О. Б. Одарущенко, доцент, кандидат
технічних наук,
О. Ю. Запорожець, магістрант 501-ТІ(м)
Полтавський національний технічний університет
імені Юрія Кондратюка

Програмна розробка імітаційнного моделювання гарантоздатних web-сервісів з урахуванням дефектів і вразливостей компонент

На сьогоднішній день нові веб-технології забезпечують дуже високу швидкість передачі інформації, одним з наслідків чого є все більша поширеность веб-додатків, які грають головну роль в наданні різноманітної інформації. Динамічний розвиток інтернет-технологій викликаний, зокрема, можливістю цих технологій надавати віддалені послуги. Активно впроваджуються інтернет-служби, які здійснюють бізнес-операції, замовлення квитків, номерів готелів, надають послуги в галузі науки, проектування та ін. Саме тому великого значення набувають якість обслуговування і гарантоздатність веб-сервісів.

Наслідком стрімкого поширення веб-додатків є проблема збільшення мережевих атак, пов'язаних з недосконалістю використовуваних технологій. Аналіз мережевих атак за останні роки показує, що акцент змістився в бік комерціалізації кіберзлочинів. Проведення важливих операцій через Інтернет обумовлює підвищені вимоги до гарантоздатності і безпеки інформаційних систем. Кожна хвилина простою бізнес-критичних систем може призвести до значних збитків і знизити репутацію компанії.

Існують різні способи забезпечення стійкості веб-сервісів від атак, такі як: застосування брандмауерів і апаратних систем виявлення атак, адміністративні обмеження компанії. Та через постійно зростаючу складність сучасних веб-сервісів навіть найсучасніші засоби захисту не завжди забезпечують необхідну стійкість системи до атак. Тому важливим

стає вибір компонентів веб-сервісу з врахуванням уразливостей кожного з них.

Імітаціонне моделювання з урахуванням дефектів і вразливостей компонент дозволяє підвищити точність оцінки гарантоздатності web-сервісів та дослідити залежність показників гарантоздатності від інтенсивності і кратності атак. Отримані результати можна використати для вибору таких компонентів веб-сервісу, котрі будуть забезпечувати кращу гарантоздатність.

Мета роботи

Метою роботи є програмна розробка імітаціонного моделювання гарантоздатних web-сервісів з урахуванням дефектів і вразливостей компонент. Основною цілю моделювання сервіс-орієнтовоної системи є підвищення точності оцінки гарантоздатності таких систем.

Поставка задачі

Вивчити типову архітектури web-сервісу та принципи побудови і структури бази даних уразливостей NVD.

Створити програмну реалізацію імітаціонного моделювання гарантоздатних web-сервісів з урахуванням дефектів і вразливостей компонент.

Використовуючи отриману програму дослідити залежності показників гарантоздатності від параметрів моделювання таких як інтенсивність і кратність атак, конфігурація окремих каналів web-сервіса.

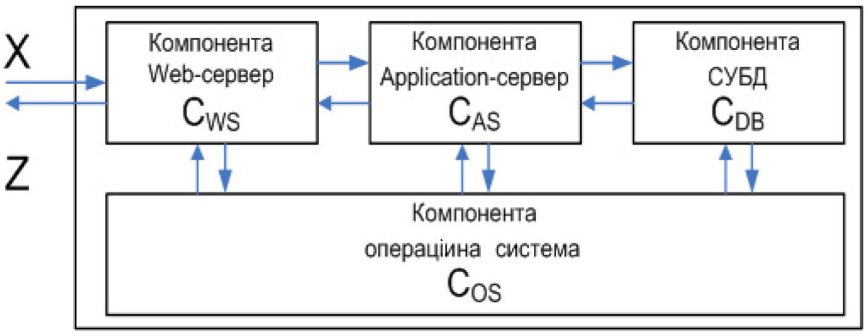
Аналіз моделюємої системи

Основною обчислювальною ланкою архітектури Web-сервісу є «провайдер послуг» .Він виконує обробку запитів, що надходять від клієнтського додатка, і виконання основних завдань бізнес-логіки.

