08.08.2023

ВІДГУК

офіційного опонента – завідувача кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, д.т.н., професора Смірнова Олексія Анатолійовича

на дисертаційну роботу

Василишина Святослава Ігоровича

«Розробка методу використання програмних приманок як елементів захисту комп'ютерних мереж на основі технології Blockchain»,

поданої на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації» (галузь знань 12 «Інформаційні технології»)

1. Актуальність теми дисертаційної роботи

Мережеві системи містять цінні дані та ресурси, які необхідно захищати від зловмисників, а тому інтерес до безпеки та захисту інформації для мережевих системах постійно зростає. Експерти з безпеки часто використовують honeypots і honeynet для захисту мережевих систем. Програмна приманка – це технологія, яку експерти з безпеки використовують для виявлення нових методів злому від зловмисників і зловмисників. Приманки, як правило, є віртуальними машинами, призначеними для емуляції реальних машин, дії або створення вигляду запущених повноцінних служб і програм з відкритими портами, які можна знайти на типовій системі або сервері в мережі. Як проактивний захисний механізм, honeypot стає незамінним інструментом для забезпечення безпеки мережі в таких широких додатках, як Інтернет речей (IoT), бездротові сенсорні мережі (WSN), транспортні мережі тощо.

Однак через фіксовану конфігурацію та реакцію програмні приманки схильні бути виявлені зловмисниками, які в подальшому уникають такі надто очевидні пастки та розпочинають атаку на реальну систему в мережі. Не зважаючи на велику кількість досліджень у цій сфері досі залишаються невирішені проблеми, такі як: централізована система управління безпеки, обчислювальні потужності актуальних захисних систем, людський фактор. Насамперед, для вирішення цієї проблеми потрібно впровадити нові підходи для користування даною технологією, наприклад децентралізація управління, виключення людського фактору, тощо.

Технологія Blockchain володіє динамічними атрибутами, які у зв'язці з програмними приманками могли б нівелювати недоліки перших. Для цього важливо розробити та дослідити ефективність симбіозу даних технологій на прикладах зовнішніх мережевих атак.

Актуальність дисертаційної роботи Василишина Святослава Ігоровича обумовлена необхідністю побудови комп'ютерної мережі на основі технології

Blockchain, яка використовує розроблений метод використання програмних приманок як елементів захисту комп'ютерних мереж.

2. Зв'язок теми дисертації з державними програмами, науковими напрямами університету та кафедри

Наведені в дисертаційній роботі основні результати та рекомендації розроблено в межах держбюджетної науково-дослідної роботи «Розроблення та удосконалення методів та засобів захисту інформації для протидії несанкціонованому доступу в інформаційно-комунікаційних мережах» (№ державної реєстрації 0119U101690; терміни виконання - 2019-2022 рр.);

3. Наукова новизна одержаних результатів

- **Вперше** розроблена модель динамічної системи активних програмних приманок, що використовують Blockchain технологію. Ця модель в порівнянні з існуючими інтегрує децентралізовані та автоматично оновлювані атрибути пасток, що підвищює ефективність захисту мережі шляхом зменшення навантаження на мережеву інфраструктуру та часу відгуку сервісів у разі атаки.
- **Вперше,** на основі розробленої моделі динамічної системи програмних (активних) приманок, яка використовує Blockchain-технологію, за рахунок плаваючих хостів в мережі та математичного апарату обчислення динамічних атрибутів програмних приманок, розроблено метод використання програмних приманок як елементів захисту комп'ютерних мереж на основі технології Blockchain. Цей метод, на відміну від відомих, унеможливлює здійснення успішної сніфер атаки за рахунок шифрування, захищає від атаки сканування за рахунок динамічного відкривання та закривання портів, підвищує ефективність захищеності від DDoS атак та зберігає інформацію про атаки на систему на Blockchain-платформі, що забезпечує високий рівень збереження даних та гарантує їхню незмінність.
- **Набув подальшого розвитку** математичний опис обчислення динамічних атрибутів програмних приманок, який, на відміну від відомих враховує динамічні та транс локаційні можливості блокчейн-технології Solana. Це дало змогу змоделювати та оптимізувати розподіл ресурсів мережі за рахунок адаптації до змінних умов, що в результаті сприяло підвищенню ефективності захисту, зокрема забезпеченню швидкого відгуку сервісів під час зовнішніх атак.

