Данные о некоторых других событиях, напротив, не протоколируются никогда, например, о выдаче команд просмотра настроек конкретного пользователя или группы LISTGRP, или LISTUSER. Все остальные события протоколируются при условии наличия соответствующей настройки RACF. Задать настройки для аудита могут либо владельцы ресурсов, либо аудиторы. Первые могут определять, будет ли вестись протоколирование при доступе к ресурсам путем соответствующей настройки профилей защиты, причем существует возможность фильтрации протоколируемых событий по уровню доступа к ресурсу (READ, UPDATE, CONTROL или ALTER) и по результатам попыток доступа (успешна, отвергнута или любая). Аудиторы могут задавать опции протоколирования для следующих событий:

- изменение профилей защиты RACF;
- выдача любых команд RACF пользователями, имеющими атрибут SPECIAL;
- попытки несанкционированной выдачи команд RACF;
- любой доступ к ресурсам пользователей, имеющих атрибут OPERATIONS;
- любой доступ к указанным наборам данных и другим ресурсам;
- события, относящиеся к Unix System Services.

4.1.7. Администрирование

В небольших организациях для выполнения административных задач и аудита RACF может быть выделен один администратор. Однако для уменьшения влияния человеческого фактора на информационную безопасность задачи администрирования рекомендуется разделять.

В первую очередь, администраторы ни в коем случае не должны иметь доступа ко всем защищенным ресурсам, в частности, к пользовательским или системным наборам данных. Атрибут OPERATIONS рекомендуется присваивать только пользователям, чьи права используются, например, для резервного копирования/восстановления данных; иметь прав на другую работу с системой такой пользователь не должен.

Одна из рекомендуемых схем администрирования RACF включает следующие градации (из соображений надежности, для каждой из описанных ниже задач рекомендуется использовать как минимум двух человек, обладающих идентичными правами и регистрирующих свои действия в журнале):

1. Главный администратор, несущий ответственность за общую настройку RACF, определение необходимых классов защиты и групп пользователей. Все серьезные изменения в настройках RACF должны проводиться через главного администратора. Задачей главного администратора является назначение администраторов групп и аудиторов и обеспечение их необходимыми правами.
2. Администраторы групп, несущие ответственность за разграничение прав доступа к ресурсам, принадлежащим группе, а также за разделение функций администрирования и аудита внутри групп.
3. Администраторы ресурсов (опция), определяющие политику в отношении определенного (особо важного) ресурса или группы ресурсов.
4. Главный аудитор, осуществляющий общий аудит.

5. Аудиторы групп, осуществляющие аудит ресурсов, принадлежащих группе.
6. Аудиторы ресурсов (опция), отслеживающие доступ к определенному ресурсу или группе ресурсов.
7. Технический администратор, несущий ответственность за инсталляцию и апгрейд RACF, написание программ выхода, организацию межсистемного взаимодействия и поддержание целостности базы данных RACF.
8. Системные программисты, обеспечивающие функционирование операционной системы в целом. Они должны иметь полный доступ к системным наборам данных, однако, главный администратор RACF вправе запретить его и предоставлять только по особому (например, письменному) требованию.
9. Администраторы приложений, имеющих отношение к RACF, например, администраторы СУБД или TSO. Функции и наборы данных, необходимые для обеспечения работы приложений, также могут быть доступны им только по особому требованию.

Естественно, приведенная схема может изменяться в сторону усложнения, упрощения или как-нибудь еще и не является догмой.

4.2. Механизмы защиты в MVS

До того, как в операционных системах-предшественницах OS/390 появился RACF, для защиты данных, авторизации на выполнение определенных действий или функций, использовались другие механизмы. Из соображений преемственности все они поддерживаются до сих пор. Сочетание этих механизмов с RACF позволяет строить эшелонированную оборону.

MVS (MultiVirtual System) в OS/390 называют центральную часть операционной системы, занимающуюся выполнением программ, обслуживанием консолей, обслуживанием адресных пространств и другими задачами системного уровня. MVS обеспечивает следующие механизмы безопасности.

Авторизация консолей операционной системы, позволяющая разрешить или запретить ввод конкретных команд с той или иной консоли, а также ограничить вывод тех или иных сообщений на определенные консоли. Каждая консоль описывается в библиотеке системных параметров операционной системы, где кроме прочих параметров указывается уровень ее авторизации и маршрутный код. Уровень авторизации консоли определяет команды, которые можно с нее вводить. Используются следующие уровни авторизации консолей:

- NONE — консоль не предназначена для ввода команд;
- INFO — с консоли можно ввести только информационные команды;
- CONS — с консоли можно ввести информационные команды и команды управления консолями;
- SYS — с консоли можно ввести информационные команды и команды управления системой;
- IO — с консоли можно ввести информационные команды и команды управления вводом/выводом;
- ALL — с консоли можно ввести все команды перечисленных выше групп;
- MASTER — определяет главную консоль системы, с нее можно ввести все системные команды; некоторые особенно важные для операционной системы команды и подкоманды можно вводить только с главной консоли.

