Колодий К.Г.
УДК 004.05

Анализ защищенности web-сервисов

Web-интеграция бизнес-процессов компаний-партнеров позволяет на основе Интернет технологий создавать открытые и закрытые торговые площадки, проектировать сложные системы поставок и не менее сложные системы взаиморасчетов, планировать совместное производство и продвижение товара. Таким образом, экономится время, например, значительно сокращается время на телефонные разговоры и передачи факсов, практически исключаются ошибки и пропажа документов, уменьшается время на обслуживание клиента и многое другое. Web-системы, автоматизирующие бизнес процессы компаний-партнеров, получили название B2B-системы (business to business) [1]. Такие системы строятся на основе web-сервисов. Web-сервис — это программная система, идентифицируемая строкой URI (Uniform Resource Indentifier) с общедоступными интерфейсами, которые определены на языке XML. Описание этой программной системы может быть найдено другими программными системами, которые могут взаимодействовать с ней согласно этому описанию посредством сообщений, основанных на XML и передаваемых с помощью сетевых протоколов [2]. Типичная архитектура web-сервиса представлена на рисунке 1.

Работа с web-сервисами осуществляется через компьютерные сети общего пользования. При этом между web-сервисами может передаваться конфиденциальная информация, доступ к которой должен предоставляться только определенным лицам. Поэтому при внедрении web-сервиса разработчикам системы B2B необходимо обеспечить требуемый уровень безопасности.

Рассмотрим проблемы безопасности при реализации web-сервиса на примере внедрения и использования протокола SOAP [2] в Иркутском государственном университете путей сообщения (ИрГУПС).

Процесс обмена динамическими данными между разноформатными системами или web-сервисами представляет собой взаимодействие SOAP-клиента и SOAP-сервера, обменивающихся SOAP-сообщениями. После процесса установления соединения SOAP-клиент запрашивает у удаленного SOAP-сервера блок метаданных на языке WSDL [2], в котором описана структура предоставляемой для экспорта информации. На данном этапе происходит SOAP-обмен управляющими блоками. После получения метаданных клиент формирует специальный запрос на получение определенного пакета данных в едином универсальном формате. SOAP-сервер принимает запрос клиента и вызывает необходимый модуль выгрузки, который выгружает нужные данные из источника данных в единый формат передачи. SOAP-сервер формирует сообщение, проверяет его на целостность и передает по

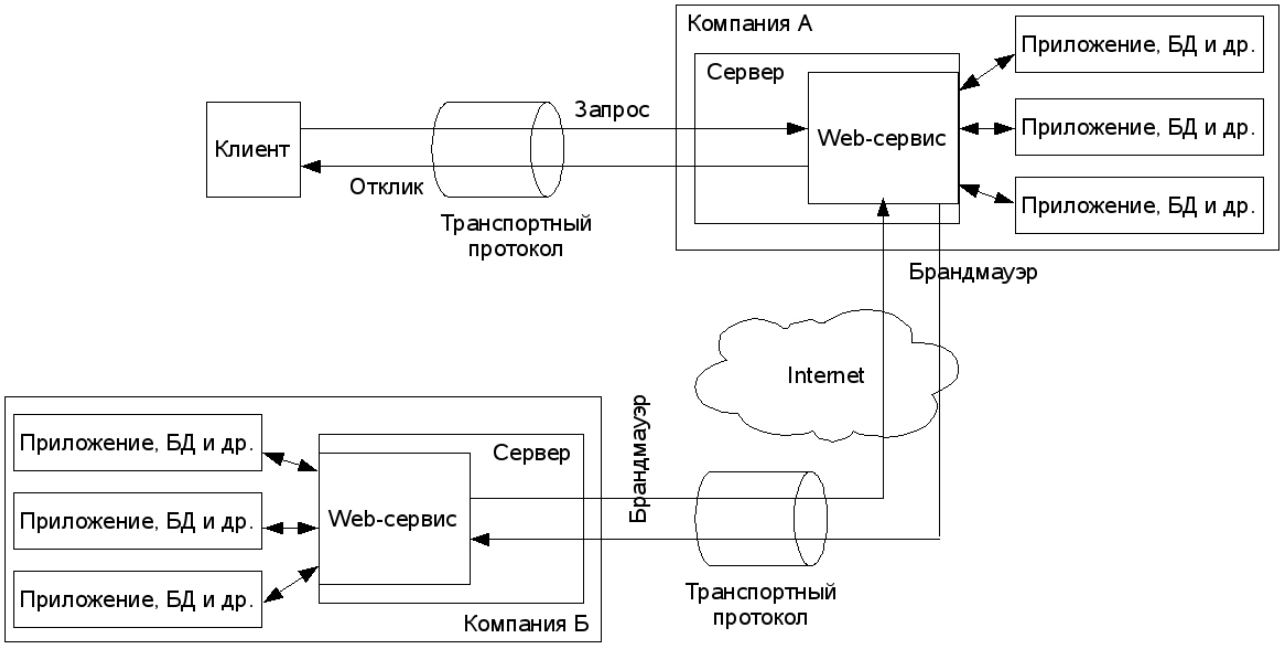

Рисунок 1.Типичная архитектура web-сервиса

линии связи (протокол HTTP) в принимающую систему. На принимающей стороне начинает работу импортирующая программа, конвертируя XML-представление во внутреннее представление источника данных.

