Голові разової спеціалізованої
вченої ради PhD 9279
Хмельницького національного
університету
доктору технічних наук, професору
Тетяні ГОВОРУЩЕНКО

РЕЦЕНЗІЯ

на дисертаційне дослідження Регіди Павла Геннадійовича
за темою «Методи та засоби організації розподілених систем виявлення інфікованих виконуваних програм, стійких до емуляції в середовищі виконання», подане на здобуття ступеня доктора філософії
з галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

1. Актуальність теми дослідження та її зв'язок із планами наукових робіт університету.

Сучасний розвиток інформаційних технологій веде до широкого впровадження технологій, що сприяє автоматизації процесів, через використання програмних застосунків. Беручи цей факт до уваги, зловмисники використовують ці застосунки для інфікування, формуючи таким чином інфіковані програми (ІП).

ІП часто набуваються поліморфних властивостей, що призводить до зміни поведінки виконання, що у свою чергу веде до зниження ймовірності виявлення. Тому актуальним є створення засобів динамічного аналізу поведінки програм для виявлення зловмисної поведінки в ІП. А при реалізації таких засобів, важливим значенням набувають технології емуляції та пісочниці, які забезпечують контрольоване ізольоване середовище для запуску потенційно небезпечних програм. Однак, зважаючи на зростаючу складність виявлення сучасних ІП та особливостей їх виконання та аналізу із використанням емуляції, доцільним завданням є використання розподіленої системи, яка забезпечить необхідну кількість обчислювальних ресурсів.

Таким чином, актуальною науково-прикладною проблемою є вдосконалення методів і засобів функціонування розподілених систем, для

підвищення ефективності виявлення зловмисної поведінки ІП на основі аналізу їхньої поведінки в ізольованих модифікованих середовищах виконання.

Дослідження, результати яких наведено в дисертації, проведені у рамках науково-дослідної тематики Хмельницького національного університету: держбюджетної науково-дослідної теми №1Б-2021 «Самоорганізована розподілена система виявлення зловмисного програмного забезпечення в комп'ютерних мережах» (ДР 0121U109936); держбюджетної науково-дослідної теми №2Б-2024 «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (ДР 0124U000980), в яких автор дисертації був виконавцем.

2. Формулювання наукової задачі та мети й задач дослідження

Здобувач правильно визначив об'єкт і предмет дослідження. Так, об'єктом дослідження визначено процес організації розподіленої системи для виявлення зловмисної поведінки в ІП, які використовують методи уникнення виявлення. Предметом дослідження встановлено методи організації розподілених систем із обчислювальними елементами, що мають рівень автономії для виявлення зловмисного прояву в інфікованих програмах. Мету дисертаційної роботи визначено, як покращення ефективності функціонування грід-обчислювальних систем із автономними обчислювальними елементами для виявлення зловмисної передачі управління головним потокам в ІП, що базується на концепції динамічного стану емулювання середовища відтворення програмних засобів.

Поставлену мету досягнуто в результаті розв'язання таких задач:

1) провести аналіз методів організації та функціонування грід-обчислювальних систем, дослідити методи оцінювання ефективності залучення обчислювальних елементів із рівнем автономії та їх безпечного і коректного функціонування для організації виявлення інфікованих програм;

2) розробити формальний опис та моделі інфікованих програм, що використовують методи уникнення виявлення, а саме ідентифікацію/визначення емульованого середовища виконання та обфускацію коду виконання, що дозволить відтворити їх поведінку для опису їх впливу на цільову систему користувача;

3) розробити та представити формальний опис функціонування і модель грід-обчислювальних систем із використанням автономних обчислювальних елементів, що повинна враховуватись при організації

захищеного та правильного (коректного) виявлення зловмисної поведінки в інфікованих програмах;

4) розробити метод синтезу засобів формування шаблонів поведінки інфікованих програм, які використовують методи уникнення виявлення, що залучають базові пісочницю та емулятор використовуючи множини станів емульованих центральних процесорів для виявлення зловмисної поведінки;

5) удосконалити метод організації грід-обчислювальних систем для оптимального розподілу завдань між залученими автономними гетерогенними обчислювальними елементами для виявлення зловмисної поведінки в інфікованих програмах;

6) удосконалити метод оцінювання довіри автономних обчислювальних елементів для оптимізації використання обчислювальних ресурів шляхом скорочення кількості повторних обчислень в грід-обчислювальних системах;

7) розробити грід-обчислювальну систему виявлення інфікованих програм, які використовують методи уникнення виявлення, для експериментального дослідження з метою покращення її характеристик та її подальшого впровадження для практичного застосування.

