Инфраструктура безопасности для динамических Грид-приложений - Обзор технологий

Демченко Ю., University of Amsterdam
demch@science.uva.nl

Аннотация
В докладе рассматриваются современное состояние технологий и проблемы построения распределенной инфраструктуры безопасности для динамических Грид-приложений. Сформулированы основные требования к сервисам безопасности и рассмотрена их интерграция с основными сервисами инфраструктуры Грид-приложений. Расмотрено использование рабочих потоков (workflow) для композиции динамических сервисов и управления контекстом безопасности. Описана модель системы контроля доступа для динамических Грид-сервисов и рассмотрены механизмы управления контекстом безопасности используя возможности XML-технологии. Дополнительно рассмотрены особенности использования концепции Виртуальных Организайи (ВО) для создания динамических ассоциаций пользователей и ресурсов. Предполагается, что данный доклад сможет сыграть положительную роль в определении перспективных направлений для исследований в области Грид приложений и сервисов безопасности для российского академичекого и университетского сектора.

1. Введение

Дальнейшее расширение использования Веб-сервисов (XML Web Services) [1] и Грид (Grid) [2] для реальных промышленных применений связано с возможностью создания динамических Грид-приложений, которые позволяли бы учитывать специфические требования и конфигурацию пользовательских задач, предоставлять услуги по требованию (on-demand), а также обслуживать динамически создаваемые виртуальные ассоциации пользователей и ресурсов. Предложенная Global Grid Forum (GGF – организация стандартизаци в Грид) Открытая Архитектура Грид-Сервисов (ОГСА, OGSA – Open Grid Services Architecture [2]) определяет базовые Грид-сервисы и интерфейсы и предоставляет базовую платформу для создания распределенных динамических Грид-сприложений. Важно отметить, что OGSA предполагает реализацию грид-сервисов на основе Веб-сервисов используя специальный профиль для описания Веб-сервисов в виде ресурсов с состоянием WSRF (Web Services Resource Framework) [3].

Реализация Грид-приложений требует специальной инфраструктуры Грид-сервисов (GridMW - Grid middleware), которая включает инфраструктуру обмена сообщениями и общих Грид-сервисов, которые архитектурно размещаются между уровнем приложений и сетевым уровнем [2]. В последнее время GridMW нашла свое развитие в рамках больших международных проектов и консорциумов таких как EGEE ((Enabling Grid for E-sciencE, http://public.eu-egee.org/), OSG (Open Science Grid, http://www.opensciencegrid.org), и Globus Alliance (http://www.globus.org/). Однако существующие решения в основном ориентированы на обьединение в Грид распределенных вычислительных ресурсов. Более широкое применение Грид для поддержки распределенных систем коллективной работы (GCE - Grid-based Collaborative Environment) требует решения множества дополнительных технических и операционных вопросов как на архитектурном, так и на уровне самих Грид-сервисов. В первую очередь это касается динамического вызова Грид-сервисов и поддержки соответствующих услуг-безопасности в динамическом режиме работы Грид-приложений.

Современные разработки GridMW, такие как Globus Toolkit version 4 (GT4, http://www.globus.org/toolkit/), позволяют стандартным образом интегрировать сервисы безопасности с основными сервисами на уровне контейнера, сообщений или самих сервисов (http://www.globus.org/toolkit/docs/4.0/security/). Дальнейшее развитие GridMW как архитектуры, ориентированной на сервисы (СОА, SOA – Service Oriented Architecture), предьявляют новые специфические требования к услугам безопасности [2, 4].

Целью данной статьи является предоставить краткий обзор существующих технологий и проблем в области построения динамически конфигурируемых сервисов безопасности для распределенных систем коллективной работы и динамического развертывания сервисов на основе Грид для определения возможных направлений исследований в области Грид-приложений и сервисов безопасности для российского академичекого и университетского сектора.

2. Особенности модели безопасности Грид-сервисов

Современная модель безопасности в Грид имеет следующие особенности (по сравнению с клиент-серверной моделью безопасности, используемой в большинстве сетевых и веб-приложений):

- Концепция Виртуальных Организаций (ВО, VO - Virtual Organisation) используется для виртуализации ресурсов и ассоциации ресурсов и пользователей
- Модель безопасности, ориентированная на услуги и позволяющая ассоциировать услуги и политику безопасности с Грид-сервисами, пользовательскими задачами или данными, представленными в виде идентификатора единого формата (так называемого End Point Reference (EPR) [3]).
- Использует механизмы безопасности на уровне сообщений, унаследованные от Веб-сервисов, при этом информация, относящаяся к безопасности, включается в заголовок используемого XML-формата сообщений SOAP (Simple Object Access Protocol) [5].
- Контроль доступа основан на мандатах идентификации (Identity Credentials) с использованием для целей аутентификации (AuthN) специального типа временных мандатов прокси-сертификатов (X.509 Proxy Certificates) [6], которые используются также для единого доступа к Грид-ресурсам (Single-Sign-on) и делегирование пользовательских полномочий при запуске распределенных задач.
- Использование глобальной системы управления доверием для Системы Открытых Ключей (СОК, PKI – Public Key Infrastructure) в Грид, основой которой является международная федерация IGTF (International Grid Trust Federation, http://www.gridpma.org/).
- Авторизация и контроль доступа основаны на использовании сертификатов атрибутов, выдаваемых службой членства в ВО (так называемый VOMS X.509 Attribute Certificate) [7].
- Используя стандартный для Веб-сервисов формат описания WSDL (Web Services Description Language) [8], сервисы и политика безопасности могут быть динамически добавлены к основным сервисам во время разворачивания и конфигурации этих сервисов, что позволяет независимо разрабатывать и одновременно безопасным образом комбинировать все компоненты приложения.
- В частном случае доступа к распределенным компьютерным ресурсам, модель контроля доступа строится на основе принятого в распределенных компьютерных системах динамического запуска пользовательских задач от имени одного из системных пользователей (так называемых pool accounts), назначаемых динамически на время выполнения текушей задачи.
- С точки зрения сетевой безопасности и сетевых экранов, некоторые Грид-сервисы могут использовать нестандартные порты из диапазона, который многие системы обнаружения атак могут расценивать как внешние атаки. Например, один из наиболее важных протоколов для обмена огромными массивами данных в Грид GridFTP может использовать одновременно несколько параллельных потоков данных через порты в диапазоне выше 1024, который выделен для свободного использования сетевыми приложениями [9].

3. Системы для коллективной работы и комплексного развертывания ресурсов на основе Грид и автоматизация рабочих потоков

Важными областями применения Грид являются системы для коллективной работы (СКР) и комплексного развертывания ресурсов по требованию (КРРТ, complex resource provisioning). При этом сама архитектура построения Грид на основе СОА предоставляет возможности динамического создания таких систем на время выполнения определенных задач и с учетом множества параметров, определяемых самим пользователем или зависимым от конкретной задачи и ее потребности в ресурсах. Обеспечение безопасной среды выполнения пользовательских задач при использовании общих физических ресурсов и общей исполнительной среды является особенно актуальным в случае доступа к супер-компьтерным ресурсам и к уникальному экспериментальному оборудованию как в научных исследованиях так и в наукоемких отраслях промышленности.

Типичные применения СКР предьявляют следующие требования к инфраструктуре Грид-сервисов [10]:

- Возможность динамического конфигурирования и развертывания для каждой задачи или эксперимента и возможность задания специфической конфигурации и начальных условий.
- Возможность работы в пределах множества административных и доверительных доменов.
- Возможность использования различных пользовательских мандатов идентификации и атрибутов, которые определяются множеством политик безопасности как отдельных доменов так и ВО.

До настоящего времени такие проблемы решались вручную посредством ручной конфигурации сервисов при их установке, что приводило к медленному разворачиванию новых приложений и высоким накладным административным расходам. Недостаточная формализация определения комплексных услуг и сложность управления рабочими потоками может приводить к медленной адаптации системы к возможным изменениям конфигурации системы, политики доступа, а также состава пользователей и их полномочий.