В связи с тем, что зачастую SOAP работает через протокол HTTP, доступ к которому не закрыт брандмауэром, web-службы подвержены тем же угрозам безопасности, что и web-приложения. Например: несанкционированный доступ, перехват и искажение информации и др.

Различным подразделениям и отделам университета необходим доступ к информации связанной с учебным процессом. В университете имеется единая база данных и несколько различных специализированных приложений, работающих как с этой единой базой данных, так и имеющих свои базы данных. Доступ к единой базе данных предоставляется посредством web-сервиса, основанного на протоколе SOAP. Внедрение web-сервиса позволило предоставить ограниченный доступ к единой базе данных. Так как внедренный web-сервис предоставляет доступ к конфиденциальной информации, то доступ к скриптам web-сервиса был ограничен с помощью базовой аутентификации. При базовой аутентификации пара логин/пароль кодируется и передается в Base64. Если злоумышленник сумеет перехватить пакеты, то сможет раскодировать логин и пароль. Так как доступ к web-сервису возможен только с компьютеров локальной сети университета, а архитектура локальной сети построена таким образом, что перехват пакетов данных существенно затруднен, то было решено, что базовой аутентификации будет достаточно.

Предположим, злоумышленник, имеющий доступ к одному из компьютеров локальной сети, получил в распоряжение информацию: URI web-сервисов и пары логин/пароль для доступа к этим web-сервисам. Часть web-сервисов в университете реализована с использованием модуля php_soap [3], который не поддерживает генерацию WSDL, поэтому злоумышленнику не удастся получить информацию о методах, предоставляемых SOAP-серверами. Часть web-сервисов реализована с использованием класса Nusoap, в котором имеется возможность генерации WSDL. Использование данного класса требуется для подключения к web-сервису программными системами, написанными на языках, которым необходим WSDL для доступа к методам SOAP-сервера. Поэтому, злоумышленник, имея в распоряжении URI и логин/пароль, сможет получить информацию о логике предметной области данных web-сервисов. Как следствие, злоумышленник сможет вызывать процедуры, находящиеся на SOAP-серверах, передавая, как корректные входные данные для извлечения информации из единой базы данных, так и передавая функциям заведомо некорректные данные с целью получения дополнительных данных и/или полного доступа к единой базе данных. Нарушить защиту можно используя различные виды атак, например, SQL Injection [4].

Разработкой методов для SOAP-сервера занимается несколько программистов (уже имеется около 250 функций), поэтому проведение полного тестирования и инспектирования исходного кода этих функций является трудоемкой задачей. Из-за недостаточности тестирования не исключается возможность наличия уязвимостей.

Проведем анализ рисков web-сервисов ИрГУПС. Существуют различные методики оценки рисков информационной безопасности (CRAMM, Method Ware, Risk Watch, ГРИФ 2006 и др.). Эти методики входят в состав коммерческих программных продуктов, поэтому полные описания алгоритмов не опубликованы. Наиболее полно описана методика ГРИФ 2006 [5] компании Digital Security. За основу возьмем модель анализа угроз и уязвимостей методики ГРИФ 2006. Для расчета рисков воспользуемся алгоритмом с одной базовой угрозой. В качестве ресурсов будем рассматривать два ресурса: web-сервис с поддержкой генерации WSDL и web-сервис без поддержки генерации WSDL. Определимся со списком возможных угроз: несанкционированный доступ к web-сервису, несанкционированный доступ к информации, несанкционированная модификация информации, несанкционированная модификация логики работы web-сервиса. В таблице 1 представлены угрозы с возможными уязвимостями.

Сотрудниками Центра информационных технологий (ЦИТ) университета была проведена экспертная оценка вероятности реализации угроз и критичности реализации угроз через существующие уязвимости (таблица 2).

Таблицы 1 и 2 представляют собой входные данные для алгоритма расчета рисков.

Произведем расчет уровней угроз. Посчитаем уровень угрозы *Th* по каждой уязвимости по формуле 1.

$$Th = \frac{ER}{100} \times \frac{P(V)}{100}, \quad (1)$$

где *ER* – критичность реализации угрозы через уязвимость,

P(V) – вероятность реализации угрозы через данную уязвимость в течение года.

