правовой защиты человека. Следует распространять информацию о механизмах и процедурах защиты прав и свобод человека и гражданина. В основном это вопрос судебной защиты, гарантий публичного доступа к суду, знания правил процедуры и возможности использования услуг адвокатов.

Новые технологии помогают развивать прямые и обратные отношения между государством и гражданским обществом, расширяют участие различных групп и групп населения в управлении страной, ее регионами и местными сообществами, а также собирают информацию на более высоком уровне. для всей ситуации и для отдельных областей развития. переехал в Россию. На этой основе улучшается принятие решений и контроль за их выполнением.

1. Кудинов Ю. И. Основы современной информатики: учебное пособие / Ю. И. Кудинов, Ф. Ф. Пашенко. - СПб.: Лань, 2018. – 256 с.
2. Кураков Л. П. Информация как объект правовой защиты: учебное пособие / Л. П. Кураков. – М.: Гелиос, 2016 г. – 240 с.
3. Стариченко Б. Е. Теоретические основы информатики: учебник для вузов / Б. Е. Стариченко. - М.: Горячая линия – Телеком, 2016. – 400 с.
4. Федотов М. А. Информационное право : учебное пособие / М. А. Федотов. – М.: Издательство Юрайт, 2019. – 497 с.
5. Чепурнова Н. М. Правовые основы информатики: учебное пособие / Н. М. Чепурнова, Ефимова Л. Л. – М.: Юнити – Дана, 2016. – 296 с.

Узденова Б.Х., Чекунова А.М., Акбаева А.А.

Моделирование угроз для веб-приложений на основе веб-служб

*Северо-Кавказская государственная академия
(Россия, Черкесск)*

doi: 10.18411/lj-01-2021-12

idsp: ljjournal-01-2021-12

Аннотация

Анализ угроз веб-приложения может привести к широкому спектру выявленных угроз. Некоторые из этих угроз будут очень специфичны для приложения; другие будут больше связаны с базовым инфраструктурным программным обеспечением, таким как веб-серверы или серверы приложений, база данных, сервер каталогов и так далее. В данной статье анализируются угрозы, которые могут быть связаны с использованием технологии веб-служб в веб-приложении. Он является частью серии статей, написанных различными академическими группами, каждая из которых посвящена одному конкретному технологическому «строительному блоку» для веб-приложений.

Ключевые слова: анализ угроз, веб-сервисы, веб-приложения.

Abstract

Web application threat Analysis can lead to a wide range of identified threats. Some of these threats will be very application-specific; others will be more related to the underlying infrastructure software, such as web or application servers, a database, a directory server, and so on. This article analyzes the threats that can be associated with the use of web services technology in a web application. It is part of a series of articles written by various academic groups, each focusing on one specific technological "building block" for web applications.

Keywords: threat analysis, web services, web applications.

Анализ и моделирование потенциальных угроз, с которыми сталкивается приложение, является важным шагом в процессе разработки безопасного приложения. Некоторые из этих угроз по своей природе очень специфичны для приложения, и

можно дать только довольно общие рекомендации о том, как идентифицировать такие угрозы. Но другие угрозы прямо или косвенно связаны с базовыми платформами, технологиями или языками программирования.

Следовательно, имеет смысл выявить и задокументировать эти технологические угрозы, а также дать рекомендации поставщикам программного обеспечения о том, как снизить связанные с ними риски. В работе представлены результаты такого анализа использования технологии веб-служб в веб-приложениях.

Веб-служба - это, по сути, интерфейс обмена XML-сообщениями для некоторых вычислительных ресурсов. стек протоколов веб-служб состоит из:

- Некоторые протоколы транспортного уровня, обычно HTTP.
- Протокол уровня обмена сообщениями на основе XML, обычно SOAP.
- Протокол уровня описания сервиса, обычно WSDL.
- Протокол уровня обнаружения сервисов, обычно UDDI.

В этой работе предполагаемой моделью связи веб-служб является SOAP через HTTP. Основные взаимодействия SOAP являются асинхронными и однонаправленными, но могут быть объединены для реализации процессов запроса/ответа или даже более сложных взаимодействий.