Авторизация APF (Authorized Program Facility) запрещает выполнять ряд машинных инструкций (известных как привилегированные, или авторизованные) из произвольных пользовательских программ. Привилегированные команды осуществляют порождение подзадач и управление ими, связь между адресными пространствами, отслеживание системных событий, организацию ввода-вывода и прочие функции, способные повлиять (в том числе негативно) на операционную систему и задачи, выполняемые в ней. В частности, механизм APF-авторизации используется для того, чтобы пользовательская программа не могла обойти проверку RACF при доступе к ресурсу. Обычно программы, выполняющие авторизованные команды, также называют авторизованными.

Программа является APF-авторизованной, если выполняются два условия:

- для первого загрузочного модуля программы установлен код авторизации (это делается редактором связей);
- программа находится в одном из библиотечных наборов данных, описанных в настройке системы как «авторизованные»; таким образом, для предотвращения возможности создания авторизованных программ достаточно закрыть доступ по записи к этим наборам данных.

4.2.1. Data Facility Storage Management Subsystem

Ряд возможностей этой подсистемы можно отнести к механизмам защиты OS/390. Например, для защиты от аппаратных ошибок и ошибок передачи и,

соответственно, обеспечения целостности данных, DFSMS использует аппаратные механизмы контрольных сумм и избыточности информации в системах хранения информации на дисках и лентах.

Кроме этого, DFSMS позволяет администратору определить пользователей и группы пользователей, которым разрешено или запрещено создавать наборы данных с определенными именами, характеристиками или физическим расположением на томах прямого доступа. При попытке пользователя создать набор данных вызываются специальные программы (Automatic Class Selection (ACS) Routines), определяющие может ли данный пользователь создать набор данных с такими характеристиками. Такой анализ делается исходя из указанных пользователем параметров создания набора данных, а также из параметров самого пользователя и способа создания набора данных. На основании анализа указанных параметров, ACS Routines могут:

- определить характеристики создаваемого набора данных, не указанные пользователем;
- изменить некоторые характеристики создаваемого набора данных (например, имя тома прямого доступа, где будет создан набор данных);
- запретить создание набора данных с возможной выдачей соответствующего сообщения.

В частности, ACS Routines анализируют имя пользователя, создающего набор данных, и идентификатор его группы RACF. Таким образом, появляется возможность дополнительного контроля за обработкой данных в OS/390 на основании настроек RACF. Во многих организациях, использующих OS/390, политики RACF и DFSMS тесно связаны, и зачастую (в небольших организациях) оба эти приложения управляются одним и тем же администратором.

Составной частью DFSMS является Hierarchical Storage Manager (HSM), приложение, позволяющее автоматизировать процесс резервного копирования/восстановления данных. При использовании HSM совместно с роботизированной библиотекой съемных носителей появляется возможность полностью освободить процесс резервирования данных от ручного труда и связанных с этим ошибок.

До появления RACF в операционных системах семейства MVS существовала парольная защита наборов данных, являющаяся в настоящее время функцией DFSMS. Пароль (или пароли) набора данных хранится в data set control block (DSCB). В зависимости от типа набора данных может использоваться до 4 паролей. Парольная защита обычных наборов данных в настоящее время не рекомендуется, однако, она по-прежнему актуальна для каталогов и файлов конфигурации ввода-вывода — IODF.

Конфигурация DFSMS может быть разделяемой между несколькими операционными системами (до 32). В таком случае можно запрещать или разрешать доступ к томам прямого доступа для тех или иных систем.

4.2.2. Hardware Configuration Definition (HCD)

Этот компонент позволяет работать с конфигурациями ввода/вывода как операционной системы или совокупности операционных систем, так и процессора или совокупности процессоров. HCD позволяет эффективно разграничить доступ к ресурсам в многомашинных комплексах или при использовании LPAR для того, чтобы к различным дисковым томам или аппаратным устройствам (например, устройствам резервирования данных) имели доступ только пользователи тех или иных машин или LPAR.

Например, IBM рекомендует устанавливать Firewall на отдельной копии OS/390, работающей в другом LPAR. С помощью HCD можно ограничить конфигурацию ввода/вывода этого LPAR только необходимыми дисками и сетевыми контроллерами.

Одной из важных функций HCD является обслуживание UIM (Unit Interface Module) — по сути дела, драйверов периферийных устройств. Существует возможность создания собственных UIM для любых нестандартных периферийных устройств.

4.2.3. Криптографическая защита данных

Архитектура обеспечения конфиденциальности информации в S/390 носит название Общей архитектуры криптографической защиты — CCA (Common Cryptographic Architecture). Поддерживается ряд стандартов ISO, касающихся использования криптографии для защиты конфиденциальности и целостности данных (8730, 8731 и 9564).

Криптогафическая защита обеспечивается двумя компонентами: аппаратным компонентом — CF (Cryptographic Facility) и программным компонентом — CFAP (Cryptographic Facility Access Program).

Эту архитектуру реализуют: средства интегрированной системы криптографии Integrated Cryptographic System Facilities/MVS, система безопасности транзакций Transaction Security System и интегрированные функции шифрования S/390 Integrated Cryptographic Feature.

