В. В. Климов, В. П. Климов

УГРОЗЫ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ ПОИСКА И КОМПОЗИЦИИ ВЕБ-СЕРВИСОВ

В последнее время становится популярной покомпонентная сборка приложений на базе сервис-ориентированной архитектуры (SOA, Service-Oriented Architecture). Концепция SOA основана на том, что бизнес-приложение состоит из большого количества компонентов. Каждый такой компонент представляет собой сервис, являющийся модулем системы SOA. Использование данного подхода к программированию ИТ-инфраструктуры позволяет крупному предприятию получить преимущества при дальнейшем развитии.

На текущем этапе построения SOA-систем на предприятиях создаются собственные UDDI *(Universal Description Discovery & Integration)* реестры сервисов данного предприятия. Также имеется глобальный UDDI-реестр всех сервисов, доступных платно или бесплатно через Интернет. Таким образом, при создании систем с SOA возникает задача эффективного отбора сервисов, исполняющих те или иные функции приложения и соответствующих запросу пользователя. Ввиду того что как локальный UDDI, так и глобальный UDDI могут содержать большое количество сервисов, эта задача является нетривиальной. Она может решаться на синтаксическом и семантическом уровнях. Так как в общем случае веб-сервис исполняется в среде, в которой нельзя гарантировать контроль безопасности из-за отсутствия физического доступа к серверам, для приложений с повышенным уровнем безопасности требуется отбирать сервисы не только по функциональным характеристикам, но и по характеристикам информационной безопасности. Следовательно, у всех веб-сервисов должны присутствовать сертификаты безопасности с 2 уровнями, на которых необходимо производить контроль: 1) контроль над соединением и передачей данных между сервисами; 2) контроль над средой выполнения веб-сервисов.

Для эффективного контроля безопасности SOA-приложений должен быть установлен уровень требований к информационной безопасности (ИБ) веб-сервисов. ИБ — это состояние ИТ, определяющее защищенность информации и ресурсов ИТ от действия объективных и субъективных, внешних и внутренних угроз, а также способность ИТ выполнять предписанные действия без нанесения ущерба субъектам информационных отношений (см. [1]). SOA-приложения сильно волнуют Интернет и бизнес-сообщества, поэтому консорциум W3C (*World Wide Web Consortium*, Консорциум Всемирной паутины) и OASIS (*Organization for the Advancement of Structured Information Standards*) предпринимают значительные усилия, чтобы SOA-приложения имели гарантированный уровень безопасности. Уровень требований устанавливается с помощью сертификатов (стандартов) безопасности. W3C и OASIS рекомендуют стандарты X.509, SPKI, XKMS, SSL/TLS, а также протоколы P3P и SAML в целях повышения информационной безопасности SOA-приложений.

SAML (*Security Assertion Markup Language* — язык разметки подтверждения безопасности) — основанный на языке XML стандарт, разработанный OASIS для обмена данными об аутентификации и авторизации между защищенными доменами, в рамках которых исполняются веб-сервисы. Стандарт SAML не зависит от платформы и состоит из утверждений, протоколов, привязок и профилей. Утверждения — это описания (высказывания) службы идентификации (*identity authority*) о конечном пользователе. Существуют три вида утверждений: авторизации, аутентификации и атрибута. Каждое в отдельности представляет собой набор общих элементов: предмет, условие и аутентификационное высказывание — и содержит информацию о типе сделанного запроса. Если запрашивается авторизация доступа к приложению, то утверждение