Использование Грид для построения систем КРРТ является самостоятельной задачей, но может также быть частью создания инфраструктуры СКР, например, обеспечение высокоскоростных каналов для наблюдения за ходом эксперимента или обеспечение доступа к результатам эксперимента, при этом подобные каналы реально могут предоставляться несколькими независимыми провайдерами. Типичный процесс комплексного развертывания

ресурсов в КРРТ включает 4 базовых этапа: поиск и обнаружение ресурсов (resource lookup); композиция комплексного ресурса, включая возможные варианты; резервирование индивидуальных ресурсов и ассоциация их с квитанцией, которая будет определять доступ к комплексному ресурсу в процессе его использования; и наконец, предоставление или доставка такой комплексной услуги или ресурса. Процесс резервирования и в некоторых случаях доставки может потребовать выполнения сложной последовательности действий, включая получение авторизации на использование индивидуальных ресурсов.

Предполагается, что использование современных средств управления рабочими потоками (СУРП) позволит автоматизировать большинство операций в обоих случаях СКР и КРРТ, предоставив дополнительно возможность управления контекстом безопасности в ходе выполнения эксперимента или предоставления ресурса [11]. В сервис-ориентированной архитектуре Грид-приложений СУРП может использоваться также как средство для интеграции/композиции динамических Грид-сервисов. Статья [12] предоставляет обширный обзор современных технологий СУРП для научных приложений (SWMS - Scientific Workflow Management Systems). Большинство SWMS исторически разрабатывались в рамках отдельных научных проектов и поэтому имеют ограниченые применение для специфических научных задач. В то же время, с развитием Веб-сервисов, промышленность уделяла значительное внимание следующему этапу автоматизации бизнес-приложений, используя возможность динамического развертывания приложений на основе Веб-сервисов. В настоящее время стандартизация описания рабочих потоков для бизнес процессов развивается в рамках специального комитета OASIS Web Services Business Process Execution Language (WSBPEL) [13].

Доступные в настоящее время средства проектирования BPEL и SWMS позволяют существенно упростить процесс автоматизации научных экспериментов и бизнес- процесов, но множество вопросов интеграции со службами безопасности и осуществления политики безопасности являются открытыми. В свою очередь системы управления рабочими потоками могут быть использованы для управления динамически изменяемым контекстом безопасности в процессе выполнения эксперимента или предоставления комплексных услуг.

4. Динамические Грид-сервисы и требования к инфраструктуре безопасности

В ОГСА и ее реализации в Globus Toolkit GT4, динамика Грид-сервисов рассматривается в двух аспектах: (1) динамическая композиция и развертывание сервисов; (2) поддержка динамических ассоциаций ресурсов и пользователей. Обе проблемы должны решаться комплексно посредством такого дизайна Грид-сервисов, который бы позволял максимально гибко (и динамически) конфигурировать сервисы при их установке/развертывании, а также учитывать динамически изменяемый контекст при их вызове (включая текущие параметры окружения и исполняющей среды, а также контекст безопасности). Как уже упоминалось, средством поддержки ассоциаций пользователей и ресурсов в Грид являются Виртуальные Организации (ВО), использование которых в динамическом режиме рассмотрено в главе 6, а также в работе автора [14].

Ниже перечислены функции, которые должны быть реализованы в инфраструктуре безопасности для динамических Грид-сервисов, при этом большинство требуемых функций может быть реализовано как расширение к существующей версии Globus Toolkit version 4 (GT4).

1) Гибкая конфигурация доверительных доменов и средства меж-доменного установления доверительных отношений. В настоящее время такая конфигурация осуществляется вручную при установке сервисов безопасности и требует предварительно установленных доверительных отношений между всеми взаимодействующими системами и компонентами.
2) Динамическое управление контекстом безопасности, необходимое для поддержки рабочих потоков и комплексного развертывания ресурсов в распределенной много-доменной среде, включая следующие компоненты:
- параметры среды и административных/структурных доменов сервисов или ресурса;
- параметры среды и пользовательские полномочия текущей сессии авторизации;
- политика доступа;
- пространство имен атрибутов (Attributes namespaces);
- формат пользовательских сертификатов и мандатов (credentials);
- доверительные домены и центры удостоверения (trust domains and authorities).

