Основные проблемы защиты информации в GRID-системах и некоторые пути их решения

Т.А. Шантина

Шуйский государственный педагогический университет

В настоящее время практически в каждой развитой стране развернуты национальные GRID-проекты, имеющие целью создание соответствующей инфраструктуры и развитие технологий, обеспечивающих удаленный доступ к разнообразным вычислительным ресурсам независимо от места расположения потребителя. Во многих странах созданы отдельные государственные органы для разработок по GRID.
интеграция баз данных.

Использование Grid-технологий позволяет решать научные, научно-практические, инженерные, медицинские и социально значимые задачи высокой информационной сложности, к решению которых до появления Grid невозможно было подступиться.

Grid-технологии представляют собой набор средств и технических решений (программных, аппаратных, организационных и т.д.), которые позволяют разрозненные разнородные компьютеры и суперкомпьютеры объединять в территориально-распределенную гетерогенную информационную и вычислительную систему. Иными словами, это объединение всех компьютеров мира в единую систему – в виртуальный суперкомпьютер невиданной мощности. Это позволит распределять и перераспределять ресурсы между пользователями, где бы они ни находились. У пользователя появляется ощущение, что вся информация, за которой он обратился, находится рядом, например, на сервере того провайдера, к которому он подключен

При построении такой системы возникает множество проблемы, одна из которых заключается в том, как обеспечить безопасность информации в GRID-системах?

Для реализации задачи ощущения пользователем того, что вся информация, необходимая ему, находится рядом, необходимо объединить всю информацию в единую базу данных, да еще и с многоканальным доступом. Построить защиту такой базы данных без присущего уже сейчас для Интернета значительного числа отказов, ответов о действительной недоступности этой информации, о превышении допустимого времени поиска, об ошибках становится задачей первостепенной важности. Цель защиты — перекрыть доступ к ресурсам и информации для тех пользователей, которые не имеют соответствующих привилегий. Таким пользователем может стать и собственник, предоставивший свой компьютер в аренду или по договору на время простоя.

Слишком сложные механизмы защиты могут негативно повлиять на производительность. Поэтому следует сначала определить приложения, для которых такой уровень защиты оправдан. Необходима возможность динамического управления уровнем защиты на основе конкретных условий работы. Такие механизмы, как локальное кэширование правил для принятия повторяющихся решений с синхронизацией, позволят увеличить производительность системы. Кроме того, для GRID потребуются апробированные методологии, благодаря которым можно будет разрешать конфликты между правилами, возникающие из-за слияния множества распределенных политик контроля доступа.

При создании архитектуры защиты для GRID нужно обеспечить поддержку широкого спектра требований к безопасности — от приложений, требующих минимальной защиты или вовсе в ней не нуждающихся, до круга задач, которым необходим высокий уровень конфиденциальности.

Базовыми элементами защиты остаются аутентификация, механизм авторизации, конфиденциальность и целостность данных, биллинг и аудит, строгое выполнение обязательств.

Аутентификация - это процесс проверки подлинности идентификационных данных, или удостоверений, участника взаимодействия. В традиционных системах аутентификация нацелена на защиту сервера. В GRID, однако, для того чтобы уберечься от самозванцев, не менее важно проверять аутентичность сервера.

Механизмы авторизации определяют, допускает ли система реализацию затребованной операции. В GRID для принятия решений подобные механизмы должны действовать на основе всех правил, установленных для каждого ресурса.

Необходимо гарантировать конфиденциальность и целостность данных. Передаваемые или хранимые данные должны быть защищены с помощью адекватных механизмов, препятствующих нелегитимному доступу. В некоторых случаях нужно сделать так, чтобы нелегитимные пользователи даже не узнали о существовании этих данных.

Биллинг и аудит играют важную роль в GRID. При создании крупномасштабных GRID -структур в коммерческом секторе, организациям потребуются механизмы, способные контролировать и подсчитывать объем использованных ресурсов и обеспечиваемых ими служб. Расчетные механизмы также гарантируют, что все стороны соблюдают соглашения об использовании ресурсов. Аудиторская информация о выполненных операциях дает возможность восстановить источник опасности или нарушения защиты.

Строгое выполнение обязательств подразумевает возможность определить, что данный участник выполнил определенную задачу или согласился на ее выполнение, даже если сам он это отрицает. В среде с большим числом участников, такой как GRID, возможность подтвердить соответствие между задачами и людьми, которые должны их выполнять, имеет немаловажное значение, особенно в спорных ситуациях.

GRID содержит различные административные домены, каждый из которых имеет свой автономный механизм защиты. Эффективная архитектура защиты должна обеспечивать протоколы, позволяющие компенсировать различия между автономными механизмами, и при этом предоставлять каждому локальному узлу полный контроль над относящимися к нему ресурсами.

В крупномасштабных GRID становится невозможным присваивание каждому пользователю регистрационного имени для доступа к каждой удаленной машине, к которой он захочет обратиться, так как число пользователей становится невероятно большим. Более правильным будет динамическое присваивание пользователю удостоверения на ресурсе, выбирая из пула удостоверений то, которое в наибольшей мере соответствует роли или правам этого потребителя.