SAML сообщает, разрешен ли пользователю вход в систему, и показывает набор его прав доступа. Если запрашивается аутентификация для сетевого ресурса или приложения, утверждение SAML указывает метод аутентификации, а также ее дату и время. В свою очередь, утверждения атрибута позволяют авторизовать пользователей для доступа к определенной информации на основании их статуса. В стандарте SAML хорошо то, что сервер управления идентификацией инкапсулирует, т. е. скрывает, реальные процессы авторизации и аутентификации, что позволяет сочетать решения безопасности от разных производителей. Одна из важных проблем, которую пытается решить SAML, — обеспечение сквозной аутентификации (технология единого входа, *Single Sign On*) при работе через браузер. Эта технология предполагает использование специального программного решения, которое будет хранить пароли пользователя от всех приложений, требующих аутентификации, и автоматически вводить их, когда приложение того требует. Т. е. подобное решение замещает собой пользователя в процессе аутентификации приложением. Доступ пользователя к хранимым паролям и настройкам происходит после аутентификации пользователя в подобную систему, совмещенную с аутентификацией в операционную систему. Таким образом, пользователь автоматически получает доступ ко всем системам, требующим аутентификации, введя однажды персональные данные аутентификации.

Платформа для предпочтений конфиденциальности (*Platform for Privacy Preferences*, или *P3P*) — это протокол, позволяющий веб-сервисам автоматически информировать браузер об их политике конфиденциальности в стандартном формате, о предполагаемом получении личных данных пользователя. Вследствие этого клиентам не нужно считаться с политикой конфиденциальности на каждом посещаемом ими сайте. Также он идентифицирует получателей данных. Протокол был разработан (W3C), чтобы предоставить клиентам больший контроль над персональной информацией во время просмотра сервисов.

Данные рекомендации относятся к концепциям веб-сервисов и Семантической паутины (*Semantic Web*). С ними организация W3C связывает успешное развитие Мировой сети. Теперь мы вплотную приблизились к OWL-S-описанию сервиса, которое ставит перед собой четыре основные задачи (см. [2]): автоматический поиск веб-сервисов, автоматическое заполнение данных, необходимых для работы веб-сервиса, автоматическая организация взаимодействия веб-сервисов, автоматический мониторинг веб-сервисов. Делаем однозначный вывод: онтологии OWL-S — это удобный способ описания семантики работы веб-сервисов. Рассмотрим три подгруппы онтологий OWL-S: профиль, модель процесса и основание (grounding). С их помощью язык OWL-S предоставляет описания политик и требований безопасности (см. [3]), предполагающих автоматическую организацию взаимодействия веб-сервисов.

Требования безопасности могут быть использованы в профиле для открытия веб-сервиса, а в модели процесса и основании (grounding) необходимы для вызова и обмена сообщениями между веб-сервисами и их запросом. Данный язык поддерживает представления политик, таких как расширения требований безопасности сервисов. Добавляется свойство policyEnforced, которое определяется как подсвойство securityCapability (см. [4]). Свойство policyEnforced описывает различные политики, которые должны быть корректно исполнены для сервиса. Оно также является подсвойством securityRequirement. В свою очередь, это подсвойство связано с областью определения агента и может быть использовано для установления рекомендаций безопасности к сервисному запросу. OWL-S-онтология была связана с Rei (см. [5]). Rei — это язык, основанный на RDF-Shema, позволяющий определять правила и ограничения по проблемно-ориентированным онтологиям. Они моделируют подсознательные понятия человека: запреты, обязательства и возможности. Данные понятия имеют четыре признака: инициатор действия, действие, условие и ограничение. Ограничение определяет условия над инициатором, действием

и другие виды организации связи, которые должны быть истинными при вызове процедуры. Условия, представляющие обязательства инициатора, описывают требования, выполняющиеся после вызова процедуры. Эти основные конструкции применяются в Rei для представления различных видов политик, в том числе авторизации и конфиденциальности. В основе онтологии Rei лежит класс Policy. Он имеет следующие подклассы PrivacyPolicy, AuthorizationPolicy и ConfidentialityPolicy. Класс Policy связан с OWL-S-онтологией, определяющей новое OWL-S-описание свойств policyEnforced. Связь OWL-S с Rei применяется в спецификации подлинности и конфиденциальности сервисов.