При этом следует отметить, что возможность управления контекстом безопасности динамически является основой для использования рабочих потоков для автоматизации процессов в Грид-приложениях и для композиции сложных сервисов.
4) Возможность обработки и управления пространствами имен всеми компонентами инфраструктуры безопасности. В распределенной много-доменной среде пользовательские атрибуты, метаданные и политика безопасности могут использовать различные пространства имен, которые могут быть выражены непосредственно в семантике самих атрибутов или неявно посредством указания источника (или центра удостоверения атрибутов). Правильное определение и использование пространста имен является важным компонентом обеспечения совместимости сервисов в распределенной много-доменной среде. Для сервисов безопасности правильная обработка семантики атрибутов является основой для доверительности сервисов.

5) Гибкое управление политикой доступа, включая возможность использования множества форматов описания политики, средства комбинирования множества политик, средства разрешения возможных конфликтов в иерархической и многодоменной среде контроля доступа на основе политики.
6) Поддержка сессии доступа (или авторизации). Несмотря на то, что первоначальная цель установления сессии авторизации - это оптимизация быстродействия системы контроля доступа за счет исключения медленного процесса оценки запроса относительно политики доступа для повторяющихся запросов, те же механизмы и средства поддержки сессии могут также использоваться для идентификации комплексных ресурсов в задачах КРРТ. Основным механизмом поддержки сессии являются квитанции, содержащие весь необходимый контекст безопасности для данной сессии и дополнительную управляющую информацию, как следует обрабатывать данные квитанции, например возможно ли делегирование полномочий при предъявлении данной квитанции, а также существуют ли какие-либо обязательства в связи с использованием ресурсов на основании данной квитанции.

5. Контроль доступа в Грид-приложениях

Системы контроля доступа в современных Грид-приложениях используют раздельные сервисы аутентификации на основе сертификатов идентификации и системы авторизации на основе политики и ролей (или атрибутов) пользователя, определяемой как Система контроля доступом на основе политики (СКДП, RBAC - Policy/Role Based Access Control) [15, 16]. Элементами такой архитектуры являются: сервис/функция аутентификации (AuthN), функция контроля доступа (Policy Enforcement Point (PEP)), функция принятия решения о доступе (Policy Decision (PDP)), база даных политик Policy Authority Point (PAP).

В СКДП привилегии пользователя определяются набором ролей (выражаемых в форме атрибутов) и политики доступа, обычно содержащей набор правил, определяющих какие действия разрешены для конкретной роли на данном ресурсе. Политика или правила доступа определяются для триады Субьект, Ресурс, Действие (СРД, SRA - Subject, Resource, Action): Субьект запрашивает определенное Действие в отношении Ресурса. В СКДП политика определяет правила доступа, а именно возможность выполнения определенного Действия в отношении Ресурса, для Субьекта, обладающего определенными привилегиями или ролями. Ресурс является обобщенным определением обьекта доступа и может быть как реальным процессом или сервисом, так и информационным ресурсом или семантическим документом, определяемым обобщенным идентификатором в форме EPR.

Рисунок 1 изображает основные компоненты, участвующие в процессе обработки запроса на доступ к конкретному ресурсу. Авторизация или контроль доступа в целом осуществляется ресурсом, к которому запрашивается доступ, посредством размещения модуля PEP на входе ресурса; решение о доступе принимается модулем PDP на основе принятой политики доступа и в соответствии с предоставленными пользователем мандатами, которые могут включать удостоверяющие идентификаторы, полномочия или ролевые функции и другие данные, предоставляемые службой аутентификации или специальной службой атрибутов (AA - Attribute Authority). При этом все или часть исходных данных могут быть предоставлены самим пользователем (push-модель) или запрошены службой авторизации (pull-модель), соответственно функции/модули PEP/PDP также могут работать в режимах push или pull. В зависимости от конкретной политики решение PDP, возвращаемое PEP, может содержать обязательства (obligations) – действия, которые должны быть выполнены PEP в зависимости от принятого PDP решения [8].

