4. Тарасов Д.О., Пелещищин А.М., Жежнич П.І. Обмежений набір операцій для роботи з базами даних // Інформаційні системи та мережі. Вісник НУ «Львівська політехніка» № 438. – Львів, 2001. – С. 125-131.

5. Bales D. J. Beginning PL/SQL: From Novice to Professional. – Apress, 2007. 476 p.

Надійшла 3.5.2008 р.

УДК 004.052.2: 004.77

А.А. ФУРМАНОВ, В.С. ХАРЧЕНКО
Национальный аэрокосмический университет им. Н.Е.Жуковского, «ХАИ», Харьков
Ю.Л. ПОНОЧОВНЫЙ
Национальный технический университет Украины «КПИ»

МЕТРИКИ ДИВЕРСНОСТИ WEB-ПРИЛОЖЕНИЙ С УЧЁТОМ УЯЗВИМОСТЕЙ

Предложена модель дефектов многоверсионных web-приложений с учётом уязвимостей. Систематизированы метрики диверсности для этих приложений. Сформулированы рекомендации по их использованию для оценки гарантоспособности.

Введение

Одним из способов повышения показателей гарантоспособности [1, 2] информационно-управляющих компьютерных систем является использование многоверсионных технологий [3]. Существуют различные подходы к применению многоверсионных технологий в системах критического применения, однако, в области web-технологий их использование ограничено отсутствием промышленных технологий разработки многоверсионных web-приложений и связанной с этим высокой стоимостью разработки. Современный уровень развития web-технологий и высокая конкуренция в банковском секторе актуализируют задачу использования бизнес-критических технологий в сети Интернет.

В основе многоверсионных технологий лежит принцип диверсности (разнообразия), для оценки уровня которой служат метрики диверсности [4, 5]. Основные концепции оценки диверсности детально изложены в [4, 6, 7].

Web-приложения функционируют в условиях возможных информационных воздействий – сетевых атак, которые могут использовать уязвимости отдельных компонентов системы. Однако, существующие методики оценки гарантоспособности web-систем, базирующихся на использовании диверсности, недостаточно учитывают этот фактор. Это обусловлено тем, что идея применения диверсности для разработки гарантоспособных web-приложений сформирована сравнительно недавно, а информация об уязвимостях их компонент представлена недостаточно полно.

Цель статьи – разработка модели дефектов многоверсионных web-приложений и метрик диверсности для них с учётом уязвимостей.

Модель дефектов и уязвимостей в версиях

Уточним ряд понятий, необходимых для построения модели.

Дефект – любое несоответствие версии требованиям спецификации, результат ошибки, допущенной при разработке. Проявление дефекта при использовании системы (реализации версии) ведёт к ошибке вычислительного или управляющего процесса, т.е. имеет место сбой или отказ и система переходит в неисправное или неработоспособное состояние [1].

Уязвимость – особый вид дефекта, представляющий собой слабозащищённое место в программе, позволяющее злоумышленнику нарушить такие характеристики гарантоспособности (информационной безопасности) системы, как конфиденциальность, целостность, доступность и управляемость.

С учётом [1, 7] дадим классификацию множеств дефектов и уязвимостей многоверсионной системы на примере двухверсионного web-приложения. Эти множества классифицируем следующим образом (рис. 1):

а) по принадлежности к множествам дефектов (уязвимостей) разных версий:

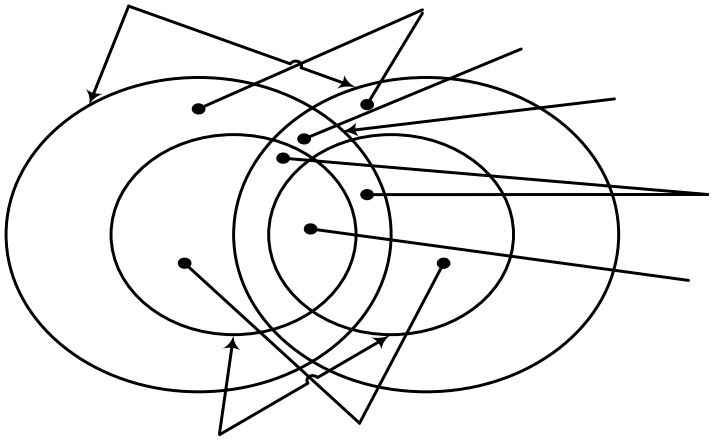


Рис. 1. Классификация дефектов и уязвимостей многоверсионного web-приложения

- относительные (индивидуальные) – принадлежащие только к одной из версий;
- абсолютные – одновременно принадлежащие ко всем версиям;
- групповые – принадлежащие одновременно к нескольким версиям (проявляются при количестве версий n>2);