В соответствии с архитектурой CCA центральные устройства ЭВМ могут быть дополнены средствами шифрования ICRF (Integrated Cryptographic Feature), обеспечивающими скорость шифровки/расшифровки, равную скорости

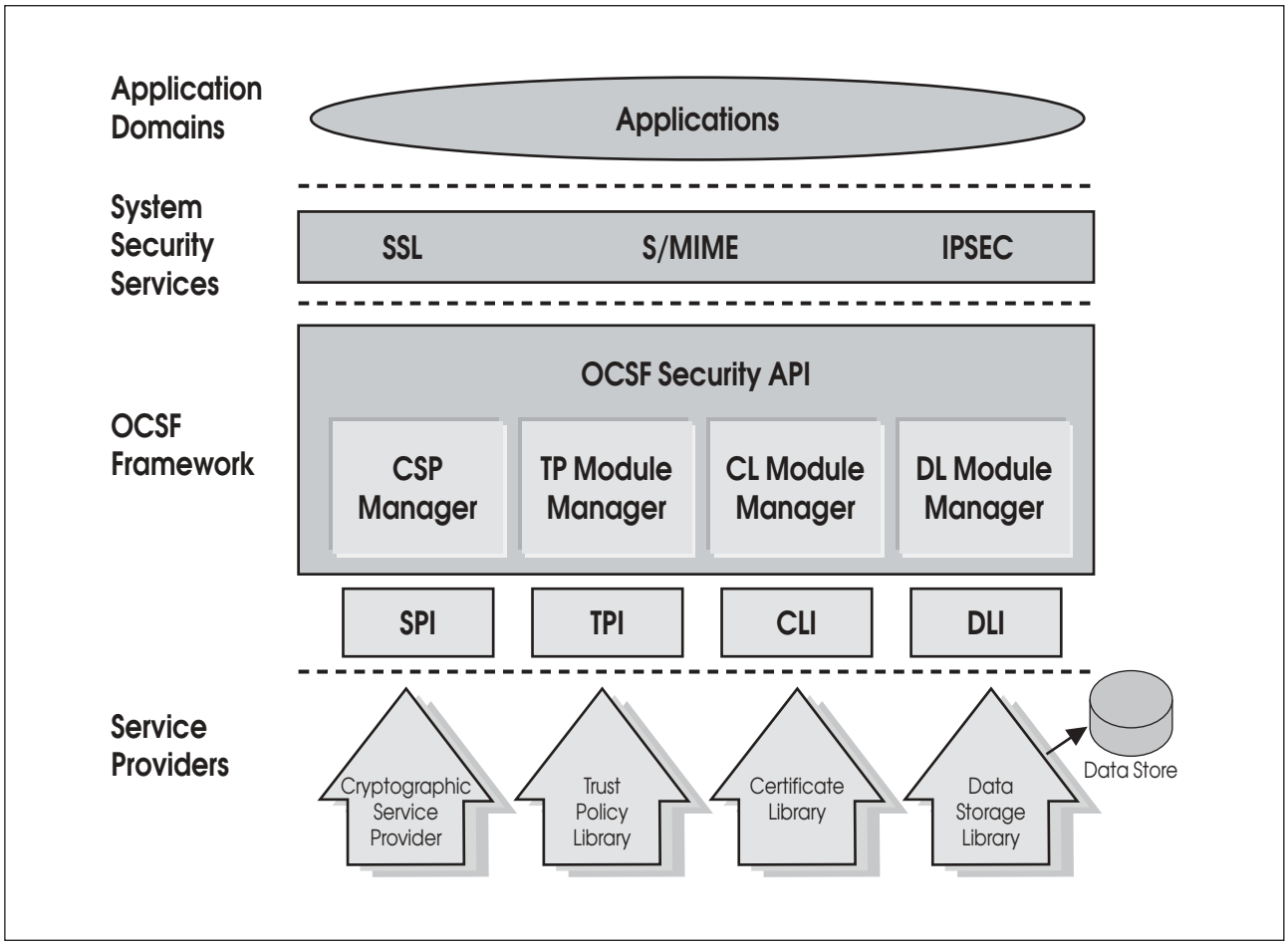

Рис.5. Архитектура OCSF

работы центрального процессора (процессор может иметь в своем составе либо векторное, либо криптографическое устройство). Аппаратные средства шифрования могут устанавливаться на одном или двух процессорах. Для микропроцессорных моделей выпускаются криптографические сопроцессоры.

В OS/390 существует ряд криптографических компонентов, реализующих криптографию как программно, так и с использованием специализированных аппаратных устройств. Основным продуктом такого рода является Integrated Cryptographic Service Facility (ICSF). Это средство использует алгоритм шифрования DES и нуждается в наличии криптографического сопроцессора.

Open Cryptographic Services Facility (OCSF) является программным продуктом, обеспечивающим прикладной программный интерфейс к системам криптографии для задач, работающих в Unix System Services. Архитектура OCSF приведена на рисунке 5. Она включает в себя 4 уровня:

- Application Domains обеспечивает поддержку приложений, например, SET (Security Electronic Transactions) или пользовательских приложений.
- System Security Services обеспечивает протоколы безопасности, используемые на уровне Application Domains, например, SSL. Кроме того, уровень System Security Services включает в себя утилиты, необходимые для инсталляции и конфигурации OCSF.
- OCSF Framework является центральным компонентом этой архитектуры и обеспечивает механизм управления модулями поставщиков услуг, для доступа к которым обеспечивается прикладной программный интерфейс (Application Programming Interface, API).
- Service Providers (поставщики услуг) — программные и аппаратные компоненты, обеспечивающие необходимые способы защиты. Ряд поставщиков услуг предлагаются IBM, однако, возможно использование поставщиков услуг других производителей программного и/или аппаратного обеспечения.