Сообщения SOAP - это сообщения на основе XML для обмена структурированной и типизированной информацией. SOAP может использоваться для реализации RPC, но фокус смещается на документооборот на основе информации в последней разработке веб-службы.

Рядом с исходным и принимающим узлами веб-службы можно определить промежуточные узлы, как показано на (рис. 1). Эти промежуточные узлы могут обрабатывать SOAP-сообщение и добавлять в него дополнительную информацию.

Рисунок 1 - Поток процесса SOAP-сообщения

Эта работа также делает предположение, что WSDL используется для определения открытого интерфейса к веб-службе. Описание веб-службы на основе WSDL может включать сведения о доступных функциях, вводе информации и адресной информации. WSDL обычно генерируется инструментами, а не вручную.

Использование динамического обнаружения веб-служб в веб-приложениях еще не получило широкого распространения. Следовательно, данная работа не рассматривает уровень обнаружения сервиса.

Общая архитектура веб-приложений представлена. В рамках этой архитектуры для веб-приложений технология веб-служб может использоваться для различных целей. Некоторые примеры включают:

1. Упаковка устаревших приложений: включение функциональности устаревших приложений в веб-приложение часто выполняется путем предоставления устаревшему приложению фасада веб-службы, который может использоваться сервером приложений.

2. Разделение веб-сервера и сервера приложений: Если веб-сервер взаимодействует с сервером приложений по протоколу SOAP/HTTP вместо RPC, брандмауэру между DMZ (содержащим веб-сервер) и средним уровнем достаточно открыть порт 80.

3. Богатые клиенты: браузер может загружать компоненты клиентских приложений (например, Java-апплеты или сборки, NET) с веб-сервера. Эти компоненты могут взаимодействовать с веб-сервером с помощью веб-служб.

4. Интеграция служб «building block»: повторно используемые службы приложений, такие как проверка подлинности или хранение, могут быть доступны в виде веб-служб и использоваться в различных веб-приложениях.

5. Многоступенчатая обработка: веб-службы поддерживают асинхронную модель обмена сообщениями. Один запрос может пройти через несколько посредников до достижения конечного пункта назначения.

6. Виртуальные организации: веб-сервисы могут использоваться для интеграции бизнеса в бизнес, создания полезных федераций автономных субъектов.

Чтобы сохранить список выявленных угроз в разумном размере, представляем только наиболее актуальные угрозы в этом разделе. Что касается этих угроз, то здесь дается лишь краткий обзор. Для выявления наиболее значимых угроз делаем два предположения. Во-первых, предполагаем, что сетевые компании и серверы защищены в соответствии с передовой практикой. Учитываем, что внутренний злоумышленник может получить доступ к сети компании, но без каких-либо привилегий на любой из серверных систем. Во-вторых, предполагаем, что атаки будут направлены на сервер.

Учитывая возможные экземпляры веб-служб в веб-приложении, наиболее актуальным считается сценарий, в котором клиент маскируется при взаимодействии с веб-сервером. Слабая аутентификация клиента или ее отсутствие может привести к несанкционированному доступу к веб-службе. Если DMZ не может быть доверенным, может быть подмены угрозы между веб-сервером и сервером приложений.

Самый высокий риск для фальсификации, существует на стороне клиента. Злоумышленник может изменить все активы, находящиеся на клиентском компьютере или перемещаемые по каналу HTTP. Это приводит к следующим угрозам, которые считаются наиболее актуальными в этой категории.

Заменяется SOAP-сообщение, что приводит к непреднамеренному дублированию действия сервера или несогласованности на сервере.

Сообщение SOAP подделано или злонамеренно построено, что приводит к целому ряду проблем на стороне сервера, таких как раскрытие информации из-за брошенных исключений или нарушений из-за злонамеренного ввода (например, атаки SQL-инъекции в базу данных).

WSDL-файл, отправляемый клиенту, содержащий важную контактную информацию (например, URL-адреса). Изменение этой информации может ввести клиента в заблуждение.

