ВІДГУК

офіційного опонента

Трубчанінової Карини Артурівни

на дисертаційну роботу **Цао Вейлінь**

«МЕТОД ПІДВИЩЕННЯ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ТЕХНОЛОГІЙ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ»,

представлену на здобуття наукового ступеня доктора філософії

за спеціальністю 123 – Комп'ютерна інженерія

Актуальність теми

Забезпечення безпеки програмного забезпечення (ПЗ) є критично важливим, оскільки помилки у ПЗ можуть призвести до великих проблем, включаючи порушення конфіденційності, цілісності і доступності даних, а також можуть спричинити серйозні проблеми з безпекою в Інтернеті та комп'ютерних мережах.

Сучасні дослідження показують, що одним з механізмів захисту програмного забезпечення є тестування його безпеки. Цей процес повинен виконуватися на всіх етапах життєвого циклу розробки програмного забезпечення. Але нажаль існуючи методи, підходи та засоби потребують певного вдосконалення. При цьому існує безліч різних рекомендацій технічного, соціального, психологічного та інших напрямків з ефективного використання зазначеного механізму захисту. Це і незалежний аудит програмного забезпечення, використання чітко сформульованої політики з налагодженою системою оповіщення, а також інструментів для резервного копіювання, і звичайно автоматизація процесу з використанням інструментів реверсної інженерії та активного виявлення, які б знаходили як дозволені, так і недозволені прийоми кодування.

Синтез технологій автоматизованого тестування безпеки ПЗ та глибоке машинне навчання можуть допомогти підвищити безпеку ПЗ, виявляючи і виправляючи помилки раніше, ніж вони можуть бути експлуатовані зловмисниками. Крім того, ці технології можуть знизити вартість та збільшити ефективність процесу тестування безпеки.

Таким чином, розробка методу підвищення безпеки програмного забезпечення на основі технологій тестування на проникнення є актуальним науковим завданням.

Дисертаційну роботу виконано на кафедрі комп'ютерної інженерії та програмування Національного технічного університету "Харківський політехнічний інститут".

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертаційній роботі.

Положення та висновки, наведені в дисертаційній роботі Цао Вейлінь, в достатній мірі обґрунтовані як з наукового, так і з технічного поглядів. Обґрунтованість отриманих у роботі наукових положень, висновків і рекомендацій базується на використанні математичного апарату теорії машинного навчання, теорії імовірності та математичної статистики, теорії інформації, методів математичного та імітаційного моделювання з використанням ліцензійного програмного забезпечення.

Дослідження виконані з використанням математичного апарату та сучасного комп'ютерного моделювання. Результати перевірені шляхом проведення практичних експериментів, що підтверджує обґрунтованість наукових положень, висновків і рекомендацій, сформульованих в дисертаційній роботі.

Достовірність результатів досліджень.

Достовірність результатів теоретичних досліджень підтверджується результатами відповідних експериментальних досліджень.

Наукові результати застосовані під час створення імітаційних моделей з використання математичного пакету MathCad.

До основних нових наукових результатів дисертації слід віднести наступне:

1. Вперше був розроблений метод автоматизованого тестування на вторгнення з використанням пошукової системи Shodan, платформи аналізу безпеки мережі MulVal і даних про вразливості програмного забезпечення CVE для введення та створення реалістичних сценаріїв атак і перевірки для глибокого навчання з технологією підкріплення. Це дозволило сформувати дерево атак для різних процедур навчання, оптимізувати відповідні сценарії автоматичного тестування безпеки програмного забезпечення, а отже, підвищити ефективність процесу безпеки програмного забезпечення.

2. Удосконалена математична модель процесу тестування на проникнення в комп'ютерні системи, відмінна від відомих можливістю тестування безпеки спеціалізованих інформаційних платформ комп'ютерних систем, що дозволило оцінити ймовірність часу тестування на проникнення в заданому інтервалі.

3. Розроблено математичну модель процесу тестування на проникнення в комп'ютерні системи. Відмінною рисою цієї моделі є використання розподілу Ерланга як основного при математичній формалізації процесів переходу від стану до стану. Це дозволило, з одного боку, уніфікувати математичну модель і представити процес тестування на більш високому рівні ієрархії тестування, з іншого боку, спростити його.

Значимість отриманих результатів для науки і практичного використання.