Организации, участвующие в работе GRID, должна иметь свои собственные механизмы защиты. Организации могут просто адаптировать имеющиеся у них ресурсы к работе в среде GRID. Нужно, чтобы пользователи могли применять свои локальные идентификационные данные для аутентификации внутри своего собственного домена, а затем, с учетом аутентификационного контекста, получать доступ к удаленным узлам. Таким образом, защитная структура должна обеспечивать трансляцию аутентификационного контекста из локального домена в общее представление, которое могут использовать другие узлы.

Создать доверительные отношения в GRID тоже непросто. Субъект X может совместно работать с двумя субъектами, которые конкурируют между собой и не должны знать о совместной работе X с соперником. В такой ситуации контексты должны оставаться изолированными, а сам факт существования каждого из них — оставаться конфиденциальным.

Еще один сценарий использования GRID предусматривает делегирование мандатов. Пользователь A может предоставить свои права доступа субъекту Y, позволив ему обращаться к ресурсу GRID от имени A. Это усложняет доверительные отношения, поскольку ресурс может доверять самому пользователю, но не Y, хотя у последнего есть мандат, переданный ему A. Зеркалирование сложных социальных соглашений и согласований правил существенно затрудняет создание GRID-системы и защиту находящейся в ней информации. Частично можно решить эту проблему используя кратковременные мандаты, созданные на основе постоянных мандатов пользователей. Интерактивное хранилище мандатов может содержать мандаты пользователей и предоставлять по мере необходимости мандаты с меньшим сроком действия.

Архитектура GRID должна скрывать от пользователей сложности организации тех или иных процессов, позволять им поддерживать свои локальные шаблоны доступа и при этом предоставлять возможности GRID-систем. Однако, приложения в GRID могут предъявлять свои требования к защите. Для защиты GRID программное обеспечение промежуточного уровня должно включать в себя механизмы, позволяющие выполнить все эти требования.

Менеджеры ресурсов хотят быть уверены в конфиденциальности пользователей и ресурсов. Им может потребоваться скрыть не только данные, но и само их существование. Кроме того, архитектура защиты должна оберегать систему от вредоносного кода пользователей из других организаций.

Участники GRID-систем хотят быть уверены, что их системами не будут злоупотреблять, и что другие стороны обеспечат обусловленное заранее качество обслуживания. Хотя межсетевые экраны способны защитить системы своих организаций от недобросовестного использования, они могут препятствовать и легитимным взаимодействиям. Даже если, несмотря на все предосторожности, возникает угроза или происходит атака, расчетная информация должна быть доступна, поскольку именно она позволяет установить, какая из сторон послужила источником угрозы. Но поскольку расчетная информация является распределенной, добиться этого непросто; крайне важно, чтобы все заинтересованные стороны предоставляли корректную информацию. Еще одна проблема — разумное использование этой информации.

Динамическая природа доверительных отношений GRID также влияет на защиту ресурсов. Например, в конце любого конкретного взаимодействия организации-участники должны иметь возможность закрыть доступ, чтобы предотвратить нелегитимное обращение к своим ресурсам. Изменения в информации, необходимой для аутентификации и определении прав доступа, следует распространять на все соответствующие субъекты в GRID.

Правила управления ресурсами, охватывающими тысячи узлов в GRID-системах, — настоящий кошмар для администраторов. Им необходимо размещать и контролировать ресурсы, чтобы выявлять их недобросовестное использование. Если GRID объединяет множество узлов, администраторы должны установить и поддерживать иерархию Certificate Authority (CA). Прежде чем будет выполнена любая транзакция, следует сформировать иерархию CA и уполномоченных по регистрации, установив между ними доверительные отношения.

Сейчас специалисты по защите GRID занимаются, в первую очередь, созданием строительных блоков, которые могут стать основой для распределенной инфраструктуры защиты, рассчитанной на критически важные приложения и коммерческие реализации GRID следующего поколения. С этой целью специалисты определяют протоколы и механизмы, позволяющие создавать над инфраструктурами организаций защитные «купола», которые необходимы для формирования доверительной среды при совместном использовании ресурсов. Приоритетной при создании защиты для GRID является

разработка протоколов, которые будут предотвращать нелегитимный доступ, поддерживая при этом интероперабельность между разнородными узлами GRID. Для создания производственных сред GRID необходимо решить вопросы, связанные с обнаружением вторжений и минимизацией возможного вреда от них. Протоколы защиты GRID должны обеспечивать интероперабельность, поддерживая при этом различные локальные домены. Сейчас установление доверительных отношений и инициация совместной работы предполагают значительную трату времени и сил. Чтобы обеспечить эффективную совместную работу в среде GRID, потребуются автоматические протоколы для формирования динамических GRID и правил доступа в режиме реального времени. И службам, и клиентам необходима возможность устанавливать соглашения об уровне обслуживания, предусматривающие поддержку определенных параметров защиты и тем самым позволяющие повысить уровень достоверности информации.

Литература

1. Lavanya Ramakrishnan. Securing Next-Generation Grids. IEEE IT Pro, March — April 2004. IEEE Computer Society, 2004, All rights reserved. Reprinted with permission. Постоянный URL статьи: http://www.osp.ru/os/2004/06/184471/
2. С.М.Абрамов, А.А. Московский, В.А. Роганов, П.Е. Велихов Суперкомпьютерные и GRID-технологии., доклад
3. Intuit – информационный ресурс в сети Интернет, http://www.intuit.ru