Провайдер послуг складається з чотирьох компонентів:

1. Web-сервер - приймає запити користувачів і видає результати їх обробки за допомогою протоколу HTTP;
2. Application-сервер - виконує завдання бізнес-логіки системи;
3. сервер СУБД -призначений для зберігання та обробки даних;

4. операційна система - є базовою програмною платформою системи



Структурна модель провайдера послуг.

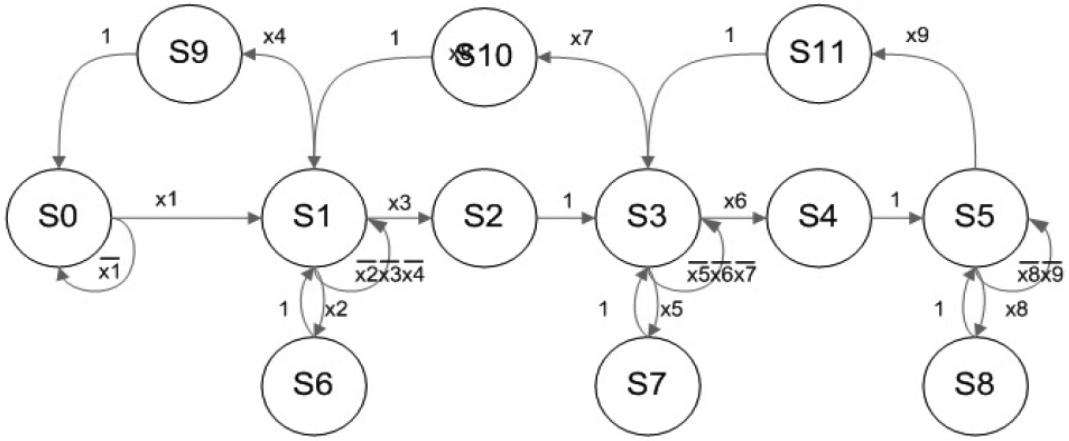
Прийнявши припущення про послідовну обробку запитів використовуючи структурну модель, було визначено множини станів та входів кінцевого автомата для Web-сервіса та складено граф схему алгоритму його роботи.

Стан	Найменування стану
S0	Очікування запиту Web-сервером
S1	Обробка запиту Web-сервером
S2	Відправлення запиту App-серверу
S3	Обробка запиту App-сервером
S4	Відправлення запиту СУБД
S5	Обробка запиту СУБД
S6, S7, S8	Виконання функції ОС
S9	Формування результату Web- сервером
S10	Формування результату App- сервером
S11	Формування результату СУБД

Множина станів автомата Web-сервіса

Вхід	Опис
x1	Отримано HTTP-запит
x2	Web-серверу необхідно виконати функцію ОС
x3	Web-серверу необхідно виконати запит до App-серверу
x4	обробка запиту Web-сервером завершена
x5	App-серверу необхідно виконати функцію ОС
x6	App-серверу необхідно виконати запит до СУБД
x7	обробка запиту App-сервером завершена
x8	СУБД необхідно виконати функцію ОС
x9	обробка запиту СУБД завершена

Множина входів автомата Web-сервіса



Автоматна модель Web-сервісу за якою будується кінцевий автомат Мура

	S0	*S1*	*S2*	*S3*	*S4*	*S5*	*S6*	*S7*	*S8*	*S9*	*S10*	*S11*
x1	*S1*											
-x1	*S0*											
x2												
x3		*S2*										
x4												
-x2-x3-x4												
x5				*S7*								
x6				*S4*								
x7				*S10*								
-x5-x6-x7				*S3*								
x8						*S8*						
x9						*S11*						
-x8-x9						*S5*						
1			*S3*		*S5*		*S1*	*S3*	*S5*	*S0*	*S1*	*S3*

Таблиця переходів автомата Мура для Web-сервісу.

Кожен компонент цього ланцюга має визначений набір вразливостей, закладений в ньому під час розробки.

При моделюванні програмних компонент основними є їх вразливості, а також реакція при атаці на будь-яку вразливость.

Тому в данній системі моделювання програмні компоненти можна представити як набір вразливостей. Для цього використовується база даних вразливостей різноманітних програм, котра містить всі необхідні дані. З їх

допомогою також можна отримати реакцію кожної компоненти на різні типи атак.

При підготовці атаки на Web-сервіс зловмисник спочатку аналізує програмні компоненти, на яких працює атакуємий сервіс. Він вивчає уразливості цих компонент і обирає одну з них, з використанням якої буде проводитись атака. Після цього зловмисник, використовуючи вразливість, створює порушення в роботі Web-сервіса – відмову в обслуговуванні, отримання некоректних результатів чи інші.

Архітектура системи моделювання

Основною цілю моделювання сервіс-орієнтовоної системи є підвищення точності оцінки гарантоздатності таких систем.

Для досягнення даної цілі системи моделювання повинна вирішувати наступні задачі:

- моделювання в статичному режимі (без урахування часових характеристик мережевих атак).
- моделювання в динамічному режимі (з урахуванням часових характеристик)
- надавати дані для подальшого аналізу і розробки гарантоздатних архітектур.

В виконуваному експерименті було змодельовано роботу web-сервіса на вибраних програмних компонентах, атаки на цей сервіс і визначено реакцію сервіса на ці атаки.

Система моделювання складається з таких основних компонент:

- БД і генератор уразливостей
- генератор атак
- сервіси, котрі реалізують визначену функціональність
- оболонка сервіса, котра ємулює вплив атак на роботу сервіса
- БД результатів.

При статичному аналізі в систему додається статичний аналізатор, а при динамічному – генератор задач і конфігуратор.

Генератор вразливостей призначений для початкової конфігурації оболонок сервісів.

Генератор, використовуючи критерії, визначає оболонці сервісу вразливості з БДУ котрі існують у даних компонент. Він запускається до початку експерменту. Результатом роботи генератора вразливостей є відповідність “сервіс- набір вразливостей”.

Дії зловмисника моделюються з використанням *генератора атак*, котрий через визначені проміжки часу надсилає оболонці сервісу “запит-атаку”, яка являє собою набір параметрів – ідентифікатор, час дії атаки та інше.

Генератор задач моделює роботу клієнтів web-сервіса, котрі звертаються до web-сервіса для виконання визначеної задачі, котру він реалізовує.

Для емуляції роботи сервісів на різних програмних компонентах для кожного з них визначається конфігурація : веб-сервер+ сервер додатків + операційна система з врахування сумісності компонентів.

Для моделюювання реакції сервера і программних компонентів на атаки використовується *оболонка сервіса*. Вона виступає як фільтр між клієнтои і сервісом, що дозволяе її підміняти відповідь сервіса на запит кліента. Відповідь формується в відповідності з поточними параметрами середовища-конфігурації системи, атаками на даний сервер.

БД результатів зберігає дані експерименту для подальшого вивчення і аналізу.

Модель дефектів (уразливостей) компонентів сервіс-оріентованих архітектур

Дефект- будь-яка не відповідність версії вимогам специфікації, результат помилки, допущеної при розробці. Прояви дефекту при використанні системи призводить до помилки обчислювального чи керуючого процесу, тобто має місце збій або відмова і система переходить в несправний або неробочий стан.

Уразливість- особливий вид дефекту, який являє собою слабозахищене місце в програмі, що дозволяє зловмиснику порушити такі характеристики гарантодатності (інформаційної безпеки) системи, як конфіденційність, цілісність, доступність, керованість.

Множина дефектів містить підмнодину уразливостей $MD = MV\ U\ MD^c$.

Головним параметром вразливості є критичність, яка визначається наслідками для компонентів. Атака характеризується такими параметрами як час дії, кратність та список вразливостей що використані.

Час дій атаки складається з двох періодів: часу безпосереднього впливу атаки (коли веб-сервіс заблокований) і часу післядії (коли відбувається відновлення сервіса в робочий стан).

Бази даних вразливостей (БДУ)

Більша частина доступних БДУ підтримує стандарт іменування вразливостей CVE (Common vulnerabilities and exposures), що гарантує відсутність перетину множин в різних БДУ.

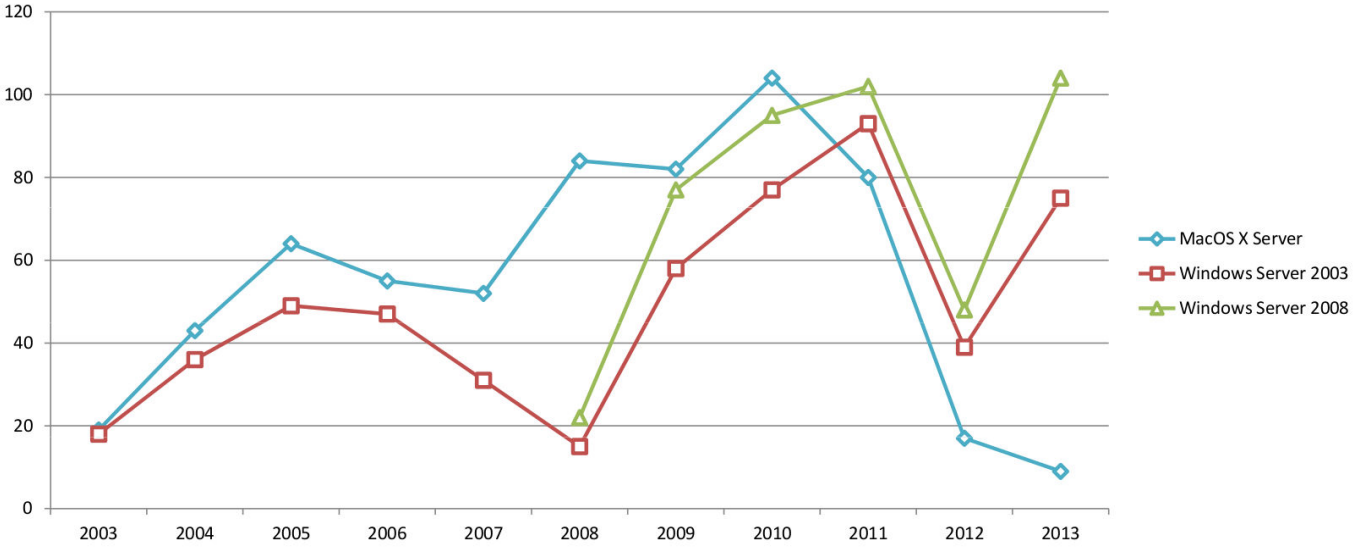
Назва БДУ	Адреса	Кількість уразливостей тис.	Ідентифікатори CVE	Дані в XML
Mitre	https://cve.mitre.org	23,4	+	+
Open Source Vulnerability Database (**OSVDB**)	https://osvdb.org	14,6	+	
National Vulnerability Database (**NVD**)	https://nvd.nist.gov/	22,5	+	+
Security Focus	www.securityfocus.com/	21	+	
Security Focus	www.securitytracker.com	11,1	+	
Secunia	www.srcunia.com	17	+	

Далі в роботі використовується БДУ NVD (National Vulnerability Database https://nvd.nist.gov/) через наявність в ній розширеної інформації про атаки, тип враження, тип атаки, серйозність атаки, діапазон атаки.

