Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0421U101749

Особливі позначки: відкрита

Дата реєстрації: 18-05-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Яковлев Віктор Михайлович
2. Yakovlev Viktor M.

Кваліфікація: 01.05.03

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 01.05.03

Назва наукової спеціальності: Математичне та програмне забезпечення обчислювальних машин і систем

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 23-04-2021

Спеціальність за освітою: математик

Місце роботи здобувача: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, буд. 40, м. Київ, 03187, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.194.02

Повне найменування юридичної особи: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, буд. 40, м. Київ, 03187, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

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

Повне найменування юридичної особи: Інститут кібернетики імені В. М. Глушкова Національної академії наук України

Код за ЄДРПОУ: 05417176

Місцезнаходження: проспект Академіка Глушкова, буд. 40, м. Київ, 03187, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 28.33.03

Тема дисертації:

1. Алгебраїчні методи виявлення вразливостей в бінарному коді

2. Algebraic Methods for Discovering of the Vulnerabilities in Binary Code

Реферат:

1. Досліджуються можливості підвищення ефективності застосування символьних методів у задачах кібербезпеки, зокрема, в задачі пошуку вразливостей у бінарному коді. Пропонується підхід, що грунтується на теорії інсерційного моделювання та алгебрі поведінок. Визначається семантика моделі програми та семантика мови програмування низького рівня на прикладі мови Ассемблера Intel x86. Розглядається формалізація поведінки моделі шляхом побудови системи поведінкових рівнянь, а також формалізація опису вразливостей коду у вигляді спеціальних шаблонів у термінах алгебри поведінок. Пропонується методика і технологія створення таких шаблонів. Представлено алгоритм приведення систем рівнянь алгебри поведінок до канонічної форми, доведено його коректність та складність. Цей алгоритм покладено в основу алгоритму алгебраїчного співставлення, доведено досяжність вразливості в моделі програми. Розроблено алгоритм лінійного алгебраїчного співставлення, який, у поєднанні з алгоритмами символьного

моделювання, значно підвищує ефективність пошуку вразливостей у бінарному коді за рахунок звуження простору пошуку і обмеження його «підозрілими» поведінками. Доведено, що цей алгоритм має лінійну складність. Показано процедуру отримання визиску (екстлойту) на основі отриманих поведінок і умов, що ведуть до вразливості. Представлено реалізацію алгоритму алгебраїчного співставлення у прототипі програмної системи пошуку вразливостей. Розглянуто шляхи можливого застосування представленої технології для пошуку нештатних входів у програмах (бекдорів).

2. Considered possibilities of increasing of effectiveness of application of the symbolic methods in the cybersecurity tasks, in particular, the tasks of discovering of the vulnerabilities in the binary code. The “traditional” methods of identifying the code vulnerabilities are insufficient. At the same time, the implementation of the symbolic methods is restricted, as these methods require exhaustive amount of computer resources, and, generally, very slow. To reduce this disadvantage, the hybrid methods and technologies are being developed. These methods implement vulnerabilities detection in several steps, where the symbolic modeling is used after some steps, which are based on another approaches, such as fuzzing, code instrumentation, neural networks etc. In this work, the approach based on the theory of insertion modelling and the behavior algebra is proposed. As a theoretical background, determined the semantics for the program model, and the semantics of low-level Assembler Intel x86 language. Considered the formalization of the model behavior by means of building of the system of behavioral equations, also the formalization of the code vulnerabilities in the form of special patterns in terms of behavior algebra. Proposed the methodology and technology of creation of such patterns. Represented the algorithm of bringing of an equation system in the terms of behavior algebra to the canonical form, is the basis of the algorithm of algebraic matching, proven its correctness and complexity. Also proven the vulnerability reachability in the program model, where a vulnerability is represented as a behavioral pattern. Developed the linear algebraic matching algorithm, which, in conjunction with the symbolic modeling algorithms, significantly increases the effectiveness of the vulnerabilities discovering in the binary code due to the restriction of the search space by the “suspected” behaviors. Proven the linear complexity of this algorithm. Represented the procedure of creating the exploit on the basis of the behaviors obtained from the algebraic matching, and the conditions that leads to a vulnerability. Represented the implementation of the linear algebraic matching algorithm in the prototype of the system for the vulnerabilities discovering. The system performs the binary code analysis in 4 steps: disassembling, translation of assembly code to the behavior algebra, algebraic matching, and symbolic modeling, which proves the reachability of the traces obtained on the matching step. Considered the ways of possible application of the technologies based on the algebraic approach for the discovering of the program backdoors.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Летичевський Олександр Олександрович

2. Letychevskyi Oleksandr O.

Кваліфікація: д. ф.-м. н., 01.05.03

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Шишацька Олена Володимирівна

2. Shyshatska Olena V.

Кваліфікація: к. ф.-м. н., 01.05.03

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Дорошенко Анатолій Юхимович

2. Doroshenko Anatolii Yu.

Кваліфікація: д. ф.-м. н., 01.05.03

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Сергієнко Іван Васильович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Сергієнко Іван Васильович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.