Практичне значення отриманих результатів полягає в адаптації процесу тестування програмного забезпечення до підвищених вимог безпеки та можливостей засобів автоматизації тестування, використовуючи технології глибокого навчання з підкріпленням.

Практичне значення отриманих результатів полягає в наступному.

1. Набір математичних моделей процесу тестування на проникнення в комп'ютерних системах з використанням підходу мережевого моделювання GERT спростив схему тестування на проникнення в 1,7 рази з урахуванням можливих змін у процедурах (включаючи додавання нових процедур і сервісів) для оцінки ймовірнісно-часових характеристик та можливості її масштабування при збільшенні обсягу та складності задач, що розв'язуються.

2. Синтез основних компонентів методу автоматичного тестування на проникнення дозволив підвищити ефективність процесу забезпечення безпеки ПЗ (зменшити відносний збиток на всіх етапах життєвого циклу ПЗ у 6 разів).

Результати дисертації впроваджені та використані в діяльності компанії "Line Up", ННЦ "Інститут судових експертиз", а також використовуються в навчальному процесі НТУ "ХПІ".

Повнота викладення результатів досліджень в опублікованих працях.

Основні положення дисертації опубліковано у 15 наукових працях, серед яких: 8 наукових статей (з них 2 включено до бази даних Scopus; 6 – у вітчизняних фахових наукових виданнях), а також 7 тез доповідей (з них 1 – включено до бази даних Scopus).

Участь здобувача у роботах, що опубліковані у співавторстві зазначена у дисертаційній роботі.

Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пункту 8 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого Постановою КМУ від 12.01.2022 р. №44.

Оцінка змісту дисертаційної роботи

Дисертаційна робота Цао Вейлінь складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, додатку.

В роботі проведено аналіз вразливостей ПЗ, зазначено на пріоритетність вимог безпеки ПЗ та обов'язковість дотримання цих вимог на всіх етапах життєвого циклу ПЗ. Проведено дослідження та порівняльний аналіз методик виявлення

вразливостей, вказано на недостатність уваги з боку розробників питань безпеки. Проаналізовано основні напрямки та підходи математичного моделювання, виділено перспективні напрямки математичної формалізації процесів тестування безпеки програмного забезпечення. Вказано на доцільність удосконалення існуючих методів тестування на проникнення шляхом синтезу нового методу тестування з урахуванням підвищених вимог безпеки.

Розроблено узагальнений алгоритм тестування, а також комплекс математичних моделей процесу тестування на проникнення до комп'ютерних систем. При цьому за основу математичної формалізації взято підхід GERT-мережевого моделювання. Це дозволило спростити схему тестування на проникнення, врахувати можливі зміни процедур (у тому числі і додавання нових процедур та послуг) оцінити імовірнісно-часові характеристики та можливості її масштабування зі збільшенням обсягу та складності завдань, що вирішуються.

У розділі розроблено математичну модель процесу тестування на проникнення в комп'ютерні системи, що відрізняється від відомих врахуванням можливостей тестування безпеки спеціалізованих інформаційних платформ комп'ютерних систем, що дозволило оцінити ймовірність влучення часу виконання алгоритму тестування на проникнення в заданий інтервал.

Запропонована математична модель процесу тестування на проникнення в комп'ютерні системи набула подальшого розвитку (модифікована). Відмінною особливістю даної моделі є використання розподілу Ерланга як основного при математичній формалізації процесів переходу зі стану. Це дозволило з одного боку уніфікувати математичну модель і представити процес тестування більш високому рівні ієрархії тестування, з іншого боку спростити її у 1,7 разу.

Розроблено метод автоматичного тестування на проникнення. Відмінною особливістю методу є комплексне використання пошукової системи Shodan, платформи аналізу мережевої безпеки MulVal, а також даних про вразливість програмного забезпечення – CVE для отримання вхідних даних та побудови реалістичних сценаріїв атак та перевірки у рамках технології глибокого навчання із підкріпленням. Це дозволило згенерувати дерево атак для різних процедур навчання та провести оптимізацію відповідних сценаріїв автоматичного тестування безпеки програмного забезпечення.

При дослідженні, відповідно до методу глибокого навчання з підкріпленням, були використані оцінки винагороди, що призначаються кожному вузлу відповідно до рейтингу CVSS. Це дозволило зменшити дерева атак та визначити атаку з більшою ймовірністю виникнення.