Система безопасности транзакций — TSS (IBM Transaction Security System) включает: под-

ключаемый к каналу ЭВМ S/370/390 IBM 4753 Network Security Processor, несколько моделей высокоскоростных криптографических адаптеров IBM 4755 Cryptographics Adapter для ПЭВМ типа IBM PC и PS/2, а также подключаемое непосредственно к IBM 4755 через интерфейс RS-232S устройство IBM 4754 Security Interface Unit, предназначенное для считывания информации с персональных карточек безопасности PSC (Personal Security Card), ввода автографа пользователя при помощи специального пера и ввода кода доступа при помощи 12-кнопочной клавиатуры.

PSC имеет такой же внешний вид, как обычная кредитная карточка. Для обеспечения идентификации владельца в нее встроен чип с микропроцессором и памятью.

Network Security Processor IBM 4753 обеспечивает шифрование в стандарте DEA. В состав устройства входит собственная память, обеспечивающая хранение до 70000 ключей, и кэш-память на 10000 ключей для быстрого доступа. Устройство комплектуется монохромным алфавитно-цифровым дисплеем, клавиатурой, Cryptographics Adapter и Security Interface Unit для обеспечения доступа оператору при проведении работ по настройке, вводу и редактированию ключей, распределению ключей. К одной ЭВМ типа S/370/390 может быть подключено до 16 устройств типа IBM 4753.

Криптографические устройства обеспечивают шифровку-расшифровку сообщений в стандарте США DEA (Data Encryption Algorithm). Поддерживаются ключи длиной до 128 бит, генерация ключей на основе генератора псевдослучайных чисел, обеспечиваются средства безопасной передачи ключей, идентификация пользователей на основе PIN и цифровая подпись. Дополнительно может быть реализован алгоритм шифрования с открытым ключом — DEA-PKA (Data Encryption Algorithm — Public Key Algorithm — RSA [Rivest, Shamir, Adelman] algorithm). Для цифровой подписи, цифровой подписи приложения (application digital signature) и цифровой подписи системы (system signature) используются ключи длиной от 512 до 1024 бит, а также специальные ключи public device authentication key и private device authentication key. Всего расширение PKA обеспечивает 20 дополнительных сервисных криптографических функций, доступных через API (Application Programming Interface).

5. Механизмы защиты в режиме LPAR

MULTIPLE LOGICAL PROCESSOR FEATURE (MLPF) — специальное обеспечение современных мейнфреймов, позволяющее применять их одновременно для работы нескольких операционных систем. Использование этого режима позволяет обеспечить быстрый переход при любых модернизациях вычислительной системы.

Процессорный комплекс с MLPF может быть разделен на несколько логических составляющих LOGICAL PARTITIONS(LPAR), в каждом из которых работает своя операционная система или любая другая программная среда. Использование этого режима позволяет обеспечить быстрый переход при любых модернизациях информационной системы без потери работоспособности. Среда, управляющая работой в режиме LPAR, представляет самостоятельную подсистему, входящую в состав ИС, характеристики которой влияют на качество функционирования ИС.

В состав этой подсистемы входит аппаратурная, программная и организационная составляющие. Эти средства являются моделезависимыми и встраиваются в ЭВМ на этапе разработки.

5.1. Реализация LPAR

Функционирование в режиме LPAR обеспечивается специальными аппаратурными и программными средствами. Эти средства являются моделезависимыми и встраиваются в машину на этапе разработки. В состав эксплуатационной документации описание этих средств и принципов их работы не входит. Поэтому вся приведенная информация получена путем исследования работы в режиме MLPF IBM подобных машин HITACHI.

Технические возможности работы ЭВМ в режиме MLPF обеспечиваются аппаратурными средствами процессора.

Встроенное в процессор специальное оборудование позволяет разделить его ресурсы, а также оперативную и расширенную память на несколько независимых логических ЭВМ. Это оборудование используется только при работе в режиме LPAR.

Специальная команда (SIE) реализует режим переключения процессора из одного LPAR в другой. При выполнении этой команды все ресурсы процессора подключаются к заданному LPAR. В этом режиме работает программная среда, используемая в данном LPAR.

Выход из режима происходит по истечении времени работы данного LPAR или наступления со-

бытий, выводящих из этого режима. Состояние выполняемого процесса сохраняется в специальных таблицах для данного LPAR. При следующей активизации данного LPAR программа начинается с сохраненной точки.

Каналы разделяются между всеми используемыми LPARами. В режиме LPAR каналы ввода/вывода функционируют точно так же, как в базовом режиме, но на завершающем этапе информация об операции ввода/вывода передается специальной программе, которая отправляет ее в необходимый LPAR.

Оперативная и расширенная память выделяется каждому LPAR. Разделение ее на разделы проводится оператором при начальной установке. Этот раздел ОП закрывается ключом защиты и изолируется от других разделов. Выделенный раздел может находиться в любом месте ОП, но для работающих в данном LPAR программ он всегда будет иметь последовательную адресацию, начинающуюся с нулевого адреса.

Выделенные каждому LPAR каналы и память недоступны для других.

Управление работой в режиме LPAR обеспечивается специальным программным обеспечением. Программы, написанные на ассемблере, записаны в загрузочном виде на внутренний носитель в специальном формате. Перед началом работы программы загружаются в память с внутреннего накопителя.

