https://doi.org/10.31891/2219-9365-2025-81-19
УДК 004.056:004.852:004.75

КАШТАЛЬЯН Антоніна
Хмельницький національний університет
https://orcid.org/0000-0002-4925-9713
e-mail: antonina.kashtalian@gmail.com

МЕТОДИ ОРГАНІЗАЦІЇ ФУНКЦІОНУВАННЯ МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМ АНТИВІРУСНИХ КОМБІНОВАНИХ ПРИМАНОК ТА ПАСТОК В КОРПОРАТИВНИХ МЕРЕЖАХ

В роботі розроблено методи для організації прийняття рішень та функціонування обманних систем на основі попереднього досвіду функціонування та різних варіантів виконання завдань. Для цього здійснено формальне подання компонентів в архітектурі мультикомп'ютерних систем та зв'язків між ними. Запропоновано розмежувати центр системи та контролер прийняття рішень. До завдань центру системи віднесено підготовку варіантів виконання завдань, а до контролеру прийняття рішень віднесено оцінювання варіантів виконання завдань з урахуванням попереднього досвіду їх застосування та вибір одного з них. Розроблено аналітичні вирази для опису процесів в мультикомп'ютерних системах, які використано в системах для забезпечення спроможності систем до самостійного прийняття рішень щодо виконуваних завдань.

Метою роботи було покращення прийняття рішень мультикомп'ютерними системами з комбінованими антивірусними приманками та пастками щодо подальших кроків за рахунок формування поліморфних відповідей на події з урахуванням попереднього досвіду застосування варіантів відповідей та функціонування систем.

За результатами запропонованих рішень було розроблено прототип системи та проведено з ним експерименти. Експерименти було проведено для випадку з вибором одного з п'яти варіантів виконання завдань і для випадку наявності всього одного варіанту виконання завдання. Згідно результатів проведеного експерименту було встановлено, що стійкість системи на протязі її функціонування є кращою для першого випадку, тобто з урахуванням запропонованих рішень, порівняно з традиційним підходом за другим варіантом. Таким чином, розроблені рішення щодо функціонування систем з урахуванням попереднього досвіду дозволили синтезувати стійкіші системи.

Ключові слова: системи обману; багатокомп'ютерні системи; мережа з приманками; пастка; приманки; виявлення зловмисного програмного забезпечення.

KASHTALIAN Antonina
Khmelnytskyi National University

METHODS FOR ORGANIZING THE FUNCTIONING OF MULTI -COMPUTER SYSTEMS OF ANTIVIRAL COMBINED BAITS AND TRAPS IN CORPORATE NETWORKS

The work has developed methods for organizing decision -making and functioning of fraudulent systems on the basis of previous experience of functioning and different options for completing tasks. To do this, formal submission of components in the architecture of multi -computer systems and the connections between them. It is proposed to differentiate the system center and decision -making controller. The tasks of the Center of the system include preparation of options for completing tasks, and the decision -making controller includes evaluation of options for completing tasks, taking into account the previous experience of their application and the choice of one of them. Analytical expressions have been developed to describe the processes in multicomputer systems used in systems to ensure the ability of systems to make independent decision -making on the tasks performed.

The purpose of the work was to improve decision making with multi -computer systems with combined antiviral baits and traps on further steps by forming polymorphic answers to events, taking into account the previous experience of using the response and functioning of systems.

According to the results of the proposed decisions, the prototype of the system was developed and experiments were conducted with it. The experiments were conducted for the case with the choice of one of the five variants of tasks and for the case of just one option. According to the results of the experiment, it was found that the stability of the system during its functioning is the best for the first case, that is, taking into account the proposed decisions, compared to the traditional approach in the second option. Thus, developed decisions on the functioning of systems, taking into account the previous experience, allowed to suggest more stable systems.

Keywords: deception systems; multi-computer systems; honeynet; trap; baits; malware detection.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Ресурси корпоративних мереж та компоненти їх інфраструктури залишаються найбільш цікавими для зловмисників [1, 2] порівняно з рештою об'єктів комп'ютеризації [3]. Вони є найбільш поширеними та типовими, що спрощує їх розуміння зловмисниками і, відповідно, спонукає до зловмисних дій в них. Крім того, в контексті їх конфігурування для протидії зловмисникам вони мають власні обчислювальні ресурси, які можуть бути застосовані для забезпечення кібербезпеки та захисту інформації [3]. Або вони можуть доповнені певними незначними засобами чи системами, які в поєднанні з наявними, можуть забезпечити належний рівень кібербезпеки в них.

