



City Research Online

City St George's, University of London

Citation: Netkachova, K. & Pokrova, S. V. (2011). Оценка и обеспечение безопасности систем электронного образования на основе веб-сервисов. Бизнес Информ, 6, pp. 183-186.

This is the published version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: <https://city-ref-test.eprints-hosting.org/id/eprint/4159/>

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to [City Research Online policy](#).

ОЦЕНКА И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ ЭЛЕКТРОННОГО ОБРАЗОВАНИЯ НА ОСНОВЕ ВЕБ-СЕРВИСОВ

НЕТКАЧЁВА Е. И.

аспирантка

ПОКРОВА С. В.

Симферополь

В настоящее время широко применяется сервис-ориентированная архитектура при разработке программных комплексов в различных сферах деятельности человека, в том числе и в образовании. Принципы функционирования систем электронного обучения позволяют интегрировать сервис-ориентированные технологии и реализовывать на базе технологии веб-сервисов различные виды и формы обучения от комплексных систем дистанционного образования до небольших коммерческих тренингов.

Использование сервис-ориентированного подхода при построении e-learning систем подробно описаны в работах [1 – 4] и других исследованиях.

Однако веб-сервисы, на основе которых строятся системы дистанционного обучения, зачастую используют коммерческие предразработанные программные компоненты, которые могут иметь уязвимости. Этот факт, в свою очередь, поднимает вопрос безопасности и отказоустойчивости систем такого типа.

Таким образом, актуальными являются разработки в области оценки и обеспечения надежности и безопасности систем электронного образования, построенных на веб-сервисах.

В данной работе проанализирована архитектура отказоустойчивых систем и предложена реализация веб-сервиса, который производит анализ существующих уязвимостей и программных патчей и позволяет организовать реконфигурацию сервис-ориентированных систем для обеспечения их безопасности и отказоустойчивости.

ПОСТРОЕНИЕ ОТКАЗОУСТОЙЧИВЫХ ВЕБ-СЕРВИСОВ

Веб-сервис представляет собой компонент технологии построения распределенных приложений, основанной на сервис-ориентированной архитектуре. Каж-

дкий компонент веб-сервиса может иметь определенный набор уязвимостей. Под уязвимостью будем понимать особый вид программных дефектов, позволяющих злоумышленнику нарушить такие характеристики информационной безопасности, как целостность, конфиденциальность, управляемость и доступность.

Вероятность безотказной работы веб-сервиса, построенного на стандартной последовательной архитектуре, является произведением вероятностей всех составляющих. Отказ любого из компонентов приводит к отказу работы всего веб-сервиса. Поэтому основной подход повышения надежности такой архитектуры заключается в использовании диверсности (многоверсионности). Такой подход подробно описан в работах [5, 6], основная схема представлена на рис. 1.

компонентов является выбор и систематизация данных об уязвимостях. Существует целый ряд источников, которые предоставляют информацию об уязвимостях в программном обеспечении с целью помочь идентифицировать и устранить известные проблемы безопасности. CVE [7], NVD [8], XForce [9], CERT [10], Secunia [11], SecurityFocus [12] – это далеко не полный список таких источников. Эффективная работа с данными из этих и других источников лежит в основе оценки и обеспечения безопасности программных систем. С целью систематизации, хранения и последующей обработки информации предлагается использовать реляционную базу данных. На рис. 2 представлена модель «сущность-связь» разработанной базы данных.

