ВІДГУК

рецензента – доцента кафедри захисту інформації,
Національного університету "Львівська політехніка",
к.т.н., доцента Гарасимчука Олега Ігорьовича
на дисертацію
Василишина Святослава Ігоровича
«Розробка методу використання програмних приманок як елементів захисту комп'ютерних мереж на основі технології Blockchain»,
подану на здобуття наукового ступеня доктора філософії за спеціальністю
125 «Кібербезпека та захист інформації»
(галузь знань 12 «Інформаційні технології»)

Актуальність теми дисертації.

Останнім часом зростає інтерес до безпеки та захисту інформації для мережевих систем. Мережеві системи містять цінні дані та ресурси, які необхідно захищати від зловмисників. Експерти з безпеки часто використовують honeypots і honeynet для захисту мережевих систем. Програмна приманка – це сучасна технологія, яку експерти з безпеки використовують для виявлення нових методів злому від зловмисників. Її також можна визначити як «ресурс інформаційної системи, цінність якого полягає у несанкціонованому або незаконному використанні цього ресурсу».

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 Інтернету речей (IoT), бездротових сенсорних мережах (WSN), транспортних мережах 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 забезпечити децентралізацію управління, виключення людського фактору, тощо. Технологія Blockchain володіє динамічними атрибутами, які у з'вязці з програмними приманками могли б нівелювати недоліки перших. Для цього важливо розробити та дослідити ефективність симбіозу даних технологій на прикладах зовнішніх мережевих атак.

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

Дисертаційні дослідження виконувались у відповідності до наукового напряму кафедри захисту інформації Національного університету «Львівська

політехніка» – «Дослідження систем технічного захисту інформації, каналів зв'язку та комп'ютерних мереж, фізичного захисту інформації та криптографії», в межах кафедральної науково-дослідної роботи: «Розроблення та удосконалення методів і засобів захисту інформації для протидії несанкціонованому доступу в інформаційно-комунікаційних мережах» (шифр ЗІ-7) (№ держреєстрації 0119U101690) (2019 р.-2022 р.).

Наукова новизна роботи полягає в тому, що:

1. Вперше розроблена модель динамічної системи активних програмних приманок, що використовують Blockchain технологію. На відміну від відомих дана модель інтегрує децентралізовані та автоматично оновлювані атрибути пасток, що дало змогу підвищити ефективність захисту мережі шляхом зменшення навантаження на мережеву інфраструктуру та часу відгуку сервісів у разі атаки.
2. Набув подальшого розвитку математичний опис обчислення динамічних атрибутів програмних приманок, який, на відміну від відомих враховує динамічні та транслокаційні можливості Blockchain-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.
3. Вперше, на основі розробленої моделі динамічної системи програмних (активних) приманок, яка використовує Blockchain-технологію для підтримки безпеки, прозорості та адаптивності до зовнішніх атак, 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 збергіє інформацію про атаки на систему на Blockchain-платформі, що забезпечує високий рівень збереження даних та гарантує їхню незмінність.

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 допущень під час вибору математичних моделей і коректному використанні математичного апарату. Крім того, достовірність підтверджується результатами комп'ютерного моделювання та практичною реалізацією системи динамічних програмних приманок, а також збіжністю з результатами експериментальної верифікації.

Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних курсів, де можуть бути застосовані отримані результати.

Наукові результати, отримані автором, можуть бути використані при розробці та побудові новітніх мережевих систем, які використовують технологію

Blockchain та програмні приманки в якості активного захисту та для підсилення наявних систем захисту в приватних або державних компаніях

Також їх можна впровадити у навчальний процес у курсі "Нормативно-правове забезпечення та міжнародні стандарти кібербезпеки" для студентів спеціальності 125 «Кібербезпека та захист інформації».

Практичне значення одержаних результатів полягає у можливості їх безпосереднього застосування для підсилення наявних систем активного та пасивного захисту в корпоративних та державних підприємствах.

1. Розроблена модель динамічної системи активних пасток на основі програмних приманок побудованих на системі Blockchain, яка дала змогу в залежності від різних ситуацій моделювання (в залежності від атаки) 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. Удосконалення математичного апарату програмних приманок за рахунок додавання та обчислення динамічних атрибутів програмних приманок дало змогу 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. Підвищено 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. Система активних пасток не дозволяє декодувати інформацію без відповідного ключа конфіденційності, що забезпечує захист каналу передачі даних та запобігає витоку даних через перехоплення та розшифрування інформації під час її передачі. Експеримент з сніфер атакою на розроблену модель системи показує, ефективність реалізації захисту від перехоплення на основі шифрування.

4. Удосконалення алгоритму визначення та передачі вузлових хостів в системі Blockchain, за рахунок впровадження плаваючих хостів в мережі, підвищило загальну адаптивність мережі реагувати на зовнішні атаки. Цей алгоритм, на відміну від відомих дозволяє системі реагувати на атаки типу сканування та закривати порти доступу реагуючи на зловмисні дії. Результати експерименту під час атаки сканування на відкриті порти дозволили автоматизувати закриття портів, за рахунок зміни основного хоста, що ускладнює збір інформації та можливість доступитись до системи ззовні.