Комплекс программ состоит из модулей, выполняющих функции управления LPAR. К числу таких модулей относятся:

- монитор;
- служба времени;
- обработка прерываний;
- связь с управляющей консолью;
- установка режимов работы;
- обработка ошибок;
- ввод запросов;
- вывод сообщений.

Программы, написанные на ассемблере, записаны в загрузочном виде на внутренний носитель в специальном формате. Перед началом работы программы загружаются в память с внутреннего накопителя.

Эта программная среда является надстройкой над всеми программными системами, используемыми в LPARах.

Компонент/функция	1	2	3	4	5	6
RACF	+	+	+			
MVS		+			+	
Parallel Sysplex		+			+	
Терминальные приложения	+	+	+			
DFSMS		+	+		+	
HCD		+				
DCE Security	+	+	+		+	+
Сервер LDAP	+	+	+		+	+
ADSM	+	+	+		+	
Сервер Telnet		+	+			+
Web-сервер	+	+	+			+
Сервер FTP		+	+			
Сервер NFS		+	+			
OCSF					+	+
SNA	+	+			+	+
Firewall	+	+	+	+		+
Kerberos	+				+	+
SSL					+	+
SNMP	+	+	+		+	+
SMF			+			
syslogd			+			

Таблица 1. Реализация сервисов безопасности на платформе S/390

6. Реализация сервисов безопасности на платформе S/390

В этом разделе рассматриваются особенности реализации сервисов безопасности на платформе S/390 средствами, рассмотренными выше. Рассматриваются следующие сервисы безопасности:

1 — идентификация/аутентификация;

2 — разграничение доступа;
3 — протоколирование и аудит;
4 — экранирование;
5 — контроль целостности;
6 — обеспечение конфиденциальности трафика.

В Таблице 1 сопоставлены сервисы безопасности и элементы системы безопасности S/390.

6.1. Идентификация/аутентификация

Существуют варианты реализации идентификации/аутентификации пользователей в OS/390. Основным механизмом является использование RACF, но возможно и использование специфических функций безопасности ряда приложений.

Аутентификация пользователей RACF осуществляется при входе в систему однократно. При работе с системой для доступа к ресурсу используются права, определенные для данного пользователя, и повторно пароль не запрашивается. Кроме указания имени пользователя и пароля, возможна идентификация с помощью идентификационных карт (OIDCARD) при работе со специального терминала. В целях обеспечения дополнительной защиты, доступ пользователя к системе может быть ограничен по времени и дням недели. В случае использования суррогатных пользователей (если активен класс защиты SURROGAT), возможно выполнение определенных функций одному пользователю «от имени» другого без указания пароля.

Пароли пользователя хранятся в базе данных RACF в зашифрованном виде. Для их шифрования можно использовать как стандартный, так и пользовательский алгоритм. RACF обладает средствами разделения и резервирования базы данных.

Приложения, работающие в OS/390, пользуются авторизацией пользователя, являющегося их владельцем. Для разных типов приложений имя владельца определяется по-разному, например, для процедур — с помощью класса защиты STARTED, для пакетных заданий — с помощью указания ключевых слов в операторе JOB.

Для аутентификации пользователя или приложения вместо пароля можно также использовать так называемый PassTicket, генерируемый RACF и используемый однократно.

Ряд приложений OS/390 (Сервера Telnet, FTP) позволяют ужесточить аутентификацию пользователя, например, посредством дополнительной проверки IP-адреса клиентского приложения (в частности, сервера FTP или Telnet).

При соответствующей настройке возможен вход пользователя в некоторые приложения без идентификации. В этом случае он пользуется либо минимальными правами доступа к ресурсам, либо правами доступа, определенными через класс защиты SURROGAT.

Система идентификации/аутентификации пользователей, применяемая в RACF, считается одной из наилучших. Обеспечение единого процесса аутентификации для доступа ко всем системным ресурсам позволяет упростить работу конечного пользователя, а также централизовать администрирование. Описанные выше дополнительные возможности не обязательны к применению, однако позволяют придать большую гибкость системе информационной безопасности.

Многие средства: Web-сервер, терминальные приложения (TSO, CICS), DCE, сервер ADSM, Firewall, SNMP дают возможность использовать собственную системы аутентификации. В этом случае доступ к защищенным ресурсам для пользователей, прошедших не-RACF аутентификацию, осуществляется в соответствии с UACC (Universal Access).

6.2. Разграничение доступа

Все ресурсы, защищаемые RACF, имеют описание в базе данных RACF в виде профилей защиты. Профили защиты, описывающие однотипные ресурсы, объединены в классы защиты. Доступ к ресурсу для пользователей определяется параметром UACC (универсальный доступ), а также списком доступа Access List, указываемыми для каждого профиля защиты. Для определения профиля защиты ресурса необходимо активизировать соответствующий класс защиты.

Если пользователь описан в Access List профиля защиты, то доступ осуществляется в соответствии с правами, указанными в нем, в противном случае — в соответствии с правами, указанными в UACC.