3. Наукова новизна одержаних автором результатів полягає в наступному:

1) вперше розроблено модель грід-обчислювальних систем, в якій враховано вимоги до залучення автономних та гетерогенних обчислювальних елементів для забезпечення виконання задач із перевіркою на коректність в динамічному середовищі виконання, і яка дає змогу залучити під'єднані обчислювальні елементи для аналізу поведінки виконання інфікованих програм, забезпечуючи розподілений процес виявлення зловмисного прояву в інфікованих програмах;

2) розроблено новий метод синтезу засобів формування шаблонів поведінки інфікованих програм, який на відміну від відомих відрізняється залученням пісочниці для їх виконання у наборі створюваних модифікованих ізольованих середовищах за допомогою виконання програмних переривань та базового емулятора із визначеним набором реалізованих низькорівневих інструкцій, що дає змогу отримувати з них шаблони поведінки на множинах станів емульованих центральних процесорів з метою виявлення зловмисної поведінки з урахуванням

особливостей методів уникнення від виявлення, які реалізовані зловмисниками;

3) удосконалено метод організації функціонування грід-обчислювальних систем, який на відміну від відомих залучає жадібний алгоритм для оптимізації навантаження між автономними гетерогенними обчислювальними елементами та використовує додаткову чергу активних задач, що дає змогу забезпечити збалансоване виконання поставлених задач в розподілених системах із динамічно змінюваною топологією для розподіленого виявлення зловмисної поведінки в інфікованих програмах;

4) удосконалено метод оцінювання довіри автономних обчислювальних елементів, який на відміну від відомих використовує механізми призначення ролей із використанням елементів нечіткої логіки, що дає змогу оптимізувати використання обчислювальних ресурсів шляхом скорочення кількості повторних обчислень у системах, що функціонують в динамічному середовищі.

4. Аналіз основного змісту дисертації

У вступі обґрунтовано актуальність задачі підвищення ефективності виявлення інфікованих програм, що використовують методи уникнення виявлення. Визначено перспективність грід-обчислювальних систем та засобів аналізу, що використовують пісочниці та емуляцію. Представлено зв'язок теми з науковими дослідженнями, результати роботи та приклади впровадження.

У першому розділі здійснено огляд предметної області дослідження, розглянуто наявні комерційні програмні засоби та системи, призначені для виявлення зловмисного програмного забезпечення, а також проаналізовано підходи та методи, що використовуються з цією метою. Окрему увагу приділено аналізу існуючих розподілених обчислювальних систем, їх архітектурі, принципам побудови та характерним особливостям функціонування.

У другому розділі подано особливості виконання інфікованих програм та представлено їх модель, що враховує виявлення емуляції, обфускацію та стратегії виконання. Описано архітектури засобу формування поведінки та центрального серверу, що забезпечує розподілений аналіз. Обидві архітектури подано через їхні компоненти й функції із використанням алгебраїчної структури.

У третьому розділі запропоновано метод формування шаблонів поведінки інфікованих програм шляхом виконання в модифікованих ізольованих середовищах із використанням базового емулятора та програмних переривань для виявлення зловмисної поведінки. Розглянуті удосконалені методи розподілу навантаження між активними обчислювальними елементами системи та метод оцінювання довіри до них на основі рольової моделі та нечіткої логіки.

У четвертому розділі наведено опис реалізованих компонентів програмних частин центрального серверу та обчислювального елемента, зокрема використаних бібліотек і особливостей їх розробки, що забезпечують функціонування розподіленої системи. Розглянутий мережевий протокол обміну повідомленнями та наведено результати експериментів з аналізом ефективності системи.

У висновках подано здобуті теоретичні та практичні результати досліджень.

Додатки містять наукові статті, що відображають результати роботи, акти про впровадження, а також лістинг коду розробленого програмного забезпечення.

5. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій.

Наукові висновки та рекомендації, подані в дисертації, ґрунтуються на правильному використанні методів функціонування грід-обчислювальних систем та методів синтезу засобів формування поведінки виконання інфікованих програм. Достовірність одержаних результатів підтверджена їх апробацією на міжнародних та всеукраїнських наукових конференціях, а також практичним впровадженням.

6. Практичне значення отриманих результатів

За результатами виконаних досліджень здобувачем розроблено методи та засоби підвищення ефективності функціонування грід-обчислювальних систем виявлення інфікованих програм за рахунок синтезу засобів для формування поведінки виконання інфікованих програм в модифікованих ізольованих середовищах.

Розроблено централізовану розподілену систему виявлення зловмисного програмного забезпечення, що залучає обчислювальні елементи враховуючи їх автономність та гетерогенність. Система

використовує залучені обчислювальні елементи для розгортання засобів формування поведінки виконання інфікованої програми в модифікованих ізольованих середовищах, тим самим забезпечуючи розподілене виявлення зловмисної поведінки в інфікованих програмах. Реалізований метод виявлення зловмисної поведінки в ІП демонструє успішність в більшості випадків 98-99%, при виконанні аналізу згенерованих сімейств моделей ІП на основі досліджених технік протидії емуляції.

Експериментальні дослідження підтвердили коректність функціонування централізованої грід-обчислювальної системи для виявлення зловмисної поведінки.