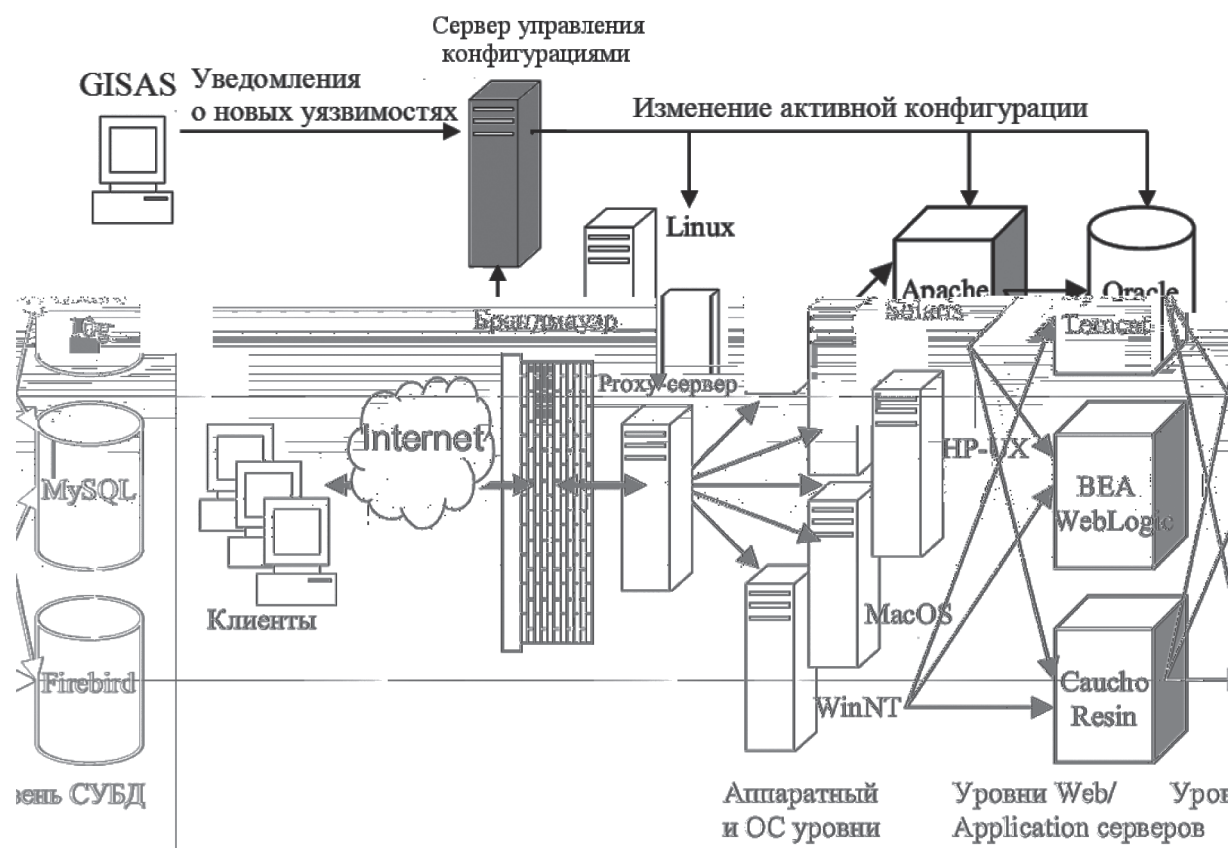


Рис. 1. Архитектура отказоустойчивой сервис-ориентированной системы

Одним из важнейших компонентов данной архитектуры является GISAS (Global Internet Security Alarm Service) - программный модуль анализа уязвимостей. В данной работе мы представляем реализацию такого модуля в качестве веб-сервиса, который анализирует уязвимости в программных компонентах, производит расчеты показателей безопасности и отказоустойчивости и предоставляет информацию для последующей автоматической реконфигурации многоверсионной системы.

АРХИТЕКТУРА И ПРИНЦИП РАБОТЫ ВЕБ-СЕРВИСА

Первым этапом разработки веб-сервиса для оценки безопасности и отказоустойчивости программных

Для решения задачи выбора и систематизации данных из разнородных источников с целью последующего их использования при оценке характеристик OTS компонентов предлагается следующая процедура.

1. Выполнить преобразование информации из исходного формата в объектную модель.
2. Произвести фильтрацию с целью выявления среди полученного на предыдущем этапе множества объектов программной модели, построенных загрузчиком, тех объектов, которые являются уязвимостями.
3. Выполнить отображение (mapping) свойств исходных объектов в свойства объектов предложенной нами системы.

4. Произвести конвертацию полученной объектной модели в реляционную.

Полученная реляционная база данных используется веб-сервисом для решения задачи оценки программных компонент.