Затем посчитаем уровень угрозы по всем уязвимостям *CTh*, через которые реализуется данная угроза по формуле 2.

$$CTh = 1 - \prod_{i=1}^{n}(1 - Th_i), \quad (2)$$

где Th_i – уровень данной угрозы по *i*-ой уязвимости.

Все значения находятся в диапазоне от 0 до 0,667. Чем выше значение, тем выше уровень данной угрозы.

Далее посчитаем общий уровень угроз *CThR*, действующих на ресурс по формуле 3.

$$CThR = 1 - \prod_{i=1}^{n}(1 - CTh_i), \quad (3)$$

где CTh_i – уровень *i*-ой угрозы для данного ресурса.

Общий уровень угроз ресурсам составил для web-сервиса без WSDL 0,89 и для web-сервиса с WSDL 0,854.

Для расчета риска ресурсов необходимо задать критичность ресурса *D*. Так как университет является не коммерческой организацией, то уровень критичности был оценен в уровнях. Количество уровней может быть в диапазоне от 0 до 100, где 100 — максимальное значение критичности ресурса. Экспертами критичность обоих ресурсов была оценена в 100 уровней.

Теперь можно рассчитать риск ресурсов *R* и риск информационной системы в целом *CR* по формулам 4 и 5 соответственно.

$$R = CThR \times D \quad (4)$$

$$CR = (1 - \prod_{i=1}^{n}(1 - \frac{R_i}{100})) \times 100, \quad (5)$$

где R_i – риск *i*-ого ресурса.

В таблице 3 представлены результаты расчета риска ресурсов в уровнях. Чем больше значение риска, тем выше критичность данного ресурса.

Для защиты рассматриваемых ресурсов используются различные средства защиты (контрмеры). Произведем расчет эффективности используемых контрмер (таблица 4) исходя из экспертных оценок степени сопротивляемости.

Для расчета уровня угроз *Th* требуется учитывать степень сопротивляемости контрмеры, являющейся вероятностной характеристикой. Обозначим степень сопротивляемости через *S*. Если *S* равно 0%, то эффект от использования контрмеры отсутствует. Если же *S* равно 100%, то контрмера полностью перекрывает уязвимость. Тогда величина $1 - \frac{S}{100}$ есть остаточная вероятность реализации угрозы через данную уязвимость.

С учетом контрмер уровень угрозы *Th* будем рассчитывать по формуле 6.

$$Th = \frac{P(V)}{100} \times \frac{ER}{100} \times (1 - \frac{S}{100}) \quad (6)$$

Значение рисков рассчитываем аналогично оценке рисков без учета контрмер.

Эффективность контрмер рассчитывается по формуле 7

$$E = \frac{R_{old} - R_{new}}{R_{old}}, \quad (7)$$

где R_{old} – риск без учета контрмер,

R_{new} – риск с учетом контрмер.

Эффективность может принимать значение от 0 до 1, где 1 означает, что все уязвимости полностью закрыты.

Таблица 1

Входные данные: список угроз и уязвимостей

Ресурс	Угрозы	Уязвимости
Web-сервис без WSDL	Угроза 1 *Несанкционированный доступ к web-сервису*	Уязвимость 1 *Отсутствие должной аутентификации*
		Уязвимость 2 *Отсутствие шифрования*
	Угроза 2 *Несанкционированный доступ к информации*	Уязвимость 1 *Отсутствие проверки входных данных*
		Уязвимость 2 *Доступ к метаданным*
	Угроза 3 *Несанкционированная модификация информации*	Уязвимость 1 *Отсутствие проверки входных данных*
		Уязвимость 2 *Доступ к метаданным*
	Угроза 4 *Несанкционированная модификация логики работы web-сервиса*	Уязвимость 1 *Отсутствие проверки входных данных*
		Уязвимость 2 *Распределение прав доступа к файлам*
Web-сервис с WSDL	Угроза 1 *Несанкционированный доступ к web-сервису*	Уязвимость 1 *Отсутствие должной аутентификации*

Продолжение таблицы 1

Входные данные: список угроз и уязвимостей

Ресурс	Угрозы	Уязвимости
		Уязвимость 2 *Отсутствие шифрования*
	Угроза 2 *Несанкционированный доступ к информации*	Уязвимость 1 *Отсутствие проверки входных данных*
		Уязвимость 2 *Доступ к метаданным*
	Угроза 3 *Несанкционированная модификация информации*	Уязвимость 1 *Отсутствие проверки входных данных*
		Уязвимость 2 *Доступ к метаданным*
	Угроза 4 *Несанкционированная модификация логики работы web-сервиса*	Уязвимость 1 *Отсутствие проверки входных данных*
		Уязвимость 2 *Распределение прав доступа к файлам*