5. Розроблений метод використання програмних приманок, що побудований на основі використання технології Blockchain вимагає більше ресурсів від нападника для здійснення атаки на мережу: потужності комп'ютерів, серверів з яких здійснюється атака а також більше фізичного часу, що збільшує час для фахівців з кібербезпеки для реагування та контр дії нападу до 45%. Було проведено однакову кількість атак як на централізовану систему, яка використовує програмні приманки так і на динамічну систему, яка побудована на розробленому методі. Найбільшу різницю видно не на всіх сервісах: Apache та Nginx динамічної системи зазнають під час атаки майже однакового з центральним аналогом результатів.

Однак сервіси Vsftpd та MySQL вимагають використання значно більших ресурсів від нападника, що показує ефективність розробленого методу у плані захисту комп'ютерної мережі. З тридцяти проведених атак розроблена модель успішно заблокувала 50% в той час як централізована всього 13%, що показує покращення захисних можливостей розробленої моделі. Захист децентралізованої моделі мережі під час DDoS атаки вищий на 14%. Захист децентралізованої моделі мережі під час атаки сканування вищий на 44%, майже в два рази. Захист децентралізованої моделі мережі під час сніфер атаки вищий на 37%. Загальний захист комп'ютерної мережі побудованої з використанням програмних приманок на основі технології Blockchain вищий на 37% в порівнянні з централізованим аналогом, що є підвищенням глобального рівня захисту мережі в півтора рази.

Запропоновані в роботі підходи та методи дають змогу суттєво підсилити існуючі системи активного та пасивного захисту в корпоративних та державних підприємствах. Розроблена модель динамічної системи активних програмних приманок, що використовують блокчейн технологію інтегрує децентралізовані та автоматично оновлювані атрибути пасток, що дає можливість підвищити ефективність захисту мережі шляхом зменшення навантаження на мережеву інфраструктуру та часу відгуку сервісів у разі атаки. Це оптимізовує 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.

Результати дисертаційної роботи впроваджено у технологічні процеси ТОВ «Н-ІКС СПЕЙС» (м.Львів).

Зауваження по дисертації.

1. Оскільки дисертаційна робота за своїм науковим напрямом спрямована на підвищення захисту комп'ютерних мереж, то у першому розділі дисертаційної роботи автору доцільно було б більше уваги приділити аналізу альтернативних методів використання програмних приманок та систем обману. Це б дозволило підвищити ґрунтовність обраної теми та підкреслити проблеми, які мають місце при використанні програмних приманок для захисту від кіберзлочинів.

2. У роботі варто було б привести результати впливу закритої Blockchain мережі на зовнішні відкриті мережі. Дане обґрунтування дозволило б представити можливості і обмеження застосування Blockchain технології для різних типів мереж, в тому числі при використанні її для роботи програмних приманок.

3. У дисертаційні роботі розглядаються не всі сучасні цільові атаки на комп'ютерні мережі, можливість їх комплексування та гібридність, що не дозволяє в повному обсязі оцінити високий рівень захищеності розробленої мережі. Вибір цільових атак, які здійснював автор при представлені експериментальної частини, дозволив б оцінити обмеження, які має розроблений метод.

4. В роботі декларуються перспективи використання даної технології для військових, зокрема для координації БПЛА, проте в самому тексті дисертаційної роботи не згадано в який спосіб запропонована модель може бути там застосована.

5. Під час дослідження особливостей використання приманок автор не згадує про ефективність захисту від внутрішніх атак або інсайдерів в розробленій мережі.

6. У роботі зустрічаються описки, неточності формулювання, варто було притримуватись однакової термінології

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

Висновок

Не зважаючи на виявлені недоліки дисертаційна робота Василишина Святослава Ігоровича на тему «Розробка методу використання програмних приманок як елементів захисту комп'ютерних мереж на основі технології Blockchain» є завершеною науковою працею, яка представлена на здобуття наукового ступеня доктора філософії за спеціальністю 125 "Кібербезпека та захист інформації" (галузь знань 12 «Інформаційні технології»), яка за своїм змістом, структурою, обсягом, науковою новизною та практичним значенням відповідає паспорту спеціальності 125 "Кібербезпека та захист інформації" та чинним вимогам, які встановлені у "Порядку присудження ступеня доктора філософії", який затверджений Постановою Кабінету Міністрів України від 12.01.2022 р. №44, а її автор заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 "Кібербезпека та захист інформації".

Офіційний рецензент
Кандидат технічних наук, доцент,
Доцент кафедри захисту інформації
Національного університету
"Львівська політехніка" Олег ГАРАСИМЧУК

Підпис к.т.н., доцента Гарасимчука О.І. засвідчую.
Вчений секретар
Національного університету
"Львівська політехніка" Роман БРИЛИНСЬКИЙ
к.т.н., доцент