веб-сервисом с помощью SOAP-сообщений, передаваемых по HTTP протоколу методом POST. На представленной выше схеме (см. рис. 1) в качестве клиента веб-сервиса выступает сервер управления конфигурациями. Он содержит информацию обо всех программных ком-

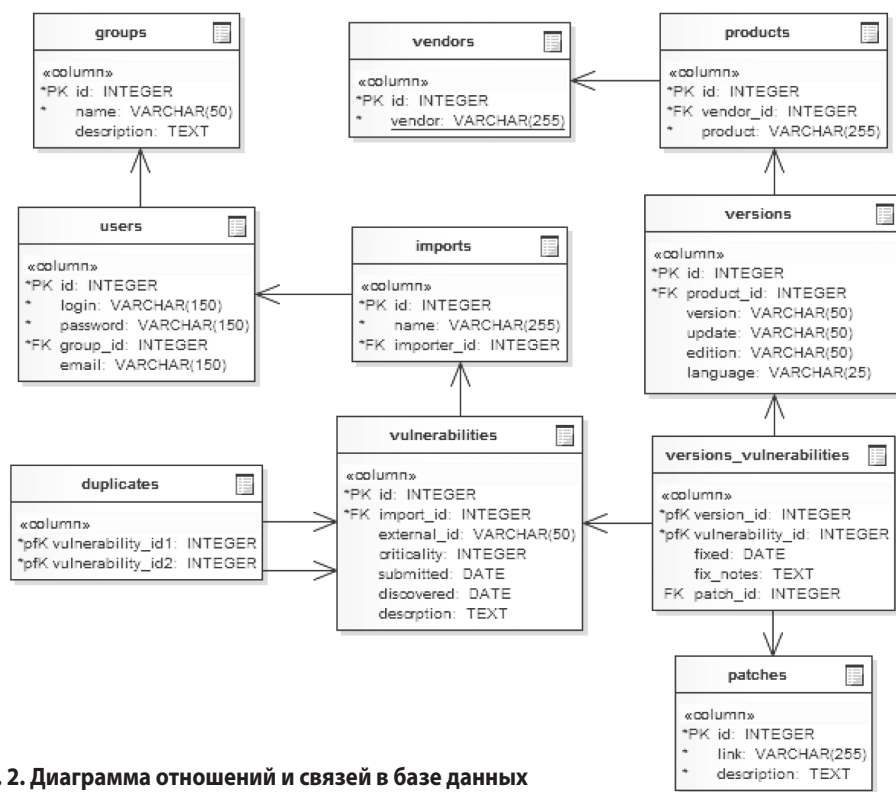


Рис. 2. Диаграмма отношений и связей в базе данных

Рассмотрим архитектуру и принцип работы разработанного веб-сервиса.

Веб-сервис реализован на платформе Microsoft .Net с использованием сервера IIS и базы данных MS SQL Server. Интерфейс веб-сервиса описан в формате WSDL. Клиентские приложения взаимодействуют с

компонентах, используемых в системе, и о том, как эти компоненты связаны между собой.

Архитектура веб-сервиса представлена на рис. 3.

Процесс использования веб-сервиса состоит из следующих этапов.

1. Сервер управления конфигурациями с определенной периодичностью посылает SOAP запросы на веб-сервис с целью проверки безопасности используемых компонентов. Тело такого запроса представляет собой XML сообщение, которое содержит список программных продуктов, их производителей, версий и языков.

2. Веб-сервис получает запрос и обращается к базе данных для получения необходимой информации по каждому конкретному компоненту. На основе полученной информации выявляются открытые угрозы безопасности. Далее рассчитываются различные характеристики безопасности и безотказности программных продуктов, такие как число обнаруженных уязвимостей, степень их критичности, частота отказов, время восстановления, вероятность безотказной



Рис. 3. Архитектура разработанного веб-сервиса

работы и т. д. С помощью экстраполяции полученных результатов производится прогнозирование характеристик в будущем.

Методы оценки по разнородным данным об уязвимостях программных компонент описаны в работах [13, 14, 15]. При наличии патча для исправления бреши в безопасности ссылка на патч извлекается из базы данных и также включается в ответ. Таким образом, на основании извлеченных и рассчитанных значений формируется SOAP ответ веб-сервиса, который отправляется клиенту.

3. Клиент автоматически анализирует полученный ответ веб-сервиса и принимает решение динамической переконфигурации системы, применяет патчи к программным компонентам или перезагружает узлы с альтернативным ПО, в котором не обнаружено брешей.