Запрос к RACF на доступ определенного пользователя к определенному ресурсу делают прикладные программы, называемые в этом контексте менеджерами ресурсов. RACF обеспечивает менеджеры ресурсов информацией о правах пользователя на доступ к ресурсу; выполнение действий по запрещению или разрешению доступа осуществляется менеджерами ресурсов. В роли менеджера ресурсов могут выступать, в частности, терминальные приложения, базовая операционная система MVS, DFSMS, DCE, LDAP, ADSM, различные сервера TCP/IP и другие приложения, в том числе нестандартные и пользовательские.

Для пользователей RACF, с одной стороны, и профилей защиты ресурсов, с другой стороны, могут быть определены параметры классификации

безопасности, позволяющие осуществлять дополнительную проверку авторизации пользователя на использование ресурса.

Такой способ разграничения доступа к ресурсам позволяет обеспечить доступ к ресурсам только для авторизованных на это пользователей, однако, требует серьезной предварительной настройки.

HCD позволяет разграничить доступ к физическим ресурсам между машинами, работающими в многомашинном комплексе, в том числе в среде Parallel Sysplex.

6.3. Протоколирование и аудит

Многие компоненты, входящие в OS/390 и занимающиеся информационной безопасностью, обеспечивают протоколирование и аудит. RACF использует методы оповещения пользователей при попытке неавторизованного доступа к ресурсу, сбор статистики обращений к ресурсу, а также создание записей в базе данных SMF. Для дальнейшего анализа этих записей используется ряд специальных средств и утилит, позволяющих определять слабые места в системе безопасности. В принципе, SMF поддерживает интерфейс для написания пользовательских приложений выгрузки и анализа данных.

Другие компоненты, отвечающие за информационную безопасность, также используют SMF для протоколирования. Некоторые из компонентов могут параллельно использовать собственные журналы или стандартный сервер Unix syslogd (в частности, firewall).

Многие сервера (сервер Telnet, FTP, LDAP, Web, ADSM, DCE, NFS, Firewall, SNMP и другие) позволяют протоколировать все соединения, а также осуществлять трассировки. Обычно хранение и обработку этих данных обеспечивает подсистема управления заданиями JES.

Терминальные приложения, в частности, TSO, также позволяют производить протоколирование при работе пользователя. В специальный файл заносится информация о том, какие команды выдавал, какие файлы изменял и какие задания запускал пользователь TSO в течение сеанса. Оглавление библиотечного набора данных хранит статистическую информацию о дате и времени последней модификации разделов, а также о пользователе, осуществлявшем эту модификацию, однако, не все приложения, работающие с разделами библиотек, способны представлять и модифицировать эту информацию.

Централизация информации по безопасности OS/390 с возможностью ее накопления позволяет осуществлять анализ системы безопасности в целом и ее компонентов в отдельности. Оповещение о попытках неавторизованного доступа может быть эффективно использовано для быстрого реагирования на атаки извне или изнутри.

6.4. Экранирование

На базе OS/390 может быть реализован firewall или межсетевой экран, позволяющий ограничить доступ к локальной сети извне. Firewall for OS/390 реализует следующие функции: фильтрацию IP-пакетов, трансляцию сетевых адресов (NAT), организацию виртуальных частных сетей (VPN), протоколирование, удаленную конфигурацию, поддержку протокола RealAudio, FTP прокси-сервер, SOCKS-сервер, сервер доменных имен. Для достижения большей защиты данных рекомендуется запускать firewall for OS/390 в отдельном LPAR или на отдельном процессоре.

Firewall for OS/390 реализует стандартные функции межсетевых экранов, однако, вследствие высокой надежности и закрытости OS/390 имеет преимущества перед реализацией межсетевых экранов на других платформах.

6.5. Контроль целостности и обеспечение конфиденциальности трафика

Для контроля целостности данных и обеспечения конфиденциальности трафика в OS/390 используются следующие методы:

- контрольные суммы;
- избыточность информации;
- поддержка протокола SSL (версий 2 и 3);
- поддержка Kerberos;
- криптографические функции.

В частности, для реализации криптографических функций наряду со средствами, использующими западные алгоритмы шифрования и требующими специальной аппаратной поддержки, может использоваться средство Open Cryptographic Services Facility (OCSF), позволяющее использовать пользовательское программное и/или аппаратное обеспечения для обеспечения криптографических функций.

Метод контрольных сумм используется, в частности, при SNA-соединениях, а также при использовании протокола SNMP версии 3. Защищенные SSL-соединения могут использовать сервера Web, Telnet, LDAP, ADSM, Firewall.

7. Особенности реализации политики информационной безопасности на платформе S/390

Любая политика безопасности должна строиться на основе следующих принципов:

- «все запрещено, что не разрешено»;
- непрерывность защиты в пространстве и времени, невозможность обхода защитных средств;
- равнопрочность обороны по всем направлениям;
- эшелонированность обороны.

7.1. «Все запрещено, что не разрешено»

Система должна содержать лишь те компоненты и связи, которые необходимы для ее функционирования (с учетом требований надежности и перспективного развития), а права субъектов должны быть минимально достаточными для выполнения ими своих служебных обязанностей.

Система безопасности OS/390 частично удовлетворяет данному принципу. С одной стороны, в OS/390 практически нет компонентов (за исключением необходимых для функционирования собственно операционной системы), работающих «по умолчанию». На этапе планирования инсталляции можно определить какие подсистемы, компоненты и их функции необходимо активизировать. Те компоненты, которые не активизированы при инсталляции, можно активизировать позже, когда в них возникнет необходимость. Например, при активизации стека TCP/IP автоматически активизируются только клиентские приложения и сервер Telnet; все остальные сервера (Web, FTP, NFS, LPD и другие) могут быть запущены позже, а могут вообще не использоваться.

