Обеспечение гибкой системы контроля доступа в Веб-сервисах и Грид-системах

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

Аннотация
В докладе рассматриваются современные технологии построения гибкой системы контроля доступа для Веб-сервисов и Грид-систем с использованием промышленных стандартов описания политики доступа и контекста безопасности XACML и SAML соответственно. Предложена модель зон безопасности ресурса, которая может быть использована для разработки и анализа распределенных систем контроля доступа.

1 Введение

Современная архитектура безопасности Веб-сервисов (XML Web Services) и Грид (Grid) представляет собой достаточно хорошо разработанный набор стандартов, который постепенно находит свое внедрение в коммерческих и свободно-распространяемых продуктах и средствах разработки приложений [1, 2].

Базовыми функциями контроля доступа являются аутентификация и авторизация (AA - AuthN, AuthZ), корректная и эффективная реализиция которых составляет основу построения безопасных Веб-сервисов и построенных на их основе Грид-систем.

Инфраструктура безопасности веб-сервисов и Грид потребовала разработки новой концепции обеспечения безопасности выполнения задач в распределенной вычислительной среде и в среде, ориентированной на услуги (СОУ) [3, 4]. Ее отличие от сетевой системы безопасности, которая в основном обеспечивание безопасные каналы передачи данных между общающимися сетевыми узлами или компьютерами, в том, что в Грид безопасность должна быть обеспечена для задачи и данных, которые могут обрабатываться на многих компьютерных узлах и перемещаться от одного компьютера к другому в процессе выполнения. В сетевой безопасности контекст безопасности (идентификация пользоватедя, его мандаты (credentials)) обеспечиваются между двумья узлами в сети (host-to-host), в Грид безопасности контекст безопасти должен быть привязан к самой задаче или данным и обеспечивать для них такие сервисы безопасности как целостность, конфиденциальность, аутентификация и авторизация. Все эти сервисы и контекст безопасности не должны нарушаться при перемещении данных или задач от одной вычислительной системы к другой. Безопасность в Грид неизбежно требует использование всего спектра возможностей XML Security and Web Services Security (короткий обзор указанных технологий содержится в [5, 6]).

2 Современная архитектура контроля доступа на основе политики

Важной чертой современной архитектуры безопасности, ориентированной на Веб-сервисы, является разделение функций аутентификации и авторизации и использование инфраструктуры управления доступом на основе политики и ролей (или привилегий) пользователя, определяемой как Policy/Role Based Access Control (RBAC) или Система контроля доступом на основе политики (СКДП) [7, 8]. Элементами такой архитектуры являются: сервис/функция аутентификации (AuthN), функция контроля доступа (Access Enforcement Function (AEF) или Policy Enforcement Point (PEP)), функция принятия решения о доступе (Access Decision Function (ADF) или Policy Decision (PDP)), Policy Authority Point (PAP), представляющий собой базу данных, содержащую набор политик доступа (Access Control Information (ACI) или Policy).

Политика (policy) является важным компонентом современных AA-технологий и позволяет упростить управление СКДП посредством разделения процесса создания и обслуживания политики, который является скорее административной функцией владельца или оператора ресурса, и самой технической процедуры использования политики в приложениях. Политика определяет специфические требования и правила в отношении использования пользовательских данных, делегирования, соблюдения конфиденциальности и приватности, - для сервисов аутентфиикации, или правила доступа к ресурсам – для сервисов авторизации. Политика или правила доступа определяются для триады Субьект, Ресурс,

Акция (Subject, Resource, Action): Субьект запрашивает определенную Акцию в отношении Ресурса. В СКДП политика определяет правила доступа, а именно возможность выполнения определенной Акции 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 URI (Uniform Resource Identifier) [9].

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 в соответствии с предоставленными пользователем мандатами (credentials), 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 сами 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 обьязательства (obligations) – действия, которые должны быть выполнены PEP в зависимости от принятого PDP решения [8].

В более сложном случае распределенных приложений может возникнуть необходимость комбинирования политики доступа приложения или сервиса, которая реализуется СКДП, и собственно ресурса, которая как правило ограничена списком доступа ресурса (ACL – access control list) или стоп-списком (ban-list или black-list).

В открытой гетерогенной среде, которой по определению являются Веб-сервисы и Грид-системы, PEP может получить запрос, использующий различные форматы данных и использующий различную семантику запроса (или пространство имен - namespace), а также ссылающиеся на различные политики или PAP. В этом случае, PEP должен иметь возможность направить запрос соответствующему типу PDP, который способен обработать этот запрос. Существенно, чтобы запрос в целом обрабатывался одним PDP, который однако может делать запросы к другим PDP, если возникает необходимость обрабатывать отдельные компоненты запроса в соответствии с принятой/базовой политикой доступа. Сущестующие стандартные языки описания политики доступа такие как XACML [8] и AAA [10] предоставляют механизмы для ссылки на внешние политики или условия. Коплексная.комбинированная политика может быть создана модулем PAP на запрос от PDP, или обработана самим PDP в процессе обработки запроса от PEP. PEP также может выполнять трансляцию форматов данных, семантики или пространства имен для приведения их к абстрактному формату используемой политики и воспринимаемому конкретным PDP.