Таблица 2

Входные данные: экспертная оценка

Ресурс	Угроза/уязвимость	Вероятность реализации угрозы через данную уязвимость в течение года (%), *P(V)*	Критичность реализации угрозы через уязвимость (%), *ER*
Web-сервис без WSDL	Угроза 1/ уязвимость 1	100	0
	Угроза 1/ уязвимость 2	100	0
	Угроза 2/ уязвимость 1	100	20
	Угроза 2/ уязвимость 2	20	0
	Угроза 3/ уязвимость 1	95	60
	Угроза 3/ уязвимость 2	20	0
	Угроза 4/ уязвимость 1	10	100
	Угроза 4/ уязвимость 2	70	90
Web-сервис с WSDL	Угроза 1/ уязвимость 1	100	0
	Угроза 1/ уязвимость 2	100	0
	Угроза 2/ уязвимость 1	80	20
	Угроза 2/ уязвимость 2	80	0
	Угроза 3/ уязвимость 1	80	60
	Угроза 3/ уязвимость 2	80	0
	Угроза 4/ уязвимость 1	10	100
	Угроза 4/ уязвимость 2	70	90

Таблица 3

Риск ресурса

Ресурс	Общий уровень угроз по ресурсу (%), *CThR*	Риск ресурса, *R*	Риск по информационной системе, *CR*
Web-сервис без WSDL	0,885	88,5	98,32
Web-сервис с WSDL	0,854	85,4	

Таблица 4

Контрмеры

Ресурс	Угроза/уязвимость	Контрмера	Степень сопротивляемости контрмеры (%), *S*
Web-сервис без WSDL	Угроза 1/ уязвимость 1	Базовая аутентификация	90
	Угроза 1/ уязвимость 2	Шифрование SSL	95
	Угроза 2/ уязвимость 1	Проверка входных данных	98
	Угроза 2/ уязвимость 2	Ограничение генерируемых метаданных	80
	Угроза 3/ уязвимость 1	Проверка входных данных	98
	Угроза 3/ уязвимость 2	Ограничение генерируемых метаданных	80
	Угроза 4/ уязвимость 1	Проверка входных данных	98
	Угроза 4/ уязвимость 2	Проверка прав	90
Web-сервис с WSDL	Угроза 1/ уязвимость 1	Базовая аутентификация	90
	Угроза 1/ уязвимость 2	Шифрование SSL	95
	Угроза 2/ уязвимость 1	Проверка входных данных	98
	Угроза 2/ уязвимость 2	Ограничение генерируемых метаданных	0
	Угроза 3/ уязвимость 1	Проверка входных данных	98
	Угроза 3/ уязвимость 2	Ограничение генерируемых метаданных	0
	Угроза 4/ уязвимость 1	Проверка входных данных	98
	Угроза 4/ уязвимость 2	Проверка прав	90

Риск ресурсам с учетом контрмер и эффективность контрмер составили: для web-сервиса без WSDL 7,8 и 0,911 соответственно; для web-сервиса с WSDL 7,5 и 0,912 соответственно.

Для информационной системы в целом получим:

– риск по информационной системе *CR* с учетом контрмер равным 14,7;
– эффективность контрмер по информационной системе $E = 0,85$.

Расчет рисков показал, что исследуемые ресурсы действительно имеют большое значение для функционирования единой информационной системы университета. Поэтому обеспечение безопасности этих ресурсов есть одна из важнейших задач. Значение эффективности контрмер показывает, что используемые средства защиты существенно снижают возможность нарушения безопасности исследованных ресурсов. Это подтверждается на практике, когда введение даже простых средств защиты существенно снижает вероятность угрозы.

БИБЛИОГРАФИЯ

1. Минетт Стив B2B-маркетинг: разные подходы к разным типам клиентов. Полное руководство. — М.: «Вильямс», 2004. — 208 с.

2. Хабибулин И.Ш. Разработка Web-служб средствами Java. — Спб.: БХВ-Петербург, 2003. — 400 с.: ил.

3. Джон Коггэолл PHP 5. Полное руководство. — М.: «Вильямс», 2006. — 752с.

4. Threat Classification. Официальный сайт Web Application Security Consortium [Электронный ресурс] — http://www.webappsec.org/projects/threat/

5. Н. Куканова. Методика оценки риска ГРИФ 2006 из состава Digital Security Office. Официальный сайт ООО "Диджитал Секьюрити" [Электронный ресурс] — http://www.dsec.ru/about/articles/grif_ar_methods/