С другой стороны, сервисы безопасности OS/390 по умолчанию разрешают все, что не запрещено. Для достижения обратного эффекта необходима их серьезная настройка. При активизации новых продуктов и приложений необходим контроль над тем, какое влияние они могут оказать на целостность системы безопасности.

После активизации RACF в его базе данных существует лишь один пользователь, активны всего три класса защиты и ни одного профиля защиты. В этом случае пользователи могут получать неограниченный доступ к системе через приложения, не пользующиеся RACF для аутентификации. Для того, чтобы реализовать принцип «все запрещено, что не разрешено», необходимо, во-первых, активизировать необходимые классы защиты и профили защиты в них, во-вторых, определить пользователей и, объединив их в группы, установить правила доступа пользователей и групп к ресурсам, и, в-третьих, запретить приложениям использовать не-RACF аутентификацию.

Следует отметить, что новые, недавно включенные в OS/390 приложения и функции следуют этому принципу. Они не позволяют выполнять определенные действия, пока они не будут явно разрешены. В качестве примера можно привести HCD и Firewall.

7.2. Непрерывность защиты в пространстве и времени, невозможность обхода защитных средств

Защита должна осуществляться все время и, в частности, в периоды регламентных работ, действий прикладных и системных программистов, системных администраторов.

Сервер безопасности OS/390 декларирует именно такой подход к безопасности ресурсов. Для обращения пользователей к защищенным ресурсам менеджеры ресурсов обязательно запрашивают степень авторизации этих пользователей у RACF или аналогичного продукта. Этот принцип в OS/390 может быть нарушен в следующих случаях:

1) **Использование сетевых сервисов**. Многие сервера, обеспечивающие доступ к OS/390 по сети (например, сервер Web) не обеспечивают его защиты по умолчанию. Для безопасности доступа необходимы дополнительные настройки этих серверов. Перед началом использования подобных сервисов необходимо тщательное планирование их настройки с точки зрения безопасности.
2) **Использование привилегированных (авторизованных) команд ассемблера**. Программа, использующая такие команды, может выполнить любые действия в обход системы безопасности. По умолчанию создание и запуск таких программ разрешен. Используя функции сервера безопасности совместно с Authorized Program Facility (APF), необходимо на этапе инсталляции операционной системы запретить создание и выполнение таких программ (за исключением системных).

7.3. Равнопрочность обороны по всем направлениям

Посредством грамотной настройки системных компонентов и анализа собираемой информации можно практически исключить слабые звенья защиты на техническом уровне. Путем разграничения функций администрирования и аудита системы безопасности, а также разделения функций администрирования между несколькими администраторами можно минимизировать воздействие человеческого фактора на надежность защиты.

7.4. Эшелонированность обороны

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией — управление доступом и, как последний рубеж, — протоколирование и аудит, затрудняющие незаметное выполнение злоумышленных действий.

Архитектура S/390 в силу своей централизации позволяет упростить физическую защиту.

В Сервере безопасности OS/390 реализованы все перечисленные средства программно-технической защиты, требующие лишь настройки. RACF выполняет идентификацию и аутентификацию пользователей, менеджеры ресурсов — управление доступом, и, наконец, RACF и SMF — протоколирование и обеспечение аудита.

7.5. Архитектурная безопасность

Архитектурная безопасность базируется на соблюдении следующих принципов:

- простота архитектуры, минимизация и упрощение связей между компонентами, унификация и упрощение компонентов, использование минимального числа протоколов;
- апробированность решений, ориентация на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку;
- построение системы из компонентов, обладающих высокой надежностью, готовностью и обслуживаемостью;
- управляемость, возможность сбора регистрационной информации обо всех компонентах и процессах, наличие средств раннего выявления нарушений информационной безопасности, нештатной работы аппаратуры, программ и пользователей;
- простота эксплуатации, автоматизация максимального числа действий обслуживающего персонала.

Операционная система OS/390 имеет длительную историю развития, некоторые элементы унаследованы еще от OS/360 и весьма архаичны, поэтому принцип простоты архитектуры для нее выполним не в полной мере. Однако существует возможность в определенных пределах минимизировать число компонентов и упростить их.

Компоненты OS/390, в основном, делятся на две группы. Первая группа включает компоненты, унаследованные из предшествовавших операционных систем начиная с 1960-х годов. Вторая группа — компоненты, попавшие в OS/390 из мира Unix. И те, и другие компоненты прошли многолетнюю апробацию; большинство факторов риска из этих компонентов исключено. Этим же обуславливается их высокая надежность. С точки зрения обслуживания компоненты OS/390 не являются простыми, что обусловлено широтой и сложностью решаемых ими задач, а также высокой гибкостью этих компонентов.

Как аппаратные средства S/390, так и программные средства OS/390 обеспечивают широчайшие возможности для сбора информации о протекании процессов, а также о нештатных ситуациях. Имеется возможность как протоколирования такой информации с дальнейшей обработкой, так и немедленного оповещения ответственных лиц при возникновении нештатных ситуаций.