До розроблюваних систем забезпечення безпеки та захисту інформації [4, 5] висуваються вимоги аналогічні типовим системам щодо якості систем і програмних засобів [3], керування життєвим циклом [5], гарантування в життєвому циклі [6], цілісності систем [7], процесів життєвого циклу систем і керування ризиками [8], оцінювання процесів [3], а також спеціальні вимоги в контексті специфіки виконуваних ними завдань [9]. Такими вимогами є вимоги щодо методів захисту і безпеки прикладних програм [3, 4], процесів оброблення вразливостей [1], керування інформаційною безпекою [3] тощо. Проте, незважаючи на такі вимоги до систем та організації процесів в них, які визначені, зокрема в [3], систематизовані та повинні бути виконанні в процесі синтезу систем, на практиці такі системи мають недоліки в частині виконання своїх функцій із забезпечення безпеки та захисту інформації, а також власної стійкості щодо зловмисних впливів [4].

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Для певних типів зловмисних загроз розроблені окремі засоби та системи. В корпоративних мережах засоби і системи, які розроблені для виявлення ЗПЗ та запобігання КА тощо, комбінують для покращення кібербезпеки та захисту інформації. Зокрема, застосовують системи моніторингу загроз, брандмауери, системи виявлення вторгнень тощо, але проблема протидії зловмисним впливам залишається невирішеною, тобто вони недостатньо ефективні [4] не тільки при самостійному застосуванні, а також і при поєднанні на різних етапах виявлення та протидії. Найбільшою проблемою засобів і систем виявлення [1] є їх неспроможність належним чином здійснювати виявлення атак нульового дня та нових зловмисних впливів, а також здійснювати детальний аналіз поведінки зловмисника.

Перспективним напрямом для подолання проблем щодо протидії та виявлення зловмисних впливів в корпоративних мережах [1, 4] є застосування технологій та засобів обману зловмисників, які можуть здійснювати впливи ззовні та зсередини корпоративних мереж. Використання таких засобів регламентовано методичними рекомендаціями в [3]. Вони здатні вирішувати завдання щодо виявлення атак нульового дня, нових зловмисних впливів та збирати дані про поведінку зловмисника з метою її подальшого аналізу. Крім того, такі системи та засоби уповільнюють роботу зловмисників, створюють відчуття небезпеки для них та спонукають зловмисників неефективно використовувати свої ресурси. Засоби та системи, функціонування яких передбачає використання обманних технологій, можуть бути поєднані та поєднуються з рештою засобів та систем забезпечення безпеки і захисту інформації в корпоративних мережах, що покращує ефективність протидії зловмисним впливам. Але проблема залишається і вимагає від розробників постійного удосконалення наявних та розроблення принципово нових засобів і систем. В контексті засобів і систем для обману зловмисників можна виокремити такі напрями для подальшого розроблення, які б могли покращити їх функціонування в цілому: технології обману в корпоративних мережах; архітектура систем обману; архітектура засобів обману. Засоби обману можуть бути окремими об’єктами в корпоративних мережах, а можуть також бути частинами чи компонентами [3] обманних систем.

Технології обману в корпоративних мережах повинні постійно оновлюватись. Зловмисники отримують інформацію з відкритих джерел щодо різних комерційних засобів та систем з обманними технологіями, які пропонуються для корпоративних мереж. Тому, вони можуть їх досліджувати. А також, ефективність дослідження зростатиме особливо у випадку перебування зловмисників безпосередньо в периметрі захисту корпоративних мереж. Крім того, складним завданням для розробників обманних технологій є оцінювання їх ефективності та доцільності застосування при певних умовах. Тобто, безпосередньо самі варіанти обману мають бути різноманітними і такими, що дійсно можуть спрацювати при зловмисних впливах в корпоративних мережах. Ці варіанти обману можуть бути реалізовані безпосередньо окремими засобами обману або в архітектурі систем обману [4].

Кіберобман є ключовим проактивним методом кіберстійкості [4], який створює значну плутанину у виявленні та націленні на кіберактиви. Однією з ключових цілей кіберобману є приховування справжньої особистості кіберактивів, щоб ефективно відвернути супротивників від критично важливих цілей і виявити їхню діяльність на ранніх етапах ланцюжків атак. Для його забезпечення реалізовано адаптивний захист, тобто стратегію кіберзахисту, в якій набір конфігурацій системи динамічно змінюється з метою підвищення невизначеності та складності для зловмисників, які намагаються виявити та використати вразливості. Щоб покращити кібергнучкість мереж здійснюють багатовимірний адаптивний захист на рівні мережі в повному масштабі за межами фізичних обмежень мереж шляхом використання програмно-конфігурованої мережі (SDN). Також, враховуючи зростання складності кібератак, яке знижує ефективність експертного втручання людини через їх повільний час реагування, потрібно розробляти обманні засоби і системи на основі динамічного прийняття рішень [4]. Системи постійно піддаються атакам, що значно спрощує завдання зловмисникам, оскільки реагування на атаки полегшує збір інформації про організацію захисту корпоративних мереж. Це пов'язано з тим, що програмне забезпечення та протоколи традиційно були розроблені для забезпечення інформативного зворотного зв'язку для виявлення та виправлення помилок, а не для приховування причин несправностей. Тому, багато традиційних засобів безпеки у відповідь на