Что же касается предоставления описания безопасности и требований в OWL-S, то они поддерживаются профилем OWL-S с помощью двух параметров сервиса, первый — securityCapability — определяет, какие требования безопасности могут быть обработаны веб-сервисом, а другой — securityRequirement — определяет, какие требования безопасности веб-сервиса ожидают и обязаны поддерживать его клиенты. Эти два параметра могут использоваться в процессе открытия веб-сервиса в комбинации с функциональными способностями веб-сервиса. Поэтому можно искать сервис, продающий книги и использующий сертификат X.509 (первоначально он связывал открытый ключ с назначенным именем). Это требование безопасности используется для шифрования специального заголовка WS-Security. Оно выражено через данные соответствующей онтологии, с использованием параметра securityRequirements. Тот же подход используется для представления политик, с той разницей, что использовался Rei, а не протокол РЗР. Где WS-Security, WS-Trust и WS-SecureConversation — это спецификации, определяющие дополнения к SOAP для защиты на уровне сообщения, аутентификации и идентификации данных. Безопасность на уровне сообщения не ограничена одним типом учетных данных и дает разработчикам возможность более тонкой настройки.

Доверие к безопасности ИТ обеспечивается двумя способами: реализацией в них необходимых функциональных возможностей и осуществлением комплекса мер по обеспечению безопасности при разработке продуктов и систем ИТ. Из этого следует, что у ИБ есть три основные задачи: обеспечить целостность данных, их конфиденциальность и доступность.

Была разработана собственная система, один из модулей которой позволяет получить безопасное соединение между сервисами. С целью повышения уровня безопасности вводится уникальный показатель информационной безопасности веб-сервиса — Security of Information (SoI), позволяющий проводить более эффективный анализ на пригодность обработанного поисковым роботом веб-сервиса перед добавлением его в базу данных по сравнению с другими системами, в которых не предусмотрены дополнительные проверки на этом этапе. Рассчитывается SoI так:

$$SoI = D \bigcap E \bigcap F \quad (1),$$

где D — соединения, угрожающие безопасности системы;

E — соединения, не удовлетворяющие нормативам по величине времени задержки сигнала ответа;

F — соединения, не удовлетворяющие нормативам по качеству передачи данных.

Каждый из параметров (D,E,F) принимает значение либо 0 в случае ошибки, либо 1 в случае успеха. Если $SoI = 1$, данный сервис принимается поисковым роботом. Если $SoI = 0$, он отсеивается поисковым роботом.

Одной из наиболее сложных и интересных частей данной системы является реализация семантической композиции сервисов. Необходимо было гарантировать семантическое взаимодействие сервисных интерфейсов, в основе которого лежит формальная модель, позволяющая описать сервисы, идентифицировать сходства между ними и, наконец, скомпоновать сложные сервисы. Была предложена формальная модель соответствия сервисов с неполной информацией. Эта модель решает

задачи проверок подобия между сервисными описаниями для классификации и выбора наиболее похожего сервиса, который удовлетворяет запросу (см. [6]). Предложен подход к обнаружению похожих сервисов с неполной информацией, базирующейся на расширениях OWL-S-описаний сервиса клиента на основе использования онтологии предметной области (см. [7]). И был описан подход к обнаружению сервисов, который основан на их новых типах сходства (полного, с избыточной и недостающей информацией) и двух алгоритмах для исчерпывающей и пошаговой генерации сходных сервисных описаний на OWL-S. Основными проблемами данного подхода являются:

1. Избыточные огромные базы сгенерированных расширенных описаний, которые необходимо хранить и обрабатывать (см. [4]).

2. Никак не решается задача возможной противоречивости сгенерированных сервисных описаний. При условии, что в онтологиях предметной области могут по-разному описываться одни и те же понятия, непонятно, какое из противоречивых сгенерированных описаний сервисов выдавать клиенту и какое из них будет наиболее релевантным запросу клиента.