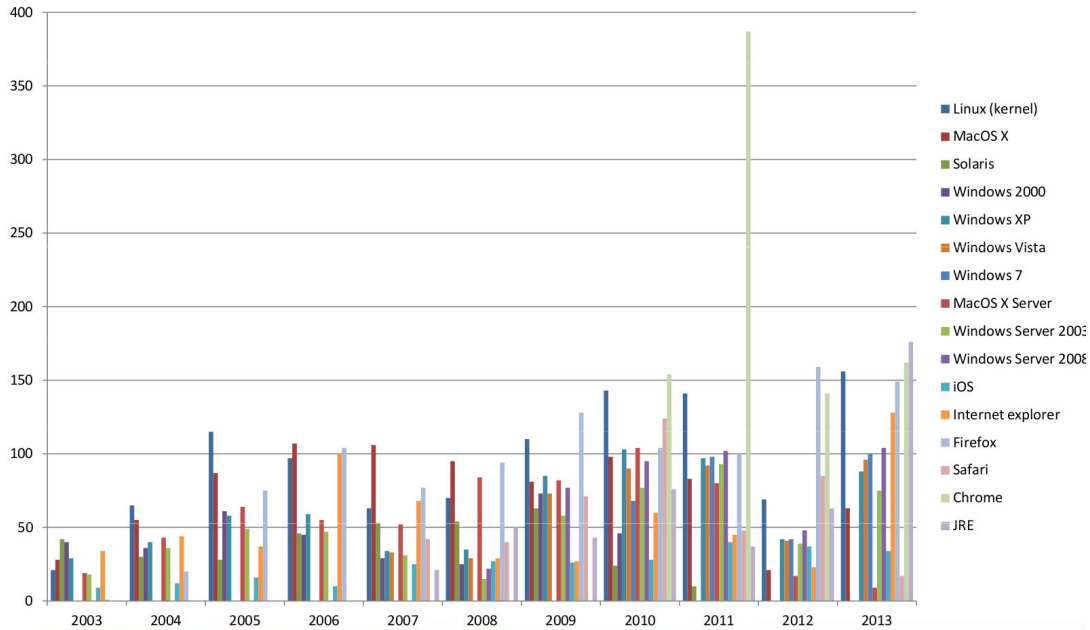
Для подальшого аналізу БДУ NVD в форматі XML була конвертована в базу даних MySQL з відповідною структурою.

Обробку даних, перенесених в реляційну БД зручно проводити за допомогою запитів мови SQL.

Результати SQL запитів



Кількість вразливостей серверних ОС



Кількість вразливостей деяких популярних програмних продуктів

Висновки

У виконуваному експерименті була змодельована робота web-сервіса на вибраних програмних компонентах, атаки на цей сервіс і визначено реакцію сервіса на ці атаки. Була вивчена типова архітектура web-сервера, описаний алгоритм роботи web-сервіса, побудований скінчений автомат Мура для отриманого алгоритму. Створена програмна реалізація імітаційної моделі та інтерфейс користувача програми.

Визначена імітаційна модель дозволяє підвищити точність оцінки та дослідити залежність показників гарантоздатності web-сервісів від інтенсивності і кратності атак. Отримувані результати роботи можна застосовувати для вибору такої конфігурації компонентів веб-сервісу, яка буде забезпечувати кращу гарантоздатність.

Література

1. Куланов С. А., Локазюк В. Н., Одарущенко О. Н., Поморова О. В., Сиротюк А. И., Фурманов А. А., Харченко В.С. Моделирование гарантоспособных систем и сетей. Практикум / Под ред. Харченко В.С. – Национальный аэрокосмический університет им. Н. Е. Жуковского “ХАИ”, 2008. – 175 с.
2. Харченко В.С., Боярчук А. В., Куланов С. А., Локазюк В. Н., Одарущенко О. Н., Поморова О. В., Фурманов А. А. . Моделирование гарантоспособных систем и сетей. Лекционный материал / Под ред. Харченко В.С. – Национальный аэрокосмический університет им. Н. Е. Жуковского “ХАИ”, 2008. – 336 с.
3. Web Services Architecture [Электр. ресурс] - Режим доступа: http://www.w3.org/TR/ws-arch/.
4. Web service [Электр. ресурс] – Режим доступа http://en.wikipedia.org/wiki/Web_service.