Все компоненты OS/390 можно настроить таким образом, чтобы максимально упростить их эксплуатацию. С использованием системных средств, языков программирования возможно создание сценариев, как работающих внутри одного приложения, так и использующих различные приложения и сервисы. Существует также ряд других способов автоматизации действий пользователей и обслуживающего персонала, начиная от определения функциональных клавиш и до использования специализированных средств сторонних производителей (например, функция Automation Option программного продукта NetView).

8. Анализ возможных подходов к реализации модулей шифрования, соответствующих отечественным стандартам

Существует три возможных подхода к реализации модулей шифрования для обеспечения конфиденциальности передаваемых данных в OS/390.

I. **Создание аппаратно-программного комплекса криптографии под управлением OS/390**. В OS/390 существует возможность написания UIM (драйверов) для любого нестандартного периферийного оборудования, подключаемого к мэйнфрейму по параллельному, ESCON или FICON интерфейсам. Таким образом, существует возможность создания программного или программно-аппаратного комплекса шифрования, работающего под управлением OS/390. В частности, можно добиться того, что ни по одному внешнему интерфейсу мэйнфрейма не будут передаваться нешифрованные данные.

   При таком подходе:
   - возможно организовать перехват любых данных и их шифрование «на лету»;
   - во-вторых, обеспечивается высокая надежность криптосистемы, обусловленная надежностью работы OS/390 в целом;
   - в-третьих, легко обеспечить отсутствие «узких мест» по производительности ввода/вывода.

   Недостатком является необходимость использования высококвалифицированных разработчиков.

II. **Использование OCSF**. В OS/390 входит ряд программных продуктов, обеспечивающих функции шифрования. Ряд из них использует также аппаратную поддержку, например, криптографические сопроцессоры и другие подобные устройства. Использование их напрямую неприемлемо, однако, один из программных продуктов (OCSF — Open Cryptographic Services Facility) позволяет обеспечить подключение собственных программных или программно-аппаратных модулей шифрования, для использования их затем прикладными программами через интерфейс API.

   Архитектура OCSF включает в себя 4 уровня:
   - Application Domains обеспечивает поддержку приложений.
   - System Security Services обеспечивает протоколы безопасности, используемые на уровне Application Domains, и включает в себя утилиты, необходимые для инсталляции и конфигурации OCSF.
   - OCSF Framework является центральным компонентом этой архитектуры и обеспечивает механизм управления модулями поставщиков услуг, для доступа к которым обеспечивается прикладной программный интерфейс (Application Programming Interface, API).
   - Service Providers (поставщики услуг) — программные и аппаратные компоненты, обеспечивающие необходимые способы защиты.

   Такой подход требует немного меньше усилий разработчиков, чем первый, однако, не обеспечивает той же функциональности. В частности, использование OCSF возможно только пользовательскими программами, написанными с использованием API; системные сервисы его использовать не могут.

III. Использование внешнего криптосервера. Этот подход требует меньше всего усилий на реализацию, поскольку может быть использовано апробированное решение, однако, к его производительности при высокоскоростном обмене данных должны предъявляться высокие требования.

   Требуется тщательное изучение интенсивности возможного трафика через криптосервер, изучение возможных последствий остановок криптосервера (неизбежных при использовании любой компьютерной платформы для его реализации), а также изучение способов предотвращения перегрузки криптосервера и последствий возможной перегрузки для того, чтобы определить требования к производительности внешнего криптосервера.

Заключение

1. Основными особенностями платформы S/390, определяющими возможные архитектурные решения подсистемы информационной безопасности, являются:
   - Централизованная система управления, предполагающая также и централизованное управление подсистемой информационной безопасности.
   - Вычислительные машины, относящиеся к этой платформе, можно разделять на несколько логически независимых частей, на каждой из которых могут решаться независимые задачи, возможно под управлением различных ОС.
   - Платформа S/390 является продуктом длительного эволюционного развития, решения в области безопасности хорошо апробированы и содержат целый арсенал средств обеспечения информационной безопасности на аппаратном, системном, прикладном уровнях.
2. Аппаратные средства S/390 в сочетании с соответствующим программным обеспечением позволяют организовать одновременную работу на одной ЭВМ нескольких пользователей, использующих общие ресурсы ЭВМ, и обеспечить высокий уровень защиты от несанкционированного доступа пользователей к программам и данным друг друга, пользователей к программам и данным системы, а также к общим ресурсам системы.
3. На системном уровне (уровень ОС) реализована архитектура информационной безопасности (Security Architecture) OS/390. Базовая составляющая этой архитектуры — RACF обеспечивает защиту информационных ресурсов системы и администрирование средств защиты из единого центра.
4. Криптографическая защита, соответствующая Российским стандартам, может быть реализована тремя способами:
   - написание драйверов (UIM), обеспечивающих шифрование «на лету»;
   - написание собственных функций шифрования, что допускается в ряде программных продуктов;
   - использование внешнего криптосервера.

Выбор наиболее предпочтительного способа зависит от ряда факторов.

Литература

1. Документация по IBM Security Server.
2. Документация по IBM 9672.
3. Информация по операционным системам IBM для мэйнфреймов.
4. Дополнительные материалы по вычислительным комплексам с архитектурой S/390.
5. Дополнительные материалы по обеспечению режима информационной безопасности в больших вычислительных комплексах.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
email: JetInfo@jet.msk.su
http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555