Для повышения быстродействия, СКДП может использовать квитанции (или билеты) для повторного доступа к ресурсу (AuthzTicket), которые могут быть выданы PDP на основе начального запроса или получены пользователем от PDP предварительно. С целью дальнейшего ускорения процедуры и повышения надежности, PEP может помещать AuthzTicket в собственную кэш-память. При этом обработка AuthzTicket может производиться специальной функцией, вызываемой из PEP, без запроса PDP. Формат AuthzTicket может определяться приложением, однако для открытых систем предпочтительным является использование стандартного XML формат для описания мандатов безопасности SAML (Security Assertion Mark-up Language) [17].

Дополнительная интеграция СКДП с СУПР позволит динамически управлять контекстом безопасности в распределенной много-доменной среде и в процессе выполнения много-этапных экспериментов. Следующие компоненты общей системы контроля доступа могут использоваться для выражения и передачи контекста безопасности:

- Формат идентификаторов пользователя или сервиса ID/DN, который бы позволял использовать различные пространства имен или включать контекстную информацию непосредственно в идентификатор.
- Формат атрибутов, используемых для авторизации, должен поддерживать пространства имен и обеспечивать уникальность атрибутов (например, используя форматы X.509/X.521 или URN/SAML2.0).
- Включение доменной контекстной информации или параметров окружения в идентификатор политики доступа в формате XACML или в целевой елемент политики СРД плюс елемент окружения Environment.
- Квитанции, содержащие контекст текущей сессии авторизации или идентификатор зарезервированного комплексного ресурса.
- Мандаты динамических ассоциаций пользователей и ресурсов в форме сертификатов VOMS или других форм ассоциаций.

Основой большинства предлагаемых решений и механизмов являются XML-технологии безопасности, более подробный анализ которых и примеры использования стандартов XACML и SAML в СКДП может быть найден в работах автора [18, 19].

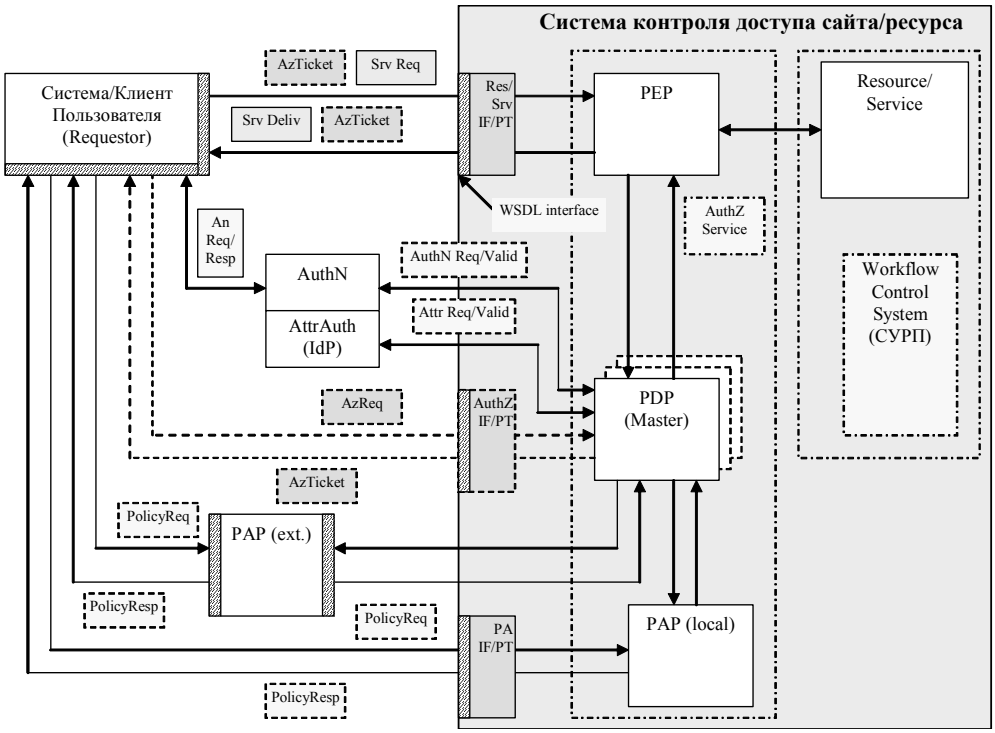

Рис. 1. Основные компоненты системы контроля доступа в динамических Грид-приложениях