Для решения данной проблемы возможно использование технологии семантического веба для описаний веб-сервисов на основе нотации OWL-S *(Web Ontology Language for Web-Services)*, разработанной консорциумом W3C, и реализации алгоритма поиска по семантическим описаниям. В то время как другие разработки в этом направлении введутся на основе нотации WSDL *(Web Services Description Language)*, где до недавнего времени отсутствовал стандартизированный способ указания *Качества защиты* (*Quality of Protection, QoP*) сервиса в документе WSDL. Предлагаемый стандарт применим только к веб-сервисам, использующим SOAP *(Simple Object Access Protocol)*. Это протокол обмена структурированными сообщениями в распределенной вычислительной среде.

Существует множество сертификатов, протоколов и других технологий, обеспечивающих корректное с позиции ИБ соединение (взаимодействие) веб-сервисов. Анализируя круг возможных угроз, приходим к следующим соображениям:

1. Разработка сервиса так же важна, как и его последующая поддержка. Сохранение целостности и корректной работы в будущем целиком и полностью зависит от профессионализма и мастерства разработчиков.

2. Ключевую роль играет стандартизация требований безопасности. Совсем недавно брандмауэры не справлялись с атаками злоумышленников, которые использовали слабые места в прикладном программном обеспечении, появившиеся в результате открытия портов, на которых исполнялись защищенные сервисы. Другими словами, сами веб-сервисы ослабляли безопасность, предоставляя посторонним лицам доступ к приложениям — именно то, чему сетевой брандмауэр должен был бы воспрепятствовать.

3. Корректными сервисами при отборе поисковым роботом считаем те, которые соответствуют требованиям ИБ, предъявляемым организациями по стандартизации Мировой сети (на данный момент времени). При этом считаем возможным учитывать собственный показатель ИБ веб-сервиса Security of Information (*SoI*) с целью повышения надежности во время соединения с сервисом.

На сегодняшний день задача поиска и композиции релевантных запросу пользователя веб-сервисов актуальна и является значимой. Текущие средства работы с веб-сервисами зачастую недооценивают возможные угрозы, имеющиеся при работе в открытом пространстве сети Интернет. При разработке систем поиска и композиции веб-сервисов всегда следует учитывать угрозы ИБ, способные обходить используемые протоколы и сертификаты защиты. Лишь тогда окажется возможным избежать больших убытков, которые могут нанести системе злоумышленники.

СПИСОК ЛИТЕРАТУРЫ:

1. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. URL: http://www.fstec/_docs/ch%201.doc.
2. *Климов В. В., Савинов Н. Л.* Система динамической композиции веб-сервисов на основе их WSDL и OWL-S описаний // Научная сессия МИФИ-2010 «Молодежь и Наука». Сборник научных трудов М.: МИФИ, 2010. Т. 2. С. 62–64.
3. *Kagal L., Finin T., Paolucc, M., Srinivasan N., Sycara K., Denker G.* Authorization and Privacy for Semantic Web Services // IEEE Intelligent Systems. July/August. 2004.
4. URL: www.csl.sri.com/~denker/owl-sec/serviceSecurity.owl.
5. *Lalana Kagal et al.* A Policy Based Approach to Security for the Semantic Web // Proceedings of the 2nd International Semantic Web Conference (ISWC2003). September 2003.
6. *Климов В. В.* Система поиска и интеграции семантических веб-сервисов // Труды III Международной научно-практической конференции «Информационные технологии в образовании, науке и производстве». Серпухов, 29 июня – 3 июля 2009 г. Часть 2. С. 169–172.
7. *Климов В. В., Климов В. П., Миронос С. А.* Построение гибких и совместимых программных продуктов с использованием технологии web-сервисов // Научная сессия МИФИ-2010. «Молодежь и Наука». Сборник научных трудов. М.: МИФИ, 2010. Т. 2. С. 79–80.