Для повышения быстродействия, СКДП может использовать квитанции (или билеты) для повторного доступа к ресурсу (AuthzTicket), которые могут быть выданы PDP на основе начального/первичного запроса или получены пользователем от PDP предварительно. С целью дальнейшего ускорения процедуры и повышения надежности, PEP может помещать AuthzTicket в собственную кэш-память. Формат AuthzTicket может определяться приложением, однако для открытых систем может использоваться стандартный XML формат для описания контекста и мандатов безопасности SAML (Security Assertion Mark-up Language) [11].

Современные технологии аутентификации и авторизации на основе политики и управления привилегиями основаны на использовании XML- технологий безопасности и позволяют обеспечивать основные сервисы безопасности как для пользователей, так и для конечных приложений,

Подробный анализ использования XML-технологий безопасности и примеры использования стандартов XACML и SAML в СКДП может быть найден в работах автора [5, 6], где также содержится анализ доверительных отношений (trust relations) в распределенных СКДП для типовой архитектуры СОУ.

3 Определение зон безопасности ресурса

Важным моментом для правильного использования, конфигурирования или последующего анализа работы СКДП систем, основаных на Веб-сервисах и Грид является создание адекватной и конструктивной модели безопасности ресурса, которая бы отражала современную архитектуру построения приложений на основе Веб-сервисов и Грид. В таких системах инфраструктура сервисов (middleware) обеспечивает среду для безопасной передачи запроса на услугу и ее безопасную доставку

запросчику или пользователю. В работе автора [12] сделана попытка предложить обобщенную модель использования СКДП на основе АА-сервисов для защиты ресурсов в СОУ архитектуре.

Рисунок 1 представляет структурированное представление СКДП Ресурса и выделяет несколько зон безопасности ресурса, которые определяются последовательно применяемыми сервисами безопасности:

Zone R0 – зона, контролируемая самим Ресурсом, которая может также включать локальное хранилище данных и локалную файловую систему; это также корневая зона доверия Ресурса.

Zone R1 – зона, которая включает агент или интерфейс ресурса и другие подсистемы, которые относятся к системной зоне доверия Ресурса и могут работать с административными привилегтями ресурса. Эта зона может включать политику доступа и PAP. Агент ресурса может также включать свою локальную систему контроля доступа, использующую локальный ACL или другой вид политики, которые однако не представленные во внешней политике доступа.

Zone RA и **Zone RAA** – зоны, защищенные соответственно функциями аутентификации и авторизации запроса и.или запросчика. Следует заметить, что аутентификация пользователя или запросчика может осуществляться как отдельная процедура перед авторизацией или как начальный этап удостоверения субьекта запроса на этапе авторизации. При этом в первом случае служба аутентификации должна выдать удостоверяющую квитанцию, которая может быть в последующем проверена и использована службой авторизации. В распределенной системе АА/СКДП служба авторизации также может выдавать квитанции в форме AuthzTicket, удостоверяющие положительное решение о доступе, однако такая квитанция должна сохранять контекст безопасности положительного процесса как AuthN так и AuthZ. Стандартным форматом для таких квитанций, как уже упоминалось, является SAML [11].

Zone RN – зона, которая включает средства доступа к сети и является фактически открытой внешнему миру. Эта зона может включать также сетевой экран (Firewall), который имеет свою политику фильтрации сетевого трафика и предназначен для защиты ресурса от внешних аттак, в основном направленных на сетевые компоненты системы.