спроби вторгнень дозволяють зловмисникам легко картографувати мережі і діагностувати вразливості системи.

В корпоративних мережах з часом їх експлуатації застарілі апаратні та програмні засоби замінюються новими. Тому, для зловмисників поле діяльності постійно підтримується в актуальному стані [1]. В змінених оновлених апаратному та програмному забезпеченні завжди з'являються певні недопрацювання розробників в контексті вразливостей, що дає змогу зловмисникам використовувати це для своїх цілей.

Використання обманних об'єктів в корпоративних мережах потребує кваліфікованого персоналу [3] і може бути складним. Зловмисник може виявити такі об'єкти та використати їх в своїх атаках. Приманки як обманні об'єкти є ресурсами в корпоративних мережах. Вони призначені для залучення, виявлення та збору інформації про комп'ютерні атаки. Переважно вони класифікуються за рівнем взаємодії, що надається потенційним зловмисникам [4]. Приманки з низьким рівнем взаємодії [10] здійснюють надання емульованих сервісів без повної функціональності серверу з метою виявлення несанкціонованої активності за допомогою псевдосервісів, що легко розгортаються. Приманки з високим рівнем взаємодії забезпечують відносно повну систему, з якою зловмисники можуть взаємодіяти, і призначені для збору детальної інформації про комп'ютерні атаки. Незважаючи на свою популярність, приманки з низьким і з високим рівнями взаємодії часто виявляються поінформованими зловмисниками, бо мають обмежений набір послуг, що дозволяє ідентифікувати їх як приманки. Наприклад, приманки можуть демонструвати шаблони трафіку та дані, які суттєво відрізняються від справжніх сервісів. Тому, розроблення приманок як окремих обманних засобів для застосування в корпоративних мережах теж залишається актуальним завданням.

Зловмисники легко досліджують сучасний Інтернет у пошуках вразливого програмного забезпечення. Це дозволяє їм зосередити свої атаки на вразливих цілях. Вони надсилають тестові дані (зонд), які створені для масового запуску певної відомої помилки в програмному забезпеченні на багато серверів у мережі. Виправлені сервери відповідають на зонд правильно сформованим виведенням, наприклад, повідомленням про помилку. Але сервери без виправлень поводяться нестабільно, наприклад, відповідають рядком сміття або аварійно завершують роботу та перезавантажуються. Спостерігаючи за останньою реакцією, зловмисник наступним кроком надсилає більш конструктивний зловмисний запит на невиправлені сервери. Наприклад, такий, що використовує помилку для захоплення потоку керування програмним забезпеченням користувача, змушуючи його виконувати зловмисні дії від імені зловмисника, а не просто аварійно завершувати роботу [10]. В результаті багатократних звернень зловмисника до одного і того ж ресурсу в мережах та опрацювання ним відповідей за різними своїми запитами виникає модель зв'язку між зловмисником і об'єктом атаки, яка відповідає стратегіям в теорії ігор. Це може бути використано розробниками систем та засобів з приманками з практичної сторони в реальних системах, а також і для моделювання таких відношень.