В расширенном клиентском сценарии злоумышленник может получить ценную информацию, проанализировав расширение браузера, отправленное клиенту. Изменение этого расширения позволяет злоумышленнику обходить проверки ввода или создавать вредоносные вызовы SOAP.

В зависимости от контекста конкретного приложения угроза изменения сведений о состоянии серверов может быть важной, но не более подробно описана в данной работе.

Следующий риск раскрытия информации вновь существует на стороне клиента. Злоумышленник может считать все активы, находящиеся на клиентском компьютере или перемещающиеся по каналу HTTP. Это приводит к следующим угрозам, которые считаются наиболее релевантными в этой категории:

- Сообщения SOAP раскрываются, возможно, утечка конкретной информации приложения, такой как номера кредитных карт.
- Файлы WSDL без необходимости раскрываются, предоставляя злоумышленнику информацию о структуре приложения.

- Реализация веб-службы приводит к утечке информации о внутренних компонентах приложения, например, путем отправки сведений трассировки стека об ошибках.

Рассмотрим краткое описание технологий противодействия:

- «Не отказ»: «не отказ» противодействует угрозе подмены. Это можно сделать только на уровне приложения. Возможные технологии включают подписи XML и аудит на уровне приложений.
- Sandboxing: Sandboxing противодействует угрозам привилегии и могут быть предоставлены операционной системой (разделение процессов) или безопасности до-ступа кода. NET.
- Безопасное кодирование: безопасное кодирование противодействует всем видам угроз.
- Обнаружение вторжений/мошенничества: обнаружение вторжений или мошенничества противодействует всем видам угроз. Как разработчик, процесс обнаружения вторжений или мошенничества можно упростить, предоставив хорошие данные аудита на уровне приложений.
- Контрмеры, связанные с доступностью: эти контрмеры противодействуют атакам, связанным с отказом в обслуживании. Доступные технологии включают фильтрацию и регулирование.

Моделирование угроз и выбор мер противодействия являются важными шагами в инженерном процессе создания безопасного программного обеспечения. Документирование угроз, присущих использованию конкретных технологий, и руководство проектировщиками в выборе мер противодействия этим угрозам может значительно облегчить эти шаги. В работе представлены результаты анализа с точки зрения использования технологий веб-сервисов для веб-приложений. Выявлены наиболее значимые угрозы и даны грубые рекомендации по снижению связанных с ними рисков.

1. Д. Де Кок, К. Вутерс, Д. Шеллекенс, Д. Сингли, и В. Пренил. Моделирование угроз для безопасности в веб-приложениях, восьмая конференция IFIP TC-6 TC-11 по Коммуникационной и Мультимедийной Безопасности (CMS 2004), сентябрь 2004 г., Великобритания, стр. 213–223
2. Р. Гримм и Х. Эйхштадт Моделирование Ошибок ASP. NET — Разработка Безопасных Приложений, восьмая конференция IFIP TC-6 TC-11 по Коммуникационной и Мультимедийной Безопасности (CMS 2004), сентябрь 2004, Великобритания, стр. 175–187
3. В. Д. Чедвик. Моделирование угроз для Active Directory. Восьмая конференция IFIP TC-6 TC-11 по Коммуникационной и Мультимедийной Безопасности (CMS 2004), сентябрь 2004 г., Великобритания, стр. 203–212
4. Примечание W3C, SOAP: Протокол Доступа к Простым Объектам 1.1, май 2000 г., <http://www.w3.org/TR/2000/NOTE-SOAP-20000508/>
5. Примечание W3C, язык описания веб-служб (WSDL) 1.1, 15 марта 2001 года, <http://www.w3.org/TR/2001/NOTE-wsdl-20010315>.

Хапаева Л.Х., Гебенова А.А., Халкечева А.А.
Правовая информатика и основы информационного права

*Северо-Кавказская государственная академия
(Россия, Черкесск)*

doi: 10.18411/lj-01-2021-13

idsp: ljjournal-01-2021-13

Аннотация

На сегодняшний день достижения информатики обширно распространены почти абсолютно во всех областях человеческой деятельности. В каждой сфере научного