б) по различимости (для групповых и абсолютных дефектов):

- различимые – вызывающие ошибки, проявляющиеся различным образом при одинаковых входных данных;
- неразличимые – вызывающие идентичные по проявлению (реакции) ошибки;

в) по типам (для групповых и абсолютных дефектов и уязвимостей)

- абсолютные и групповые уязвимости;
- абсолютные и групповые дефекты, не являющиеся уязвимостями;
- абсолютные и групповые дефекты, являющиеся уязвимостями.

На основе полученной модели могут быть получены различные метрики, оценивающие уровень диверсности, а, следовательно, и гарантоспособности многоверсионных web-приложений.

Используя предложенную классификацию, сформируем возможные множества дефектов и уязвимостей (табл. 1).

Таблица 1

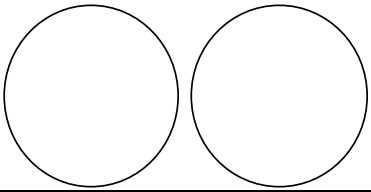
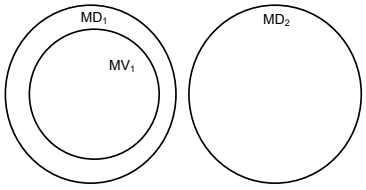
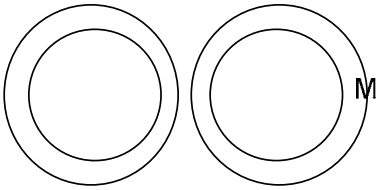
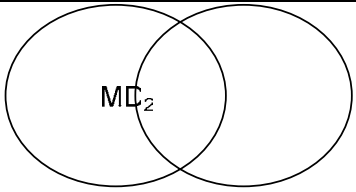
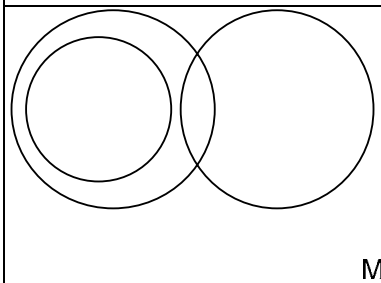
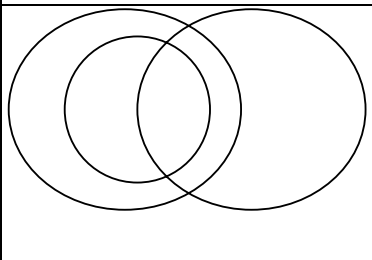
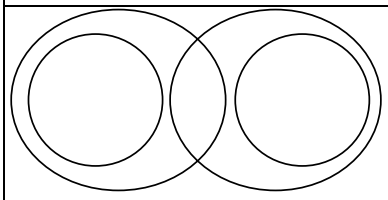
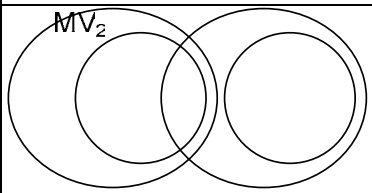
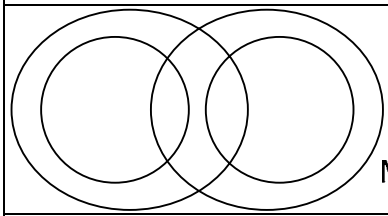
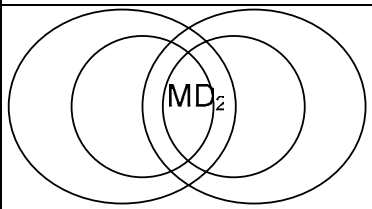
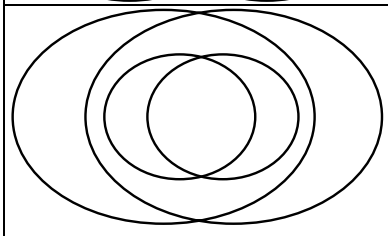
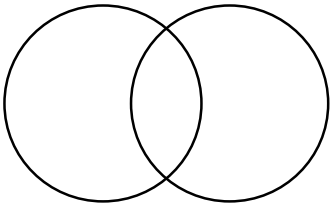
Множества дефектов и уязвимостей

№	Наименование множества	Выражение множества
1	Полное множество дефектов	$MD = MD_1 \cup MD_2$
2	Полное множество уязвимостей	$MV = MV_1 \cup MV_2$
3	Множество дефектов версии 1	$MD_1 = MD \setminus MD_2 \cup (MD_1 \cap MD_2)$
4	Множество дефектов версии 2	$MD_2 = MD \setminus MD_1 \cup (MD_1 \cap MD_2)$
5	Множество уязвимостей версии 1	$MV_1 = MV \setminus MV_2 \cup (MV_1 \cap MV_2)$
6	Множество уязвимостей версии 2	$MV_2 = MV \setminus MV_1 \cup (MV_1 \cap MV_2)$
7	Множество абсолютных дефектов	$MD^A = MD_1 \cap MD_2 = MV^A \cup MD^C \cup MD^{PR}$
8	Множество относительных дефектов версии 1, не являющихся уязвимостями	$MD^C{}_1 = MD \setminus MD_2 \setminus MV_1$
9	Множество относительных дефектов версии 2, не являющихся уязвимостями	$MD^C{}_2 = MD \setminus MD_1 \setminus MV_2$
10	Полное множество абсолютных и групповых дефектов, не являющихся уязвимостями	$MD^C = MD^C{}_1 \cup MD^C{}_2$
11	Множество относительных дефектов версии 1	$MD^R{}_1 = MD \setminus MD_2$
12	Множество относительных дефектов версии 2	$MD^R{}_2 = MD \setminus MD_1$
13	Полное множество относительных дефектов	$MD^R = MD^R{}_1 \cup MD^R{}_2$
14	Множество относительных уязвимостей версии 1	$MV^R{}_1 = MV \setminus MV_2$
15	Множество относительных уязвимостей версии 2	$MV^R = MV^R{}_1 \cup MV^R{}_2$
16	Полное множество относительных уязвимостей	$MV^R = MV^R{}_1 \cup MV^R{}_2$
17	Множество абсолютных и групповых дефектов, не являющихся уязвимостями	$MD^{CNR} = MD_1 \cap MD_2 / (MV_1 \cup MV_2)$
18	Множество абсолютных уязвимостей	$MV^{NR} = MV_1 \cap MV_2$
19	Множество абсолютных и групповых уязвимостей версии 1, являющихся уязвимостями	$MV^{PR}{}_1 = MV_1 \cap MD_2 \setminus MV_2$
20	Множество абсолютных и групповых уязвимостей версии 2, являющихся уязвимостями	$MV^{PR}{}_2 = MV_2 \cap MD_1 \setminus MV_1$
21	Полное множество абсолютных и групповых уязвимостей, являющихся уязвимостями	$MV^{PR} = (MV_1 \cup MV_2) \cap (MD_1 \cap MD_2) \setminus (MV_1 \cap MV_2)$

Рассмотрим различные комбинации соотношений между множествами дефектов и уязвимостей для случая двухверсионного web-приложения (табл. 2).

Таблица 2

Соотношения множеств дефектов и уязвимостей

Соотношение	Описание	Соотношение	Описание
	множества дефектов не пересекаются, уязвимости отсутствуют		множества дефектов не пересекаются, уязвимости присутствуют в одной из версий
	множества дефектов и уязвимостей обоих продуктов не пересекаются, уязвимости присутствуют в обеих версиях		множества дефектов пересекаются, уязвимости отсутствуют
	множества дефектов пересекаются, однако множество уязвимостей в одном продукте отсутствует		множества дефектов пересекаются, множество уязвимостей первого продукта пересекается со множеством дефектов второго продукта, однако множество уязвимостей в одном продукте отсутствует
	множества дефектов первого и второго продуктов пересекаются, однако множества уязвимостей различны между собой и между дефектами противоположных версий		множество уязвимостей первого продукта пересекаются с множеством дефектов второго продукта, однако не пересекается с множеством дефектов второго продукта
	множества дефектов пересекаются, множества уязвимостей не пересекаются		множества дефектов и уязвимостей обоих продуктов пересекаются
	множество уязвимостей первого и второго продуктов пересекаются и при этом полностью входят в множество абсолютных дефектов		множества уязвимостей представляют собой полные множества дефектов соответствующих версий

Метрики диверсности

Обычно *метрикой диверсности* называется отношение количества дефектов, парируемых за счёт версионной избыточности к общему числу дефектов версии [6] (1).

$$K = \frac{n_{distinct}}{N} = \frac{\left| MD \setminus MD^{A} \right|}{\left| MD \right|} \quad (1)$$

Сформулируем множество метрик диверсности многоверсионных web-приложений с учётом

уязвимостей. Для этого построим верхнетреугольную матрицу, столбцы и строки которой представляют собой описанные множества дефектов и уязвимостей из табл. 1, представленные номерами. Элементы матрицы, соответствующие метрикам, имеющем, на наш взгляд, практическую значимость, отметим символом “+” (табл. 3).

Таблица 3

Метрики диверсности

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
2					+	+	+							+	+	+		+	+	+	+
3				+	+		+	+			+			+			+		+		
4						+			+			+			+		+			+	
5						+								+		+			+		
6															+	+				+	
7								+	+	+			+				+	+			+
8									+	+	+										
9										+		+									
10													+				+	+	+	+	+
11												+	+	+							
12													+		+						
13														+	+	+					
14															+	+					
15																+					
16																		+			+
17																		+			+
18																					+
19																				+	+
20																					+
21																					

Всего имеем 83 метрики диверсности, свойственных web-приложениям при учёте уязвимостей. Проведём классификацию метрик диверсности, руководствуясь приведенной выше классификацией множеств дефектов, и опишем наиболее значимые из них:

1) метрики, характеризующие все версии:

- отношение общего числа уязвимостей к общему числу дефектов: $K^{VD} = \frac{|MV|}{|MD|}$;
- отношение общего числа абсолютных дефектов к общему числу дефектов: $K^{DA} = \frac{|MD^A|}{|MD|}$;
- отношение общего числа относительных дефектов к общему числу дефектов: $K^{DR} = \frac{|MD^R|}{|MD|}$;
- отношение общего числа абсолютных уязвимостей к общему числу уязвимостей: $K^{VA} = \frac{|MV^A|}{|MV|}$;
- отношение общего числа относительных уязвимостей к общему числу уязвимостей: $K^{VR} = \frac{|MV^R|}{|MV|}$;

2) метрики, характеризующие одну из версий:

a) отношение числа дефектов конкретной версии к общему числу дефектов: $K^D{}_i = \frac{|MD_i|}{|MD|}$;

b) отношение числа уязвимостей конкретной версии к общему числу уязвимостей: $K^V{}_i = \frac{|MV_i|}{|MV|}$;

c) отношение числа абсолютных дефектов конкретной версии к общему числу дефектов:

$K^{DA}{}_i = \frac{\left|MD^A{}_i\right|}{\left|MD\right|}$;

d) отношение числа относительных дефектов конкретной версии к общему числу дефектов: $K^{DR}{}_i = \frac{\left|MD^R{}_i\right|}{\left|MD\right|}$;

e) отношение числа абсолютных уязвимостей к общему числу чистых дефектов: $K^{VDC}{}_i = \frac{\left|MV^A{}_i\right|}{\left|MD^C\right|}$;

f) отношение числа относительных уязвимостей к общему числу дефектов: $K^{VR}{}_i = \frac{\left|MV^R{}_i\right|}{\left|MV\right|}$;

Кроме того, могут также вычисляться метрики, оценивающие дефекты различных типов:

- метрики уязвимостей: K^{VA}, K^{VR}, $K^V{}_i$, $K^{VA}{}_i$, $K^{VR}{}_i$;
- метрики дефектов: K^{DA}, K^{DR}, $K^D{}_i$, $K^{DA}{}_i$, $K^{DR}{}_i$;
- комплексные метрики (отношения между мощностями множеств уязвимостей и дефектов): K^{VD}, $K^{VD}{}_i$, $K^{VDCA}{}_i$.