4. Практичне значення одержаних результатів

Практичне значення результатів дисертаційного дослідження полягає у можливості їх безпосереднього застосування для підсилення наявних систем активного та пасивного захисту в корпоративних та державних підприємствах, що дозволяє:

1. В залежності від різних ситуацій моделювання до 54% підвищити пропускну здатність каналу та до 204% підвищити швидкість передачі даних під час проведення зовнішніх атак на систему в порівнянні з статичними аналогами;

2. Покращити час відгуку сервісів під час атаки типу DDoS на статичні хости, в межах таких значень – MSQL до 34%, NGNIX до 16%, APACHE до 1%, vsFTPd до 13%;

3. Підвищити ефективність захищеності каналів передачі даних в комп'ютерній мережі за рахунок впровадження розробленого методу динамічної системи активних пасток на основі програмних приманок побудованих на технології Blockchain з RSA 2048 - бітовим алгоритмом шифрування;

4. Підвищити загальну адаптивність мережі реагувати на зовнішні атаки, оскільки розроблений алгоритм, на відміну від відомих дозволяє системі реагувати на атаки типу сканування та закривати порти доступу реагуючи на зловмисні дії.

Результати дисертаційної роботи впроваджено у технологічні процеси ТОВ «Н-ІКС СПЕЙС» (м.Львів) та в навчальному процесі НУ "Львівська політехніка".

5. Мова та стиль викладення дисертації дозволяє зрозуміти суть розроблених наукових положень та одержаних практичних результатів. Дисертація відповідає вимогам, які висуваються до її оформлення відповідно до "Порядку присудження наукових ступенів" затвердженого Постановою Кабінету Міністрів України від 24.07.2013 р. №567 (зі змінами) та суттєво не відхиляються від вимог ДСТУ 3008-2015 "Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлення" й "Вимог до оформлення дисертації" затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. №40. У цілому зміст дисертації викладено послідовно та логічно.

6. Ступінь обґрунтованості наукових положень дисертації і їх достовірність та новизна.

Наведені в дисертації результати базуються на кваліфікованому підході до постановки завдань досліджень, логічно правильному обґрунтуванню прийнятих припущень під час вибору математичних моделей і коректному використанні математичного апарату. Крім того, достовірність підтверджується результатами комп'ютерного моделювання і практичною реалізацією системи динамічних програмних приманок, а також збіжністю з результатами експериментальної верифікації.

7. Повнота оприлюднення результатів дисертаційної роботи.

Основні результати дисертаційної роботи Василишина С.І. достатньо повно відображені у 19 наукових публікаціях, з яких 7 статей у наукових фахових виданнях України, 4 статті у наукових виданнях інших держав, які входять до міжнародної наукометричної бази (Scopus), та 8 матеріалів конференцій.

Перераховані публікації з достатньою повнотою відбивають наукові та практичні результати дисертації. З праць, що їх опубліковано у співавторстві, у дисертації використані лише ті результати, які отримано здобувачем самостійно.

8. Загальна характеристика структури та змісту дисертаційної роботи.

Дисертаційна робота викладена на 191 сторінках та складається з анотації, змісту, переліку скорочень, вступу, чотирьох основних розділів, в яких міститься 39 рисунків та 11 таблиць, списку використаних джерел з 101 найменування, а також 3 додатки. За структурою, мовою та стилем викладення дисертація відповідає вимогам МОН України. Робота написана грамотною українською мовою з використанням сучасної наукової термінології, а стиль викладення матеріалу є послідовним та логічним.

У вступі зазначено актуальність теми дисертації, сформульовано мету і задачі досліджень, заявлено наукову новизну та практичне значення отриманих результатів, представлено зв'язок роботи з науковими програмами, планами і темами, особистий внесок здобувача, перелік публікацій і апробації результатів.

Перший розділ присвячено вивченню досліджень та публікацій, що стосуються актуальної тематики Blockchain та програмних приманок. У цьому розділі проводиться детальний огляд технології програмних приманок, розглядаються їх потенційні можливості, значні переваги, неминучі недоліки, різні рівні взаємодій між компонентами, особливості внутрішнього дизайну та відповідні перешкоди, які можуть виникнути під час їх розгортання. Також у даному розділі звертається увага на актуальні проблеми, пов'язані з використанням приманок та обманок у контексті захисту даних у комп'ютерних мережах.

В другому розділі дисертації досліджуються можливості застосування Blockchain для захисту даних в різних кібер-областях, зокрема на об'єктах інфраструктури. Розглядаються сфери впливу, в яких дана технологія може розповсюджуватись, та як вона потенційно може використовуватись на об'єктах інфраструктури. Вивчаються можливості використання технології Blockchain в таких актуальних структурах, як урядові та військові організації, а також перспективи та можливості в комбінуванні з штучним інтелектом, великими даними та іншими передовими технологіями.