При роботі з приманками на практиці потрібно вирішити проблеми з безпекою та продуктивністю. Приманка розгалужує увесь процес сервера для створення процесу-клону у відповідь на спроби вторгнення і, при цьому, може ненавмисно копіювати певні області в адресному просторі процесів користувачів. Зокрема, в таких областях можуть бути ключі шифрування паралельних сесій, покажчики на дочірні приманки тощо. Тоді, зловмисник отримав би потенційний доступ до секретів, які може містити приманка. Практичне впровадження приманок, також, вимагає, щоб вони майже не породжували застосункових витрат для законних користувачів, працювали достатньо добре для зловмисників без породження збоїв атак і не були помітні, пропонували високу сумісність із програмним забезпеченням, яке дозволяє мультиобробку, багатопоточність та активну міграцію з'єднань між IP. Також, віддалене розгалуження сеансів зловмисників на приманки має відбуватись в реальному часі і без помітних збоїв у цільовій програмі. Це означає, що встановлені з'єднання, зокрема, з'єднання зловмисника, не повинні бути розірвані. Крім того, розгортання приманки має бути швидким, щоб не пропонувати відкриті, надійні канали синхронізації, які рекламують медовий патч. Нарешті, всі конфіденційні дані повинні бути відредаговані, перш ніж приманка відновить виконання, щоб уникнути надання зловмиснику потенційного доступу до секретів користувача. Таким чином, необхідне забезпечення продуктивності часу, яке виключає клонування на системному рівні. Наприклад, клонування віртуальних машин [11] для розгалуження сеансу. Також, може бути використана альтернатива, яка заснована на міграції процесів через контрольну точку перезапуску [12]. Щоб масштабуватися до багатьох одночасних атак, може бути використана віртуалізація на рівні ОС для розгортання розгалужених процесів у контейнери-приманки, які можуть створюватися, розгортатися та знищуватися на порядки швидше, ніж інші методи віртуалізації, такі як повна віртуалізація або паравіртуалізація [13]. Віртуалізація на рівні ОС дозволяє декільком гостьовим вузлам (контейнерам) спільно використовувати ядро свого керуючого хоста. Контейнери Linux [14] реалізують віртуалізацію на рівні ОС з управлінням ресурсами через групи управління процесами та повною ізоляцією ресурсів через простори імен Linux. Це гарантує, що процеси, файлова система, мережа та користувачі кожного контейнера залишаються взаємно ізольованими.

Міграція процесів через точку перезапуску [12] полягає в передачі запущеного процесу між двома вузлами шляхом скидання його стану на джерело та відновлення його виконання на місці призначення. Ця проблема особливо актуальна для високопродуктивних обчислень. Процес точка-перезапуск відіграє ключову роль у тому, щоб зробити концепцію щодо приманок життєздатною. Він забезпечує швидкий і безперебійний механізм для забезпечення прозорого розгалуження сеансів зловмисника та добре масштабується навіть у невеликих середовищах.

Розгалужені приманки містять оманливу файлову систему, яка не приховує всі секрети, і яка може бути пронизана дезінформацією для подальшого обману, затримки та введення в оману зловмисників.

В роботі [15] визначено дві властивості, які необхідні для успішного розгортання обманних систем на основі приманок: нерозрізненість; секретність. Нерозрізненість полягає в тому, щоб обманути зловмисника. Приманки повинні бути важко відрізнюваними від реальних об’єктів в мережах. Секретність полягає в тому, що у системі відомості про обманні об'єкти є таємницею. Таким чином, застосовується принцип Керкгоффза, згідно з яким стійкість криптографічного алгоритму не має залежати від архітектури алгоритму, а має залежати тільки від ключів. Тобто, при оцінюванні надійності шифрування необхідно вважати, що супротивник знає все про систему шифрування, що використовується, крім ключів. Тобто, безпека системи повинна полягати в секреті. Це означає, відмінності між обманними об'єктами від реальних, а не факт використання обманних об'єктів. Нерозрізнення виникає через нездатність зловмисника визначити успішність атаки результатом використання невиправленої вразливості або обманного об’єкту, що маскується під невиправлену вразливість. У той час як абсолютної, універсальної нерозрізнюваності, ймовірно, неможливо досягти, але при цьому багато форм розрізнюваності можуть бути складними для розрізнення. Секретність базується на наборі вразливостей в обманних об’єктах. Однак повне знання зловмисником деталей архітектури та їх реалізації не розкриває, які вразливості розробник виявив і виправив. Таким чином, адаптуючи принцип Керкгоффза [15] для обману, можна визначити, що обманні об’єкти не можна виявити, навіть якщо все в системі, крім них є загальновідомим. Тобто, обман ґрунтується на чітко визначених секретах, а точніше, на наборі вразливостей у цільових застосунках. Збереження цієї різниці в конфіденційності між публічністю архітектури приманок, деталей їх впровадження і таємницею того, які саме вразливості вони демонструють, важливо для створення надійних, ефективних обманних об’єктів [15] в мережах.

З часом, для покращення ефективності обманних технологій їх почали реалізовувати безпосередньо в програмних системах, в які зловмисники прагнуть проникнути, а не як незалежні системи-приманки, тобто розробляти вбудовані приманки.