Для оцінки застосовності методу проведено експеримент та згенеровано дерево

атак, також сформовано сценарій тестування та навчання. Підтверджено факт, що навіть за невеликої кількості сценаріїв навчання результати моделювання досягають значення 0.9 щодо найбільш раціонального шляху атаки.

Вдосконалено спосіб оцінки ефективності методу тестування безпеки ПЗ. Його відмінністю є врахування можливості масштабування процесу розробки ПЗ шляхом впровадження фахівців з тестування безпеки (DevSecOps, SecDev, а також тестувальників на проникнення).

В основу вдосконаленого способу оцінки ефективності методу підвищення безпеки програмного забезпечення покладено метод динаміки середніх.

За допомогою вдосконаленого способу доведено доцільність використання розробленого методу підвищення безпеки ПЗ з урахуванням можливостей технології глибокого навчання з підкріпленням. Це дозволить знизити показник відносної шкоди на всіх етапах життєвого циклу до 6 разів, залежно від можливої тривалості кібервторгнення.

Висновки до розділів та за результатами роботи сформульовані чітко та відповідають змісту дисертаційної роботи.

Список використаних джерел із 134 найменувань досить повний і включає вітчизняні та зарубіжні публікації.

Анотація відображає основний зміст дисертації та достатньо повно розкриває наукові результати та практичну цінність роботи.

Академічна доброчесність

Порушень академічної доброчесності в дисертації та наукових публікаціях, у яких висвітлені основні наукові результати дисертації, не виявлено.

Усі результати, які винесено автором на захист, отримані самостійно і містяться в опублікованих роботах. У роботах, опублікованих у співавторстві, використані тільки ті ідеї, положення та розрахунки, які є результатом особистих наукових пошуків.

По дисертаційній роботі можна зробити наступні зауваження:

1. Деякі типи ПЗ можуть бути більш складними для тестування на проникнення, оскільки вони можуть містити дуже складні механізми захисту, які ускладнюють процес знаходження вразливостей.

2. Автоматизоване тестування безпеки ПЗ може бути обмежене в тому випадку, якщо не вдалося відтворити умови реального використання ПЗ. Наприклад, тестування може бути обмежене, якщо тестові середовища не повністю відображають умови реального використання ПЗ.

3. Глибоке навчання вимагає великої кількості даних для навчання моделей. Якщо даних недостатньо, може бути складно побудувати ефективну модель для

виявлення вразливостей. Також, необхідно враховувати можливість атак на саму модель глибокого навчання.

4. Важливо враховувати змінність атак і техніки атак на ПЗ, оскільки захисні методи можуть швидко застарівати. Потрібно регулярно оновлювати технології тестування і захисту, щоб зберігати ефективність захисту від нових загроз.

Вказані недоліки не впливають на загальну позитивну оцінку виконаної роботи. Дисертація є актуальною і має високу наукову цінність та практичну значущість.

ВИСНОВОК

Дисертаційна робота Цао Вейлінь «МЕТОД ПІДВИЩЕННЯ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ТЕХНОЛОГІЙ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ» за своїм змістом відповідає спеціальності 123 – Комп'ютерна інженерія. Дисертація є завершеною науково-дослідною роботою, яка розв'язує важливу науково-практичну задачу, що складається в підвищенні точності прийняття рішень щодо безпеки програмного забезпечення на основі синтезу комплексу математичних моделей і методу підтримки прийняття рішень щодо безпеки програмного забезпечення..

Подана дисертаційна робота Цао Вейлінь «МЕТОД ПІДВИЩЕННЯ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ТЕХНОЛОГІЙ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ» відповідає спеціальності 123 – Комп'ютерна інженерія, відповідає вимогам до дисертацій на здобуття наукового ступеня доктора філософії, а саме вимогам пунктів 6, 7, 8 і 9 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого Постановою КМУ від 12.01.2022 р. №44, а здобувач Цао Вейлінь заслуговує присудження наукового ступеня доктора філософії за спеціальністю 123 – Комп'ютерна інженерія.

Офіційний опонент
Професор кафедри транспортного зв'язку
Українського державного університету
залізничного транспорту, д.т.н., професор
12.06.2023 Карина ТРУБЧАНІНОВА

Особистий підпис
засвідчую 12.06 2023 р.
Завідуючий канцелярією
УкрДУЗТ
Карина Трубчанінова