В третьому розділі дисертації акцентується увага на методі, моделюванні та архітектурі динамічної системи, яка використовує програмні приманки та динамічні властивості Blockchain. У цьому розділі детально вивчається динамічна розподілена система управління, яка використовує динамічні властивості Blockchain та представляється розроблений метод використанні цієї системи.

В четвертому розділі проводиться дослідження стійкості розробленої системи до різних видів атак, експериментальний аналіз рівня безпеки та оцінка ефективності системи в порівнянні з існуючими рішеннями. Досліджено рівень безпеки системи та рішення щодо її захисту від трьох видів атак: атак сканування, сніфер та DDoS.

Загальні висновки дисертаційної роботи узгоджуються з метою і завданнями дослідження. За результатами дисертаційного дослідження зроблено вісім висновків, які повністю відповідають поставленим завданням. Отримані результати характеризуються науковою новизною та практичною цінністю, обгрунтовані теоретично та підтверджені експериментальними дослідженнями. В цілому дисертація Василишина Святослава Ігоровича є завершеним і повним дослідженням, яке містить розробки та відповідні їм експериментальні перевірки.

9. Зауваження до дисертаційної роботи.

1. У першому розділі автор приділяє більшу увагу огляду сучасних типів програмних приманок, проведенню аналізу технології використання програмних приманок, дослідженню їх сильних та слабких сторін та проводить поверхневий аналіз можливостей технології Blockchain для кібербезпеки та захисту інформації. Глибший аналіз технології Blockchain для кібербезпеки та захисту інформації дозволив би підвищити рівень довіри до його практичного застосування у цій сфері.

2. У другому розділі дисертації в п.2.4. автором наводяться перспективи військового застосування технології Blockchain, однак не до кінця зрозуміло, яким чином розроблений метод використання даної технології вирішує виявлені проблеми та впливає запропоновані рішення цього розділу.

3. У третьому розділі на рис. 3.4, сторінка 113, автором відображено порівняння станів основного хосту в різний період розподілу сервісів. Проте з рисунка не зрозуміло яким чином здійснюється трансформація та переміщення сервісів та служб, що має спантеличувати зловмисників та захищати розроблену систему. Автору варто було б надати додаткові пояснення та контекст трансформації та зазначити, які саме динамічні атрибути Blockchain впливають на стан хосту в різні моменти часу.

4. На сторінках 140 та 141, представлено рисунки 4.13 та 4.14, які демонструють порівняння захищеності прототипу побудованої комп'ютерної мережі з іншими аналогами, проте таке представлення потребує більш детального пояснення та підписів. Додаткові коментарі до цих рисунків покращили б інтерпретацію отриманих результатів порівняння та підкреслили вагомість висновків щодо ефективності розробленого методу.

5. У дисертаційні роботі для перевірки розробленого методу експериментально розглядаються три види атак на мережу, однак, варто було б включити також й інші сучасні атаки, що дозволило б ґрунтовніше оцінити захисні можливості мережі, яка використовує розроблений метод використання програмних приманок. Доцільно також було розглянути можливі методи атак та їхні наслідки для системи.

6. У дисертаційній роботі були помічені окремі описки, неточності формулювань та варіації термінології. Важливо забезпечити послідовність та

точність використовуваної термінології, а також перевірити роботу на граматичні та стилістичні помилки.

Слід відзначити, що визначені зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

Загальний висновок на дисертаційну роботу.

На основі критичного вивчення дисертації та праць здобувача, які опубліковані за темою дисертації об'єктивно встановлено:

1. Дисертаційна робота Василишина Святослава Ігоровича відповідає чинним вимогам пп. 6,7,8,9, які встановлені у "Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії", який затверджений Постановою Кабінету Міністрів України від 12.01.2022 р. №44;

2. Використання чужих наукових результатів без посилань на авторів у дисертації не виявлено, що свідчить про особистий внесок здобувача в науку;

3. Дисертаційна робота Василишина С.І. є завершеною науковою працею, в якій отримані нові науково обґрунтовані результати, які дозволяють підвищити ефективність захисту комп'ютерних мереж та покращити стійкість захисної системи без втрати швидкодії мережевої інфраструктури за рахунок розробки системи приманок на основі динамічних атрибутів технології Blockchain, а її автор, Василишин Святослав Ігорович, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 "Кібербезпека та захист інформації".

Офіційний опонент
Завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
доктор технічних наук, професор Олексій СМІРНОВ

Підпис професора Смірнова О.А. засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного університету,
доктор економічних наук, професор Олександр ЛЕВЧЕНКО
"08" серпня 2023 року