ПРОБЛЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДЛЯ RESTFUL-ВЕБ-СЕРВИСОВ

Аутентификация клиентов RESTful-грид-сервисов может производиться как при помощи стандартных для HTTP механизмов (Basic, Digest), так и при помощи средств, стандартных для традиционных грид-сервисов, таких как сертификаты X.509 или прокси-сертификаты. В последних случаях возможно использование специфических атрибутных сертификатов, таких как расширения VOMS.

Протокол HTTP (HyperText Transfer Protocol) имеет стандартный механизм аутентификации пользователей, использующий заголовки Authorization и WWW-Authenticate [1]. Начальная аутентификация через этот механизм производится стандартной последовательностью запрос–вопрос–ответ (request–challenge–response). Клиент посылает запрос, требующий аутентификации, сервису и получает ответ 401 Unauthenticated с заголовком WWW-Authenticate, содержащим по крайней мере один вопрос (возможно, содержащий дополнительные параметры), ответ на который клиент должен сообщить серверу в заголовке WWW-Authenticate, повторив запрос. При последующих запросах клиент может заблаговременно передавать заголовок Authorization в запросах, используя для вычисления ответов информацию исходного вопроса.

Для работы с этими заголовками определяются две стандартные схемы аутентификации, Basic и Digest, подробно описанные в [2]. Эти схемы используют в качестве параметров доступа имя пользователя и пароль. Поскольку в схеме аутентификации Basic данные передаются в форме, позволяющей перехватить имя пользователя и пароль, использовать эту схему рекомендуется только поверх защищенных соединений, например с использованием HTTP через TLS (Transport Layer Security), т.е. с использованием протокола HTTPS (Hypertext Transfer Protocol Secure).

Схема аутентификации с использованием заголовков Authorization / WWW-Authenticate предусматривает возможность использования любых расширенных механизмов аутентификации. Например, помимо стандартных схем, определенных в [2], опубликована также схема аутентификации [3], переносящая параметры сообщений WSSE [3] внутрь авторизационного заголовка.

Большинство уже существующих грид-сервисов, как построенных на протоколах WSRF/OGSA, так и использующих GSI из Globus Toolkit, применяют клиентские сертификаты X.509 и прокси-сертификаты [2] для аутентификации пользователей, поэтому аутентификация пользователей RESTful-грид-сервисов при помощи клиентских сертификатов или прокси-сертификатов является оправданной. Более того, такой способ аутентификации открывает возможность использования информации из атрибутных сертификатов [1] для принятия решений об авторизации. В частности, атрибутные сертификаты VOMS [2-3] получили достаточно широкое распространение в проектах EGEE/WLCG.

Сложность такого подхода заключается в том, что наиболее распространенные реализации HTTPS-серверов, включая Apache mod_ssl, не поддерживают аутентификацию с использованием прокси-сертификатов. Однако для сервера Apache существует дополнительный модуль расширения mod_gridsite [**Ошибка! Источник ссылки не найден.**], включающий в себя не только поддержку прокси-сертификатов для аутентификации клиентов, но и предоставляющий приложениям информацию из атрибутных сертификатов с VOMS-расширениями. К недостаткам mod_gridsite можно отнести зависимости от библиотек Globus Toolkit.

1 Fielding R., Gettys J., Mogul J., Frystyk H., Masinter L., Leach P., Berners-Lee T. Hypertext Transfer Protocol - HTTP/1.1. Tech. rep. IETF Network Working Group. 1999. June. RFC2616 (http://tools.ietf.org/html/rfc2616).

2 Franks J., Hallam-Baker P., Hostetler J., Lawrence S., Leach P., Luotonen A., Stewart L. HTTP authentication: basic and digest access authentication. Tech. rep. IETF Network Working Group. 1999. June. RFC2617 (http://tools.ietf.org/html/rfc2617).

3 Pilgrim M. Atom authentication. Available online (http://www.xml.com/pub/a/2003/12/17/dive.html).