Практическая реализация дополнительных функций по управлению контекстом безопасности требует пересмотра существующего дизайна основных компонентов СКДП, в первую очередь таких важных модулей как PEP и PDP. Причем возможные необходимые дополнительные функции предпочтительно должны выполнятся в форме расширения к существующим стандартным средствам контроля доступа в Грид и Веб-сервисах.

В настоящее время наиболее популярными являются следующие открытые платформы (OpenSource):
Acegi Security (*http://acegisecurity.org/*) – предоставляет комплексное решение для построения базовых сервисов безопасности (AuthN, AuthZ, защищенные каналов передачи сообщений) для промышленных приложений, в частности использущих платформу J2EE. Сервисы безопасности вызываются из програм-приложений посредством перехвата определенных типов событий при помощи соответствующим образом настроенных фильтров. Acegi предоставляет широкий выбор методов и схем аутентификации, однако выбор методов авторизации в настоящее время ограничен списками контроля доступа ACL (Access Control List). Существует стандартный метод расширения посредством добавления соответствующего фильтра к нужному приложению.
GT4 Authorisation Framework (GT4-AuthZ, *http://www.globus.org/toolkit/docs/4.0/security/authzframe/*) - является частью общей платформы безопасности GT4 и предоставляет широкий набор методов авторизации как специфических для Грид-приложений, так и общего применения на основе ACL, политики доступа XACML и другие. GT4-AuthZ использует процессор сообщений SOAP Axis (http://ws.apache.org/axis/) для вызова функций авторизации посредством соответствующей конфигурации так называемых перехватчиков (interceptor).

Схожесть методов вызова функций авторизации и способов расширения функций в обоих платформах позволяет реализавать необходимые функции обработки контекста безопасности в виде отдельного пакета GAAAPI (Generic AuthZ/AuthN API), который может быть интегрирован с Acegi Security или GT4AuthZ [11]. Набор функций, реализуемых GAAAPI, фактически поддерживает механизмы обработки контекста безопасности, перечисленные выше. Следующие функциональные модули входят в состав GAAAPI (и структурно располагаются между PEP и PDP):

- Модуль генерации и верификации квитанций авторизации (Ticket Authority), которые используются для идентификации сессии авторизации;
- Модуль обработки квитанций авторизации и контекста сессии (так называемый модуль Triage [11]);
- Модуль обработки семантики и пространства имен идентификаторов и атрибутов (Namespace Resolver);

- Модуль подготовки и трансляции атрибутов (Attribute Resolver), позволяющий привести все атрибуты к единому формату, требуемому PDP и соответствующей политикой безопасности; в своей работе модуль может также запрашивать внешнею верификацию атрибутов.

Для обеспечения возможности динамического установления контекста безопасности должна быть обеспечена возможность динамической конфигурации модулей PEP и PDP и их вызов с соответствующими модулями для обработки контекста запроса и политики доступа, а также конфигурация доверительных доменов, соответствующих взаимодействующим компонентам СКДП. При этом ввиду возможной сложной и многоэтапной оценки (комплексного) запроса по отношению к действующей политике доступа, PDP должен иметь возможность программирования процедуры оценки сложных запросов посредством внутреннего рабочего потока (или PDP micro-workflow).

6. Использование концепции Виртуальных Организаций (ВО) для создания динамических асоциаций пользователей и ресурсов

Виртуальные Организации (ВО) являются одной из базовых концепций в Грид и ОГСА и используется для создания виртуальных ассоциаций пользователей и ресурсов, предназначенных для выполнения определенных задач или более долгосрочного сотрудничества, например в рамках научно-исследовательских проектов [2, 14]. Доступ к распределенным ресурсам в таких обьединениях/ассоциациях осуществляется на основе членства в ВО и соответствующих прав/ролей пользователей. В таком определении ВО и динамические услуги связаны естественным образом.

Одной из главных задач инфраструктуры ВО является поддержка информационной базы данных на членов ВО будь-то пользователи или ресурсы, а также соответствующих атрибутов, определяющих группы пользователей, их роли и права. В современном GridMW ВО является компонентом распределенной системы контроля доступа и может выполнять следующие функции:

1) Динамическое управление доверительными отношениями/доменами – ВО как динамически создаваемая ассоциация ресурсов и пользователей может предоставлять контекст безопасности для системы контроля доступа, включая системы аутентификации (AuthN) и авторизации (AuthZ).
2) Преобразование атрибутов и мета-даных – такая необходимость возникает в связи с тем, что в динамически создаваемых ВО пользователи могут использовать свои исходные мандаты и атрибуты, выданные им в их “домашних” организациях.
3) Комбинация политики доступа – “федеративная” политика ВО может определять как специфические правила функционирования ВО так и правила обьединения политик членов ВО, включая возможное разрешение конфликтов.

В современных Грид-проектах ВО создаются для целей проекта на основе формального договора между членами ВО, который определяет ресурсы выделяемые для целей ВО, политику и общие службы ВО, в первую очередь членская служба (ВОЧС, VOMS – Virtual Organisation Membership Service), которая является основой для предоставления услуг или доступа к общим ресурсам и услугам ВО. В реальной жизни, организации могут предоставлять ресурсы множеству ВО и пользователи могут быть членами множества ВО, при этом система контроля доступа должна предоставлять возможность пользователям выбирать мандаты какой ВО они хотят предоставить в конкретном запросе на услуги.

Фактически ВО устанавливает свой административный домен – на основе договора между членами ВО, и доверительный домен – на основе установления общей иерархии PKI или взаимного обмена сертификатами PKI между основными сервисами, ресурсами и членами ВО, при этом ВОЧС служит в качестве доверительного брокера пользовательских аттрибутов и/или сертификатов. ВО могут рассматриваться как решение для установления безопасной среды для коллективной работы между предприятиями членами ВО без изменения собственной политики безопасности членов ВО в условиях, когда собственно ресурсы, делегированные в ВО, и сами пользователи находятся в пределах зоны безопасности предприятий и администрируются в соответсвии с внутренней политикой безопасности и доступа. При этом естественно система контроля доступа должна быть построена таким образом, чтобы основываясь на доверительных мандатах идентификации была возможность использовать атрибуты членства в ВО.

Стандартом де-факто для реализации функций ВОЧС является широко применяемая в современных Гри-проектах одноименная система VO Membership Service (VOMS) [5]. VOMS предоставляет пользовательские атрибуты, необходимые для авторизации доступа к ресурсам ВО, а также поддерживает базовые функции регистрации пользователей посредством программы администратора. Хотя изначально VOMS проектировалась для поддержки «статических» ВО для больших проектов, она может быть адаптирована для создания и управления динамическими ВО или ассоциациями и использована в системах с динамическим разворачиванием ресурсов на основе Грид. Основой для создания динамических ВО так же как и более «статических» ВО должен служить

формальный документ, определяющий административный и доверительные домены ВО, а также основные службы ВО, которые реально могут предоставляться соответствующими службами реальных организаций. Однако процесс договаривания о создании новой ВО должен быть хорошо формализован и поддаваться автоматизации. Решение указанных вопросов и построение гибкой инфраструктуры динамических ВО является на сегодняшний день актуальной темой научных исследований в Грид и GridMW.

7. Выводы

Приведенный в статье обзор технологий и проблем построения инфраструктуры безопасности для динамических Грид-сервисов имеет своей целью ввести читателя в курс ведущихся работ в области безопасности Грид-приложений в рамках международных проектов или консорциумов (таких как EGEE, OSG или Globus Alliance), а также предоставить начальную информацию для определения возможных перспективных направлений научных исследований. Предполагается, что для дальнейшего понимания и освоения обсуждаемых технологий исследователи и разработчики обратятся к использованным источниками и другим работам.