Сервер управления конфигурациями может также содержать логику для сравнения характеристик различных программных продуктов, полученных от веб-сервиса, и создания оптимальной конфигурации системы, даже при отсутствии на данный момент уязвимостей в используемых компонентах.

Таким образом, основными преимуществами разработанного веб-сервиса можно назвать:

- ✦ помощь в мониторинге безопасности программных компонентов и оповещение клиента об обнаружении новых уязвимостей.
- ✦ расчет различных показателей безопасности и безотказности на основе информации об истории эксплуатации компонента (ретроспективный анализ). Эта функциональность позволяет также сделать прогноз показателей исследуемых компонентов в будущем;
- ✦ предоставление информации о патчах для последующего автоматического устранения уязвимостей.

ВЫВОДЫ

Рассмотренный подход к построению отказоустойчивых систем с сервис-ориентированной архитектурой показал необходимость разработки веб-сервиса для оценки программных компонент на основе данных об уязвимостях. Такой веб-сервис был разработан и представлен в данной работе. Веб-сервис производит анализ данных об уязвимостях, рассчитывает различные показатели безотказности программных продуктов, используемые в дальнейшем для динамической реконфигурации системы. Сервис также предоставляет информацию о патчах, что позволяет предотвращать использование злоумышленниками существующих брешей в безопасности и поддерживать высокий уровень отказоустойчивости различных систем, в частности систем электронного образования. ■

ЛИТЕРАТУРА

1. **Jabr Mohammed A.** e-Learning Management System Using Service Oriented Architecture / Mohammed A. Jabr and Hussein K. Al-Omari // *Journal of Computer Science*.– 2010.– № 6(3).– P. 285 – 295.

2. **Vossen G.** E-Learning as a Web Service / Gottfried Vossen, Peter Westerkamp, // *Seventh International Database Engineering and Applications Symposium (IDEAS'03)*.– 2003.– P. 242.

3. **Liu J.** Modeling Learning Contents Based on Web Services / Jingjing Liu, Yijian Wu, Wenyun Zhao // *Third International Conference on Next Generation Web Services Practices (NWeSP'07)*.– 2007.– P. 135 – 140.

4. **Zhen Zhu.** Design and Implementation of Web-Services Based E-Learning System / Zhen Zhu // *First International Workshop on Education Technology and Computer Science*.– 2009.– Vol. 3.– P. 233 – 237.

5. **Gorbenko A.** F(II)MEA-Technique of Web-services analysis and Dependability Ensuring / A. Gorbenko, V. Kharchenko, O.Tarasyuk, A.Furmanov // *LNCS 4157/ Rigorous Development of complex Fault-Tolerant Systems / M. Butler et al.(eds.)*.– Springer, 2006.– P. 153 – 168.

6. **Фурманов А.** Моделирование гарантоспособных сервис-ориентированных архитектур при атаках с использованием веб-сервисов / А. А. Фурманов, И. Н. Лахижа, В. С. Харченко // *Радіоелектронні і комп'ютерні системи*.– 2009.– № 7(41).– С. 65 – 69.

7. Mitre Corp, Common Vulnerabilities and Exposures, <http://www.cve.mitre.org>

8. National Vulnerability Database, <http://nvd.nist.gov>

9. IBM Internet Security Systems, <http://xforce.iss.net>

10. Computer Emergency Response Team, <http://www.cert.org>

11. Vulnerability and Virus Information, <http://secunia.com>

12. Community of Security Professionals, <http://www.securityfocus.com>

13. **Lobachova K. I.** Assessing Software Vulnerabilities and Recovery Time: Elements Of Technique And Results / Lobachova K. I., Kharchenko V. S. // *Radioelectronic and Computer Systems*.– 2007.– № 8.– P. 61 – 65.

14. Sung-Whan Woo. Assessing Vulnerabilities in Apache and IIS HTTP Servers / Sung-Whan Woo, Omar H. Alhazmi and Yashwant K. Malaiya // *2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06)*. – 2006.– P. 103 – 110.

15. Adelard LLP: Report on the application of safety techniques to security, Part 2, Quantitative modeling Produced (2010).