ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ WEBSOLVE ПРИ РЕАЛИЗАЦИИ ПРОГРАММНОГО КОМПЛЕКСА RESTFUL-ВЕБ-СЕРВИСОВ

Афанасьев А.П., Волошинов В.В., Лисов А.А., Горбунов М.С.

ФГБОУ ВПО "МАТИ-Российский государственный технологический университет имени К.Э.Циолковского".

Механизм безопасности WebSolve соответствует современному подходу к обеспечению безопасности в Веб/грид-системах и основан на использовании инфраструктуры шифрования с открытым ключом, сертификатов стандарта X.509 и протокола TLS/SSL.

Субъектами безопасности в рамках WebSolve являются пользователи и серверы, на которых функционируют сервисы, а объектами безопасности - сервисы. Каждый пользователь и сервер имеет цифровой сертификат формата X.509, подписанный некоторым центром сертификации. Клиентское приложение, вызывающее сервисы от имени пользователя, использует сертификат данного пользователя.

Взаимная аутентификация взаимодействующих субъектов осуществляется с помощью протокола TLS/SSL и расширения HTTPS. При установлении SSL-соединения клиент и сервер обмениваются своими сертификатами и производят проверку чужих сертификатов (т.н. handshake). На данном этапе используется асимметричное шифрование с использованием пар ключей взаимодействующих сторон, что позволяет каждой из сторон убедиться в том, что другая сторона действительно обладает указанным в сертификате открытым ключом. Затем производится проверка того, что сертификат другой стороны подписан (возможно, не прямо, а через цепочку сертификатов) удостоверяющим центром, которому доверяет данная сторона. Взаимодействующие стороны могут также производить дополнительную проверку чужих сертификатов. В случае если описанные выше проверки не были пройдены успешно, сторона разрывает SSL-соединение.

После успешной взаимной аутентификации стороны переходят на использование симметричного шифрования с согласованным ключом. Подобная схема позволяет уменьшить накладные расходы, обеспечивая при этом конфиденциальности и целостность передаваемых по сети данных.

В целях упрощения доступа пользователей к сервисам также предусмотрен способ аутентификации при помощи публичных провайдеров учетных записей и протокола OpenID. Данный способ доступен только при доступе к сервису через веб-браузер. По умолчанию используются следующие провайдеры: Google, Яндекс, Mail.ru, ВКонтакте, Facebook, Twitter и любой OpenID-провайдер.

Процесс авторизации означает проверку права субъекта (клиента) на выполнение запрашиваемого действия с объектом безопасности (сервисом). При этом предполагается, что клиент уже прошел процедуру аутентификации, то есть может быть однозначно идентифицирован. В контексте WebSolve список возможных действий клиента по отношению к сервису определяется унифицированным REST-интерфейсом сервиса. Базовая политика доступа к сервису WebSolve предполагает, что получение описания сервиса является публично доступным действием, так как не является ресурсоемким и может использоваться для обнаружения сервиса клиентами или регистрации сервиса в каталоге.

Отправка запроса к сервису приводит к запуску ресурсоемкого вычислительного задания, поэтому данная операция доступна только для ограниченного круга клиентов, определяемых поставщиком сервиса. При этом требуется ограничить доступ клиентов к запросам других клиентов, например, из соображений конфиденциальности. Для этого все действия с ресурсом-запросом доступны только клиенту, отправившему данный запрос.

В защищенном режиме доступ к сервисам предоставляется с помощью протокола HTTPS, что означает необходимость снабжения веб-сервера контейнера SSL-сертификатом, для получения которого использована методика самоподписанного (self-signed) сертификата сервера.

Настройка авторизации выполняется отдельно для каждого из сервисов, размещенных в контейнере, и заключается в определении двух списков клиентов:

1. Клиенты, которым разрешена отправка запросов к сервису (т.н. allow-список, размещается в файле EVEREST_HOME/services/SERVICE_ID/allow);
2. Клиенты, которым запрещена отправка запросов к сервису (т.н. deny-список, размещается в файле EVEREST_HOME/services/SERVICE_ID/deny).

Каждый из списков оформляется в виде файла, содержащего уникальные идентификаторы клиентов.

Таким образом, технологии WebSolve гарантируют безопасный обмен данными по протоколу HTTPS и организацию контролируемого авторизованного доступа к сервисам, что является необходимым условием при функционировании распределенной среды.

Работа выполняется в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007-2013 годы» при финансовой поддержке Минобрнауки, государственный контракт 07.514.11.4024.