Теоретичні та практичні результати дослідження впроваджені в ТОВ «Nolt technologies» (м. Хмельницький), ТОВ «ІТТ» (м. Хмельницький), а також, в освітньому процесі Хмельницького національного університет при викладанні дисциплін на кафедрі комп'ютерної інженерії та інформаційних систем для спеціальності 123 Комп'ютерна інженерія, зокрема в курсах «Теорія і проєктування комп'ютерних та кіберфізичних систем і мереж», «Безпека та захист комп'ютерних систем», «Комп'ютерні мережі, системне адміністрування та кібербезпека».

7. Особистий внесок здобувача полягає в розробленні методів та засобів організації централізованих грід-обчислювальних систем для виявлення зловмисної поведінки в інфікованих програмах. Усі основні наукові та прикладні результати дисертаційної роботи отримані здобувачем самостійно. За результатами проведених досліджень основні наукові результати опубліковано у 4 наукових статтях у фахових наукових журналах України. Апробація засвідчена публікаціями 6 праць в матеріалах міжнародних та всеукраїнських конференцій, з яких чотири праці індексовані у наукометричній базі Scopus. Опубліковано 1 свідоцтво про реєстрацію авторського права на твір (програму).

8. Структура та обсяг дисертації.

Дисертаційна робота складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та чотирьох додатків. Повний обсяг роботи містить 190 сторінок друкованого тексту, з них анотація – на 10 стор., зміст – на 2 стор., перелік умовних скорочень – на 1 стор., основний текст – на 129 стор., список із 131

використаних джерел – на 17 стор., додатки – на 28 стор. Дисертація містить 27 рисунків та 10 таблиць.

9. Зауваження

1. У першому розділі дисертаційної роботи не було зроблено акценту саме на ті системи, які використовують концепцію розподілених обчислень як засіб виявлення зловмисного програмного забезпечення.

2.В роботі рисунок 2.1 який визначений як «Модель інфікованої програми» окрім самих складових частин інфікованої програми також визначає вплив визначеної моделі на операційну систему та її складові частини. Тому вказана назва рисунку не відповідає поданому зображенню.

3. Запропонований алгоритм розподілу задач базується на визначеному коефіцієнту складності виконання кожної інфікованої програми для оптимального розподілу навантаження на обчислювальні елементи. Для такої оцінки здобувач пропонує використовувати довірений обчислювальний елемент, але в явному вигляді такий елемент не фігурує на рисунку системи, а сама оцінка явно не представлена як крок запропонованого методу функціонування.

4. В роботі запропоновано використовувати рольову модель для визначення довіри кожного обчислювального елементу, але на рисунку 4.5, який демонструє налаштування розподілених обчислень в контексті рейтингу довіри, визначено параметр «Допустимий рівень», тому не зовсім ясно як це значення відноситься до запропонованих ролей, та як за допомогою представленого інтерфейсу адміністратор може керувати запропонованими рівнями довіри.

5. До одного з представлених експериментів в розділі 4 було додано 2 таблиці (Таблиця 4.5 та 4.6) із результатами аналізу поведінки виконання моделей інфікованих програм в модифікованих середовищах виконання. Ймовірно, таблиці демонструють результати проміжного аналізу визначених у формулою 3.13. Так як запропонований метод ґрунтується на результатах обох таблиць для визначення наявності зловмисної поведінки, здобувачу варто було б об’єднати таблиці в одну, та подати її в розширеному вигляді в додатках.

6. У дисертаційній роботі часто використовуються терміни «підзадачі» та «підзавдання», здобувачу варто було б узгодити термінологію з цього приводу. Окрім цього, зустрічаються деякі граматичні та стилістичні помилки, зокрема на сторінках 64, 66, 85, 104.

Однак зазначені зауваження не є принциповими, істотно не впливають на зміст дисертаційної роботи та не знижують її наукової та практичної цінності.

10. Загальний висновок.

Отже, дисертаційна робота Регіди Павла Геннадійовича за темою «Методи та засоби організації розподілених систем виявлення інфікованих виконуваних програм, стійких до емуляції в середовищі виконання» є завершеною науковою кваліфікаційною працею, яка містить новий та актуальний науково-прикладний внесок. Усі результати, які виносяться на захист, є достовірними та отримані автором особисто.

Тому, з огляду на вище вказане, вважаю, що дисертаційна робота «Методи та засоби організації розподілених систем виявлення інфікованих виконуваних програм, стійких до емуляції в середовищі виконання», яка подана на здобуття ступеня доктора філософії, за своїм науковим рівнем та практичною цінністю, змістом та оформленням повністю відповідає вимогам пп. 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (зі змінами, внесеними згідно з Постановами Кабінету Міністрів України № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024), а її автор, Регіда Павло Геннадійович, заслуговує на присудження ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Рецензент:
д.т.н., професор
професор кафедри комп'ютерної інженерії
та інформаційних систем
Хмельницького національного університету Сергій ЛИСЕНКО

«Підпис Сергія ЛИСЕНКА засвідчую»:
Проректор з наукової роботи
Хмельницького національного університету Олег СИНЮК