Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U001801

Особливі позначки: відкрита

Дата реєстрації: 03-05-2024

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: № НСВС_62_24 від 23.07.2024

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Куб'юк Євгеній Юрійович
2. Yevhenii Y. Kubiuk

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0002-7086-0976

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп’ютерні науки

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп'ютерні науки

Дата захисту: 03-07-2024

Спеціальність за освітою: Комп'ютерні науки

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 26.002.161; ID 5576

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, буд. 37, Київ, 03056, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, буд. 37, Київ, 03056, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.23, 20.56.01

Тема дисертації:

1. Аналіз програмного коду з використанням гібридного методу пошуку та класифікації вразливостей
2. Source code analysis using a hybrid method of detecting and classifying vulnerabilities

Реферат:

1. Дисертація присвячена розробці та дослідженню системи автоматизованого аналізу програмного коду для виявлення вразливостей безпеки з використанням гібридного підходу, що поєднує методи глибокого навчання та методи виявлення подібності коду. Актуальність теми зумовлена зростанням кількості вразливостей у програмному забезпеченні та потребою створення ефективних засобів їх виявлення для зниження ризиків кібератак. У роботі проведено аналіз сучасного стану проблеми, розглянуто існуючі методи та підходи до детекції вразливостей, визначено їх переваги та недоліки. На основі цього запропоновано математичні моделі аналізу з використанням нейронних мереж та ковзного хешування абстрактних синтаксичних дерев, які в поєднанні формують систему аналізу програмного коду. Наукова новизна дослідження полягає у розробці вдосконаленого методу побудови проміжного представлення коду

у вигляді кодових гаджетів та методу класифікації вразливостей на основі алгоритму ковзного хешування вузлів AST. Практичне значення підтверджується експериментальними результатами, зокрема точністю детекції вразливостей на рівні 94.1% та багатокласової класифікації в 51.1% для 40 типів загроз. Апробація результатів здійснювалася шляхом тестування розробленої системи на програмних проектах з відкритим вихідним кодом. Запропоновано сценарії інтеграції рішення в процеси безперервної інтеграції та передрелізної верифікації програмного забезпечення. Отримані результати мають теоретичну цінність, оскільки розширюють науково-методологічну базу в сфері статичного аналізу програмного коду та відкривають перспективи для подальших досліджень на перетині машинного навчання та кібербезпеки. Практична значущість полягає у можливості застосування розробленої системи для підвищення рівня захищеності програмних продуктів та зниження ризиків вразливостей.

2. The dissertation is devoted to the development and research of an automated source code analysis system for detecting security vulnerabilities using a hybrid approach that combines deep learning methods and code similarity detection methods. The relevance of the topic is due to the increasing number of vulnerabilities in software and the need to create effective means of detecting them to reduce the risks of cyber attacks. The work analyzes the current state of the problem, examines existing methods and approaches to vulnerability detection, and identifies their advantages and disadvantages. Based on this, mathematical models of analysis using neural networks and sliding hashing of abstract syntax trees are proposed, which together form a system for analyzing source code. The scientific novelty of the research lies in the development of an improved method for constructing an intermediate code representation in the form of code gadgets and a method for classifying vulnerabilities based on the AST node sliding hash algorithm. The practical significance is confirmed by experimental results, in particular, the accuracy of vulnerability detection at the level of 94.1% and multiclass classification at 51.1% for 40 types of threats. The results were tested by applying the developed system to open-source software projects. Scenarios for integrating the solution into the processes of continuous integration and pre-release verification of software are proposed. The obtained results have theoretical value, as they expand the scientific and methodological base in the field of static analysis of source code and open up prospects for further research at the intersection of machine learning and cybersecurity. The practical significance lies in the possibility of using the developed system to increase the level of security of software products and reduce the risks of vulnerabilities.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Kubiuk, Y., Chernousov, A., Savchenko, A., Osadchyi, S., Kostenko, Y., & Likhomanov, D. (2019). Deep learning based automatic software defects detection framework.
- Kubiuk, Y., & Kyselov, G. (2021). Comparative analysis of approaches to source code vulnerability detection based on deep learning methods. Technology audit and production reserves, 3(2), 59.
- Kaliuzhna, T., & Kubiuk, Y. (2022). Analysis of machine learning methods in the task of searching duplicates in the software code. Technology audit and production reserves, 4(2 (66)), 6-13.
- Kubiuk, Y., & Kyselov, G. (2023). Development of an algorithm for code clone detection in source code based on abstract syntax tree. Technology audit and production reserves, 4(2 (72)), 33-36.
- Черноусов, А. В., Савченко, А. Ю., & Куб'юк, Є. Ю. Методи виявлення помилок безпеки в програмному забезпеченні на основі глибинного навчання, XVII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та

інформатики» (Україна, м. Київ, 25-26 квітня 2019 р.) : матеріали конференції. – Київ : КПІ ім. Ігоря Сікорського, 2019.

Наукова (науково-технічна) продукція: програмні продукти, програмно-технологічна документація

Соціально-економічна спрямованість: вдосконалення процесів розробки програмного забезпечення

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0123U101334

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Кисельов Геннадій Дмитрович
2. Hennadii D. Kyselov

Кваліфікація: к. т. н., ст.н.с., доцент, 05.13.12

Ідентифікатор ORCID ID: 0000-0003-2682-3593

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, буд. 37, Київ, 03056, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Бучик Сергій Степанович
2. Serhii S. Buchyk

Кваліфікація: д. т. н., професор, 21.05.01

Ідентифікатор ORCID ID: 0000-0003-0892-3494

Додаткова інформація:

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, буд. 60, Київ, 01033, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Радівілова Тамара Анатоліївна
2. Tamara A. Radivilova

Кваліфікація: д. т. н., професор, 05.13.21

Ідентифікатор ORCID ID: 0000-0001-5975-0269

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, буд. 14, Харків, Харківський р-н., 61166, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Шаповалова Світлана Ігорівна
2. Svitlana I. Shapovalova

Кваліфікація: к. т. н., доц., 05.13.12

Ідентифікатор ORCID ID: 0000-0002-3431-5639

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, буд. 37, Київ, 03056, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Глоба Лариса Сергіївна

2. Larisa S. Globa

Кваліфікація: д.т.н., професор, 05.13.12

Ідентифікатор ORCID ID: 0000-0003-3231-3012

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, буд. 37, Київ, 03056, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Корнага Ярослав Ігорович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Корнага Ярослав Ігорович
Відповідальний за підготовку облікових документів	Куб'юк Євгеній Юрійович
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна