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

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

Використання розподілених обчислювальних систем є невід'ємною складовою сучасної наукової та прикладної діяльності. Завдяки цьому спостерігається інтенсивний розвиток методів їх розробки та організації, що сприяло формуванню низки підходів до реалізації таких систем. Різноманітність підходів забезпечує можливість створення різних типів розподілених систем з урахуванням особливостей обчислювальних елементів, способів їх підключення та взаємодії, а також специфіки поставлених перед ними завдань.

Проблеми у сфері кібербезпеки характеризуються постійним зростанням кількості зразків зловмисного програмного забезпечення та різноманітністю способів їх проникнення. Численні звіти провідних наукових лабораторій фіксують інтенсивне зростання як кількісних, так і якісних показників усіх типів сучасного зловмисного програмного забезпечення. Одним із поширених способів розповсюдження подібних загроз є інфікування відомого програмного забезпечення. Крім того, розробники таких інфікованих програм додають методи уникнення виявлення, враховуючи широке використання антивірусних програмних засобів на кінцевих пристроях користувачів. Інфіковані програми (ІП),

таким чином набувають поліморфних властивостей, що суттєво ускладнює процес їх виявлення, що обумовлює необхідність проведення їх детального аналізу та розробки ефективних методів протидії загрозам.

У дисертації запропоновано використовувати розподілені системи для проведення аналізу інфікованих програм. Зважаючи на окреслені проблеми, пов'язані із стійким зростанням кількості нових зразків інфікованих програм, а також представлений метод, що ґрунтується на використанні множини модифікованих ізольованих середовищ як пасток для аналізу, застосування розподілених обчислювальних систем є обґрунтованим рішенням. Загалом, обраний напрям досліджень є актуальною науково-прикладною задачею.

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.

Формулювання наукової задачі, мети й задачі дослідження.

Здобувачем правильно визначено об'єкт і предмет дослідження, відповідно до висунутої заздалегідь гіпотези 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 досягнено 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.

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.

Короткий аналіз основного змісту дисертації

У вступі автором обґрунтовано актуальність теми, визначено мету, основні завдання, предмет та об'єкт дослідження, наведено наукову новзину, практичне значення одержаних результатів.

У першому розділі проаналізовано предметну область, комерційні рішення та методи виявлення зловмисного програмного забезпечення. Також розглянуто існуючі розподілені обчислювальні системи, їх організацію та функціонування.

У другому розділі подано основні властивості інфікованих програм та їх функціонування. Представлено модель, що враховує методи протидії емуляції, обфускації та стратегії виконання. Описано архітектури ключових компонентів розподіленої системи виявлення інфікованих програм, а саме: засобів виконання та аналізу програм та програмної частини центрального

сервера. Обидві архітектури деталізовані з погляду їхніх складових і функціоналу для забезпечення розподіленого аналізу інфікованих програм.

У третьому розділі представлено новий метод синтезу шаблонів поведінки інфікованих програм. Він базується на використанні пісочниці та виконанні програмних переривань для формування поведінки виконання програми в модифікованому ізольованому середовищі виконання. Також удосконалено метод організації обчислень у грід-обчислювальних системах та метод оцінювання довіри обчислювальних елементів.

У четвертому розділі описано розроблені програмні компоненти центрального сервера та обчислювального елемента, деталі їхньої реалізації та використані бібліотеки, що забезпечують функціонування розподіленої системи. Представлено мережевий протокол обміну інформації між основними елементами системи. Представлено проведені експерименти, оцінку ефективності та аналіз отриманих результатів розподіленої системи.

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.

Практичне значення одержаних результатів. Розроблена централізована грід-обчислювальна система забезпечує виконання та аналіз інфікованих програм, гарантуючи стабільність роботи у розподіленому середовищі за участі автономних і гетерогенних обчислювальних елементів. Це, своєю чергою, дозволяє виявляти інфіковані програми, які використовують методи уникнення виявлення. Особливістю запропонованої системи є синтез засобів виконання інфікованих програм та формування їх поведінки виконання, які розгортаються безпосередньо на підключених обчислювальних елементах. Удосконалені методи організації функціонування цієї системи забезпечують оптимальне використання доступних обчислювальних ресурсів і зменшення кількості повторних перевірок, що є критично важливим з огляду на динамічність середовища її

функціонування. Загалом, система продемонструвала ефективність на рівні 98-99% при виявленні згенерованих моделей інфікованих програм.

У результаті проведених експериментальних досліджень з розробленою системою було підтверджене коректне функціонування централізованої грід-обчислювальної системи, та її здатність до виявлення інфікованих програм, що використовують методи уникнення від виявлення.

Особистий внесок здобувача полягає в розробленні методів та засобів організації функціонування грід-обчислювальних систем виявлення інфікованих програм, що забезпечують розв'язання поставлених у дисертації задач. 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 4 праці проіндексовані у наукометричній базі Scopus. Опубліковано 1 свідоцтво про реєстрацію авторського права на твір (програму).

Апробація метеріалів дисертації. Апробацію основних положень, ідей, висновків дисертаційної роботи проведено на науковому семінарі кафедри комп'ютерної інженерії та інформаційних систем у Хмельницькому національному університеті. Наукові результати роботи доповідались на таких конференціях: XX ювілейна міжнародна науково-практична конференція «Математичне та програмне забезпечення інтелектуальних систем» (МПЗІС-2022, Дніпро, Україна, 23-25 листопада 2022); 4th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS, Khmelnytskyi, Ukraine, March 22–24, 2023); 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS, Dortmund, Germany, 7–9 September 2023); 13th International Conference on Dependable Systems, Services and Technologies (DESSERT, Athens, Greece, 13–15 October 2023); 5th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS, Khmelnytskyi, Ukraine, March 28, 2024); The 13th International Scientific Conference («ITSec», м. Львів, Україна Травень 9-11, 2024).

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.

Зауваження.

У результаті розгляду дисертації сформовано наступні зауваження та рекомендації.

1. У роботі недостатньо уваги приділено саме грід-системам як окремому типу розподілених обчислювальних систем.

2. В запропонованому методі організації обчислень варто було б врахувати транспортні часові витрати на передачу завдання від центрального сервера до обчислювального елементу, враховуючи тип розподіленої системи запропонований для вирішення поставленої задачі.

3. В експериментах, які визначають ефективність функціонування розробленої розподіленої обчислювальної системи у порівнянні із іншими подібними системами не було проведено порівняння саме ефективності виявлення інфікованих програм.

4. У запропонованому методі оцінювання довіри здобувач використовує вагові коефіцієнти для двох наборів параметрів, що характеризують поведінкові особливості обчислювальних елементів. Однак не уточнюється методика визначення цих коефіцієнтів

5. На сторінці 17 визначено поведінку зловмисного програмного забезпечення як «аномальна(зловмисна?)» і потребує уточнення. Також, на сторінці 74 в реченні про стратегію виконання використано слово «очікуванні» два рази. Окрім цього, в роботі присутні деякі орфографічні та стилістичні помилки, а саме на сторінках 66, 93, 94.

Втім, зазначені зауваження суттєво не впливають на загальний, доволі високий, рівень проведеного дослідження.

Загальний висновок.

Вважаю, що дисертаційна робота Регіди Павла Геннадійовича за темою «Методи та засоби організації розподілених систем виявлення інфікованих

виконуваних програм, стійких до емуляції в середовищі виконання» містить нові науково обґрунтовані теоретичні та експериментальні результати в галузі 12 Інформаційні технології, які в сукупності забезпечують розв'язання актуальної науково-прикладної задачі розроблення методів для покращення ефективності функціонування централізованих грід-обчислювальних систем із залученням автономних та гетерогенних обчислювальних елементів для виявлення інфікованих програм які використовують методи уникнення виявлення, за рахунок синтезу засобів формування поведінки виконання інфікованих програм в модифікованих ізольованих середовищах.

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:
к.т.н., доцент
завідувач кафедри кібербезпеки
Хмельницького національного університету Юрій КЛЬОЦ

«Підпис Юрія КЛЬОЦА засвідчую»:
Проректор з наукової роботи
Хмельницького національного університету Олег СИНЮК