Рекомендации по использованию метрик диверсности

В зависимости от продолжительности эксплуатации и накопленной статистической информации о различных версиях, формирующих web-приложения, может быть полезна оценка различных метрик диверсности. Так, если одна из версий недавно введена в эксплуатацию либо обновлена, а по второй существует обширная статистика, то оценка общих метрик, затрагивающих обе версии, малоэффективна, и предпочтение следует отдавать относительным метрикам – $K^{DR}{}_i$ и $K^{VR}{}_i$.

В зависимости от назначения web-приложения и уровня конфиденциальности информации, которую оно обрабатывает, может учитываться вес отказа или сетевой атаки. Так, если в приложении важна конфиденциальность, то при выборе программных продуктов для версий следует стремиться к минимизации показателей комплексных метрик $K^{VPR}{}_i$.

К возникновению абсолютных дефектов и уязвимостей на практике может приводить одновременное использование одинаковых алгоритмов, протоколов обмена данными или программных библиотек, содержащих дефекты, в различных версиях. Ненулевые значения метрик дефектов, принадлежащий к множеству уязвимостей, при таких же условиях, позволяют выявить уязвимости одной версии при обнаружении дефекта во второй, т.е. в первом случае дефект проявляется как уязвимость, а во втором – как дефект.

С увеличением количества версий в системе мощность множества дефектов, принадлежащих к множеству уязвимостей, должна расти.

Выводы

Предложенные модели дефектов многоверсионных web-приложений учитывают особенности уязвимостей их компонент и описывают варианты соответствия множеств дефектов и уязвимостей различных версий.

Полученное множество метрик диверсности позволяет выявить среди них группу наиболее целесообразных с практической точки зрения и разработать методику выбора максимально диверсных (по определённым критериям) web-приложений. Дальнейшая практическая оценка с помощью метрик диверсности даст возможность выявить множество диверсных компонент, способных функционировать в системе, построенной с использованием многоверсионной сервис-ориентированной архитектуры. Элементы предложенной методики оценки диверсности могут быть использованы для построения адаптивных гарантоспособных web-систем [8].

Литература

1. Avizienis A., Avizienis, A., Laprie J. – C., Randell, B., Landwehr, C. Basic Concepts and Taxonomy of Dependable and Secure Computing // IEEE Transactions on Dependable and Secure Computing, – 2004. – Vol.1 – pp.11-33.

2. Харченко В.С. Гарантоздатність комп'ютерних систем: межа універсальності у контексті

інформаційно-технічних станів // Радіоелектронні і комп'ютерні системи. – Х.: ХАІ. – 2007. – Вип. 8. – С. 7 – 14.

3. Харченко В.С., Скляр В.В. Методика моделирования и оценки надежности цифровых систем с многоверсионным программным обеспечением // Электронное моделирование. – 2001. – № 4. – С.54-62.

4. Харченко В.С., Пискачёва И.В., Скляр В.В. Метрики диверсности программных средств: классификация, анализ и применение для оценки надёжности и безопасности компьютерных систем управления // УСИМ: Управляющие системы и машины. – 2000. – № 6-7. – С. 34-53.

5. Скляр В. В. Анализ метрик диверсности программного обеспечения // Электронное моделирование. – 2004. – № 26. – С. 95-104.

6. Lyu M.R., Chen J. – H., Avizienis A. Software diversity metrics and measurements // Computer Software and Applications Conference. COMPSAC '92. Proceedings. – 1992. – pp. 63-68.

7. Волковой А. Метод оценки многоверсионных программных средств с использованием метрик диверсности // Вісник Технологічного університету Поділля. – 2004. – № 2. – С. 143-147.

8. Gorbenko A., Kharchenko V.S., Tarasyuk O., Furmanov A. F (I)MEA-Technique of Web Services Analysis and Dependability Ensuring // Lecture Notes in Computer Science. Rigorous Development of Complex Fault-Tolerant Systems. – Springer – 2007. – pp.153-167.

Надійшла 5.5.2008 р.

