

ВІДГУК

офіційного опонента

завідувача кафедри електронних обчислювальних машин

Харківського національного університету радіоелектроніки,

доктора технічних наук, професора Коваленка Андрія Анатолійовича

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

Дисертаційна робота Цао Вейлінь присвячена вирішенню актуальної науково-технічної задачі розробки методу підвищення безпеки програмного забезпечення (ПЗ) з урахуванням можливостей синтезу технологій автоматизованого тестування безпеки ПЗ та глибокого машинного навчання. Тема дисертаційної роботи спрямована на забезпечення інформаційної безпеки, через підвищену увагу питанням безпеки ПЗ. Необхідність розробки такого методу обумовлена зростаючим використанням засобів комп'ютерної техніки у всіх сферах життєдіяльності суспільства, зокрема у системах критичного застосування. Це призводить до необхідності пришвидшення темпів розробки ПЗ, що викликає іноді нехтування питаннями безпечного програмування та тестування безпеки. В умовах використання гнучких методологій розробки ПЗ існують можливості адаптивного застосування ресурсів фірм-розробників програмних засобів. Але, на жаль, поточний стан відповідної проблематики та методів проектування розробкою демонструє переважне нехтування аспектами безпеки. Це зумовлене, з одного боку, небажанням виробників мати додаткові трати, з іншого боку, відсутністю моделей та методів проектування, що можуть обґрунтовано довести ефективність безпечного програмування та тестування.

Використання розробленого методу дозволить організаціям-виробникам ПЗ скорегувати плани проектування та розробки, а також більш ефективно

використовувати існуючий потенціал з врахуванням підвищених вимог щодо безпеки програмних засобів.

Таким чином, розробка методу підвищення безпеки ПЗ 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, що наведено 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 ймовірності та математичної статистики, теорії інформації, методів математичного та імітаційного моделювання з використанням ліцензійного ПЗ.

Дослідження виконано з використанням математичного апарату та сучасного комп'ютерного моделювання. Результати перевірено 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 застосовано 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 вторгнень з використанням пошукової системи Shodan, платформи аналізу мережної безпеки MulVal та даних вразливостей програмного забезпечення CVE для введення та побудови реалістичних сценаріїв атаки та перевірки для глибокого навчання за допомогою технології підкріплення, що дозволило згенерувати дерево атак для різних навчальних процедур, оптимізувати відповідні сценарії автоматичного тестування

безпеки програмного забезпечення, і таким чином підвищити ефективність процесу безпеки програмного забезпечення.

2. Удосконалена математична модель процесу тестування на проникнення в комп'ютерні системи, відмінна від відомих можливостей тестування захищеності спеціалізованих інформаційних платформ комп'ютерних систем, що дозволило оцінити ймовірність тестування часу на проникнення в заданий інтервал.

3. Отримано подальший розвиток математичної моделі процесу тестування на проникнення в комп'ютерні системи. Відмінною особливістю цієї моделі є використання розподілу Ерланга в якості 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 – спростити його.

Значимість отриманих результатів для науки і практичного використання

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

Практичне значення отриманих результатів полягає в наступному.

1. Комплекс математичних моделей процесу тестування на проникнення в комп'ютерних системах з використанням мережного підходу моделювання GERT спростив схему тестування на проникнення в 1,7 рази з урахуванням можливих змін процедур (включаючи додавання нових процедур і послуг) для оцінки ймовірнісно-часових характеристик і можливостей його масштабування при збільшенні обсягу і складності розв'язуваних задач.

2. Синтез основних компонентів методу автоматичного тестування на проникнення дозволив підвищити ефективність процесу безпеки програмного забезпечення (знизити відносні пошкодження на всіх етапах життєвого циклу програмного забезпечення до 6 разів).

Результати дисертації впроваджено та використано в діяльності компанії “LineUp”, Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України, а також використовуються в навчальному процесі Національного технічного університету “Харківський політехнічний

інститут”.

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 та додатків.

У вступі обґрунтовано актуальність теми дисертації, показано її наукову і практичну цінність, сформульовано мету і задачі дослідження, які необхідно вирішити для її досягнення, описано зв'язок дисертації з науковими планами та темами, приведено апробацію дисертаційної роботи і відповідні публікації.

У першому розділі проведено аналіз основних методів виявлення вразливостей ПЗ. Показано, що використання існуючих методів та методик аналізу безпеки не забезпечує точності результату в умовах нечітких вхідних даних.

У другому розділі 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-мережного моделювання. Це дозволило спростити схему тестування на проникнення, врахувати можливі зміни процедур (у тому числі і додавання нових процедур та послуг) оцінити ймовірнісно-часові характеристики та можливості її масштабування зі збільшенням обсягу та складності завдань, що вирішуються.

У третьому розділі розроблено метод автоматичного тестування на

проникнення. Відмінною особливістю методу є комплексне використання пошукової системи Shodan, платформи аналізу мережної безпеки MulVal, а також даних про вразливість ПЗ – CVE, для отримання вхідних даних та побудови реалістичних сценаріїв атак та перевірки у рамках технології глибокого навчання із підкріпленням. Результатом є генерація дерева атак для різних процедур навчання та оптимізація відповідних сценаріїв автоматичного тестування безпеки ПЗ.

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

Для оцінки застосовності методу у четвертому розділі 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).

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

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

Список використаних джерел складається зі 134 найменувань. Він є досить повним і включає вітчизняні та зарубіжні публікації.

Анотація відбиває 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, отримано самостійно і містяться в опублікованих роботах. У роботах, опублікованих у співавторстві, використано лише ті ідеї, положення та розрахунки, які є результатом особистих наукових пошуків.

За дисертаційною роботою можна зробити наступні зауваження:

1. У першому розділі автор, нажаль, приділяє недостатньо уваги аналізу методів тестування ПЗ, хоча саме ці методи було покладено в основу дослідження.
2. У другому розділі, при моделюванні технології управління та тестування програмних засобів, автор використовує підхід, що пов'язаний з використанням GERT-мереж. Але цей підхід має недоліки, пов'язані зі значним ускладненням розрахунків при додаванні елементів у структуру мережі. Тому навіть незначне ускладнення процесу тестування призведе до ускладнення самої моделі.
3. У третьому розділі, при розробці методу, автор пропонує використовувати деякі числові коефіцієнти, так звані «винагороди». Але, нажаль, теоретичного обґрунтування значень цих коефіцієнтів автор не наводить.
4. У дисертаційній роботі не наведено аргументів використання методу динаміки середніх для оцінки ефективності розробленого методу.

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-технічну задачу, що складається в підвищенні точності прийняття рішень щодо безпеки програмного забезпечення на основі синтезу комплексу математичних моделей і методу підтримки прийняття рішень.

Дисертаційна робота Цао Вейлінь «МЕТОД ПІДВИЩЕННЯ БЕЗПЕКИ

ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ТЕХНОЛОГІЙ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ» 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

доктор технічних наук, професор

завідувач кафедри електронних обчислювальних машин

Харківського національного університету радіоелектроніки



Андрій КОВАЛЕНКО

“ 12 ” 06 2023 р.

ПІДПИС ЗАСВІДЧУЮ

В.о. ректора

доктор технічних наук, професор



“ 12 ” 06 2023 р.

Ігор РУБАН