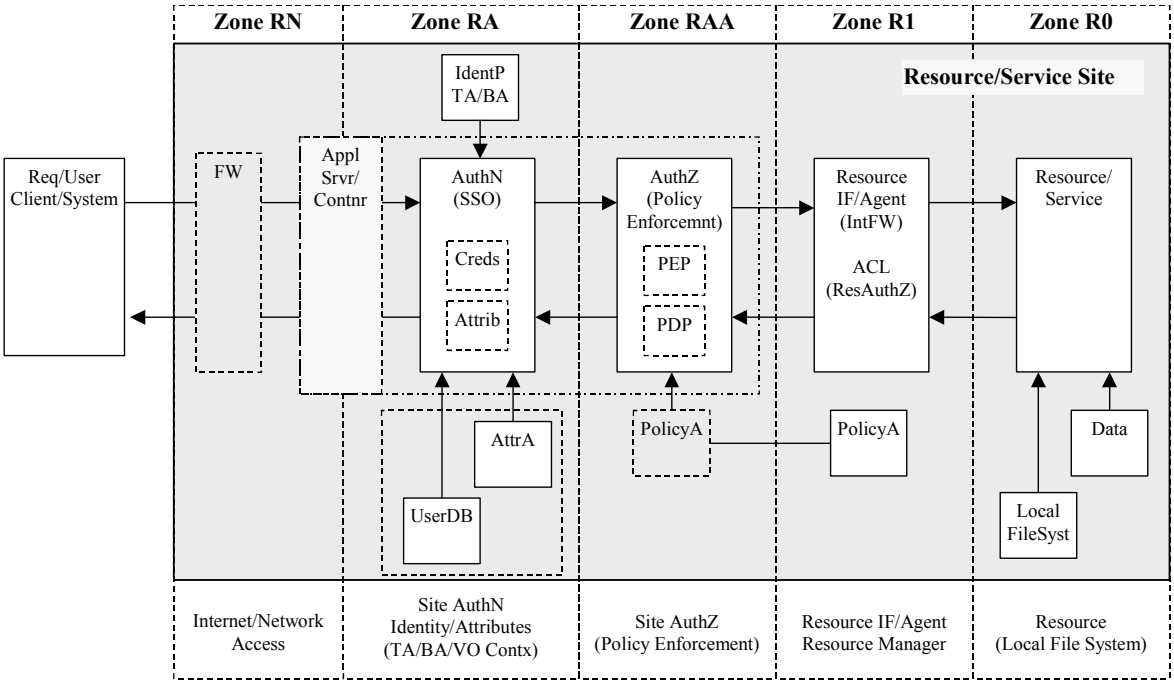

Рисунок 1. Зоны безопасности ресурса.

В зависимости от конкретной реализации, сервисы AuthN и AuthZ могут быть релизованы как отдельные или как составляющая часть сервера приложений или программного контейнера, релизующего Веб- или Грид-сервис, как например, Tomcat [13] для Java-приложений.

Предлагаемая модель зон безопасности может быть использована для анализа безопасности и

доверительных отношений как в системах, основанных на одном хосте, так и для распределенных систем.

4 Заключение

Приведенный в статье анализ технологий и методов построения гибкой системы контроля доступа на основе политики предоставляет полезную начальную информацию для разработчиков систем безопасности Веб-сервисов и Грид-систем. Предполагается, что для дальнейшего понимания и освоения обсуждаемых технологий разработчики обратятся к использованным источниками и другим работам.

Описанные модели и решения нашли свое внедрение в двух основных проектах с участием автора Collaboratory.nl и EGEE (Enabling Grid for E-sciencE). Информация о программном продукте **aaauthreach.org,** реализующем базовые функции СКДП и предоставляющим пример использования стандартных языков XACML и SAML, может быть найдена в [14].

Литература

[1] 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/

[2] Demchenko, Y., L. Gommans, C. de Laat, B.Oudenaarde, A. Tokmakoff, M. Snijders, R. Buuren, “Security Architecture for Open Collaborative Environment,” - European Grid Conference, EGC 2005, Amsterdam, The Netherlands, February 14-16, 2005, Proceedings. Series: Lecture Notes in Computer Science, Volume 3470, 2005.

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

[4] 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

[5] Job-centric Security model for Open Collaborative Environment, by Yuri Demchenko, Leon Gommans, Cees de Laat, Bas Oudenaarde, Andrew Tokmakoff, Martin Snijders. - Accepted paper for the CTS2005 Symposium, Special Session on Security and Collaboration. - May 15-19, 2005.

[6] 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

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

[8] eXtensible Access Control Markup Language (XACML) Version 1.0 - OASIS Standard, 18 February 2003 - http://www.oasis-open.org/committees/documents.php?wg_abbrev=xacml

[9] RFC 3986 - Uniform Resource Identifier (URI): Generic Syntax. - http://www.ietf.org/rfc/rfc3986.txt

[10] A grammar for Policies in a Generic AAA Environment - http://www.ietf.org/internet-drafts/draft-irtf-aaaarch-generic-policy-03.txt

[11] Security Assertion Markup Language (SAML) v1.0 - OASIS Standard, 5 November 2002 - http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

[12] Web Services and Grid Vulnerabilities and Threats Analysis, by Demchenko Y. - Draft version 0.1. http://www.uazone.org/demch/analytic/draft-xws-grid-analysis-01.pdf

[13] Tomcat Security overview and analysis - http://www.cafesoft.com/products/cams/tomcat-security.html

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