УДК 004.052.42: 004.725

Ю.В. ХМЕЛЬНИЦЬКИЙ
Хмельницький національний університет

ТЕЛЕКОМУНІКАЦІЙНІ БЕЗПРОВІДНІ ЗАСОБИ ПЕРЕДАЧІ ДАНИХ

Розвиток засобів зв'язку дозволяє одержати доступ до Internet, корпоративних, міських та локальних мереж не використовуючи існуючі кабельні системи передачі даних. Доступ до глобальних мереж може здійснюватися за допомогою стільникового телефонного і супутникового зв'язку. Для локальних мереж створюються пристрої безпровідного зв'язку на базі ряду стандартів і специфікацій IEEE 802.11 та IEEE 802.16.

Вступ

Безпровідні мережі знаходять широке застосування в таких сферах, як охорона здоров'я, роздрібна торгівля, фінанси, виробництво, складування продукції і т. д., тобто там, де працівникам доводиться часто переміщатися з місця на місце і при цьому їм необхідно передавати і одержувати інформацію. У багатьох сферах діяльності безпровідний зв'язок є часто єдиним способом організації мережі. Крім того, дана технологія надає канал в класичну провідну мережу, відкриваючи доступ до наявних баз даних. До основних переваг безпровідних мереж слід віднести легкість установки і управління, гнучкість конфігурацій, невисоку вартість, масштабованість і захист інформації. Устаткування для створення безпровідних локальних мереж звичайно включає адаптери для портативних і настільних комп'ютерів, точки доступу і відповідне програмне забезпечення. У найпростішому випадку безпровідна мережа може складатися з декількох ком'ютерів, забезпечених безпровідними мережевими картами і спільно використовують файли, принтери, модеми. Ця структура корисна, наприклад, у разі короткострокової співпраці між членами невеликої групи, що працюють над одним і тим же проектом. Мережу можна розширити і охопити значніший простір, використовуючи мережеві точки доступу, які посилають і приймають сигнали на клієнтські безпровідної мережі і від них. Дальність дії сигналів при цьому міняється. Як правило, вона складає близько ста метрів в приміщенні і до триста метрів на відкритому повітрі. У міру збільшення відстані клієнтського ком'ютера від точки доступу швидкість з'єднання зменшується. Кожна точка доступу зоною свого покриття створює так звану мікрокомірку, або стільнику комірку. Клієнтські ком'ютери безпровідної мережі можуть переміщатися по цих стільниках, зони покриття яких перекриваються. Це дозволяє здійснити роумінг для абонентів мережі. Безпровідна мережа здатна функціонувати як самостійно, так і з'єднуватися через точку доступу з провідною мережею.

Аналіз безпровідних технологій передачі даних

Безпровідні мережі працюють в частотному діапазоні від 900 Мгц до 2,4 ГГц, призначеному для промисловості, науки і медицини. Група по розробці специфікації на безпровідні мережі була створена 1990 р. Її перший продукт – стандарт IEEE 802.11 – вийшов лише в червні 1997 р. Цей документ містив необхідну інформацію для організації безпровідних локальних мереж із швидкістю передачі даних 1-2 Мбіт/с. У специфікації була вибрана смуга 83 Мгц в діапазоні 2,4-2,4835 ГГц ISM, який не вимагає додаткового ліцензування на використання практично у всіх країнах світу.

Модель OSI для специфікації 802.11 регламентувала два рівні мережі – фізичний і управління доступом до середовища передачі даних, тобто нижній підрівень канального рівня. На фізичному рівні визначалися методи модуляції і характеристики сигналів для передачі даних. У стандарт було закладено три різні методи передачі: два в радіочастотному і один в інфрачервоному діапазоні хвиль. У останньому випадку повинні бути задіяні довжини хвиль в діапазоні 850-950 нм.

Рекомендовано до друку рішенням вченої ради Хмельницького національного університету, протокол № 11 від 28.05.2008 р.

Підп. до друку 29.05.2008 р. Ум.друк.арк. 30,12 Обл.-вид.арк. 28,66
Формат 30х42/4, папір офсетний. Друк різографією.
Наклад 100, зам. № _____

Тиражування здійснено з оригінал-макету, виготовленого
редакцією журналу "Вісник Хмельницького національного університету"
редакційно-видавничим центром Хмельницького національного університету
29016, м. Хмельницький, вул. Інститутська, 7/1. тел (0382) 72-83-63