Описанные модели и решения нашли свое развитие и внедрение в двух основных проектах с участием автора Collaboratory.nl и EGEE. Информация о программном продукте **aaauthreach.org,** реализующем базовые функции СКДП и предоставляющим пример использования стандартных языков XACML и SAML, может быть найдена в [20].

Литература

[1] “Web Services Architecture,” World Wide Web Consortium Working Group Note, 11 November 2004, available from http://www.w3.org/TR/ws-arch/

[2] Foster, I. et al, “GFD.30, The Open Grid Services Architecture, Version 1.0,” Global Grid Forum, 25 January 2005. - http://www.gridforum.org/ documents/GWD-I-E/GFD-I.030.pdf

[3] Web Services Resource Framework. - http://www.globus.org/wsrf/

[4] Security in a Web Services World: A Proposed Architecture and Roadmap, Version 1.0, A joint security whitepaper from IBM Corporation and Microsoft Corporation. April 7, 2002, http://www-106.ibm.com/developerworks/library/ws-secmap/

[5] SOAP Version 1.2 specification. - http://www.w3.org/TR/soap12

[6] RFC3280. Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile. - http://www.ietf.org/rfc/rfc3820.txt

[7] "VOMS Architecture v1.1," http://grid-auth.infn.it/docs/VOMS-v1_1.pdf, February 2003.

[8] Web Service Definition Language (WSDL). W3C Note 15 March 2001 – http://www.w3.org/TR/wsdl

[9] GGF Recommendation GFD-R.20. GridFTP: Protocol Extensions to FTP for the Grid. - http://www.ggf.org/documents/GFD.20.pdf

[10] Policy Based Access Control in Dynamic Grid-based Collaborative Environment, by Yuri Demchenko, Leon Gommans, Cees de Laat, Andrew Tokmakoff, Rene van Buuren. - The 2006 International Symposium on Collaborative Technologies and Systems (CTS2006), 14-17 May, 2006 Las Vegas.

[11] Using Workflow for Dynamic Security Context Management in Grid-based Applications, by Yuri Demchenko, Leon Gommans, Cees de Laat, Arie Taal, Fred Wan. - Submitted paper to the Grid2006 Conference, Barcelona.

[12] Zhiming Zhao et al, “Scientific workflow management: between generality and applicability,” The 5th international conference on quality software, Melbourne, Australia, Sep. 19 -20, 2005.

[13] “Web Services Business Process Execution Language. Version 2.0”, OASIS Committee Draft, 21 December 2005, available from http://www.oasis-open.org/committees/download.php/16024/wsbpel-specification-draft-Dec-22-2005.htm

[14] VO-based Dynamic Security Associations in Collaborative Grid Environment, by Yuri Demchenko, Leon Gommans, Cees de Laat, Martijn Steenbakkers, Vincenzo Ciaschini, Valerio Venturi. - Acepted paper to the COLSEC2006 Workshop, 14-17 May, 2006 Las Vegas.

[15] Role Based Access Control (RBAC) – NIST, April 2003. - http://csrc.nist.gov/rbac/

[16] Godik, S. et al, “eXtensible Access Control Markup Language (XACML) Version 2.0”, OASIS Standard, 1 February 2005, available from http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[17] Cantor, S. et al, “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0,” OASIS Standard, 15 March 2005, available from http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[18] Демченко Ю. Обеспечение гибкой системы контроля доступа в Веб-сервисах и Грид-системах.- Материалы конференции RELARN-2005. - 14-18 June, 2005, Nizhny Novgorod, Russia.

[19] Using SAML and XACML for Authorisation assertions and messaging: SAML and XACML standards overview and usage examples, by Demchenko Y. - Draft version 0.2. - March 28, 2005. - http://www.uazone.org/demch/analytic/draft-authz-xacml-saml-02.pdf

[20] AAAuthreach framework and GAAAPI for AuthN/AuthZ services. - http://www.uazone.org/demch/projects/aaauthreach/index.html