Важливими характеристиками систем з приманками є їх автономність і стійкість. Висока швидкість і складність сучасних кібератак вимагає від кіберобману автономних для самоадаптації та стійких, щоб зберегти своє функціонування у випадках невдач, які можуть розкрити активи або плани обману. Тому, потрібні методи, які будуть чітко враховувати місію захисника і місію зловмисника, а також які будуть враховувати теоретичні основи, цілі, рівні та ризики автоматизації обманних систем та засобів. Оманні об’єкти можуть бути реалізовані як інтелектуальні агенти [15, 16]. Більшість активних інструментів захисту значною мірою покладаються на методи обману. Для реалізації обману в мережах можуть бути використані методи обфускації, мутація IP-адреси, міграція потоку, мутації топології, мутації зв'язування DNS/IP.

В роботі [17] пропонується двофазний метод обману, що ґрунтується на локалізації приманки. В першій фазі розробляється проактивна політика локалізації приманки, а в другій фазі пропонується реактивний обманний підхід, що динамічно визначає розташування приманок відповідно до оновлень системи виявлення вторгнень. Таким чином, система захисту частково відслідковує активність зловмисника. Метод обману комбінує використання теорії ігор та навчання з підкріпленням.

Стратегія розташування приманок в мережі повинна враховувати не тільки аспекти мережі, яка захищається, а й вподобання зловмисників [18]. Для досягнення цієї мети запропоновано метод із використанням теорії ігор, який генерує оптимальну стратегію розташування приманки відповідно до сценарію атака-захист. Запропонований метод враховує зміни в підключенні до мережі. Представлена модель динамічної гри для двох гравців, що явно враховує розвиток майбутнього стану в результаті змін у підключенні. Цільова функція захисника складається з двох частин Перша частина максимізує ймовірність того, що зловмисник потрапить в приманку, а друга мінімізує витрати, необхідні для обманного середовища та переналаштування топології мережі. Робота [19] зосереджена на динамічному розташуванні приманок та пропонує розподілену схему приманок.

В роботі [20] сформульовано теоретико-ігровий підхід для опису політики локалізації приманки, що захищає найбільш цінні ресурси мережі, та розроблено модель двох гравців для дослідження компромісу різноманіття.

В роботі [21] пропонується масштабований алгоритм розташування приманок над графом атак. Сформульована стратегічна гра для двох осіб з нульовою сумою між захисником і зловмисником. Ця ігрова модель враховує практичну модель загрози відповідно до наявної інформації про зловмисника.

В роботі [22] розроблено новий теоретико-ігровий фреймворк, в якому реалізовано подвійну гру для проектування обманних механізмів, що складаються з генератора, стимулюючого модулятора та модулятора довіри. Показано, що оптимальний модулятор довіри може спричинити бажані дії з боку зловмисників.

В роботах [23, 24] розглянуто перелік обманних тактик, завдяки яким приманки отримують переваги. Було використано ідеї теорії кіберобману та планування.

В роботі [25] наведено унікальні переваги механізмів безпеки, які ґрунтуються на обмані та запропоновано фреймворк, за допомогою якого можна інтегрувати технологію обману в захист комп'ютерної системи. В роботі [25] розглянуто проблему захисту від атак в мережах IoT з приманками з точки зору теоретико-ігрової моделі обману з участю зловмисника та захисника. В роботі [25] запропоновано захисний механізм на основі обману, який включає теорію ігор для моделювання взаємодії між засобом захисту та зловмисником. Використано сигнальну гру з ідеальною баєйсівською рівновагою для дослідження стратегій та визначення важливих наслідків для цього типу динамічних ігор з неповною інформацію. В роботі [26] проведено дослідження двостороннього обману, при якому виконується маніпуляція як приманки, так і цільової системи. Ідея полягає в покращені захисту шляхом створення приманки, схожої на цільову систему, або наданням цільовій системі схожості із приманкою.

Використання систем з приманками пропонується в роботі [27] для забезпечення рівня безпеки, який є наступним рівнем після типових рівнів. Розроблено приманку з використанням генерації функції, в яку задано алгоритми машинного навчання з метою ідентифікації та класифікації сесій атакуючого зловмисника. В роботі [28] здійснено аналіз різних типів атак на кадри клієнта та різний підхід до їх виявлення і вирішення. В роботі [29] створено підроблений сервер для відволікання зловмисників.

В корпоративних мережах для забезпечення безпеки та захисту інформації від працівників пропонується використання датчиків зашифрованих приманок [30]. Ефективність мережевих систем виявлення вторгнень [31] низька через високий відсоток хибно позитивних спрацювань. Використання приманок дозволяє зменшити це число. Система запобігання вторгненням є методом моніторингу зловмисної активності в системі безпеки мережі. Встановлено, що використання приманок в поєднанні з системами виявлення вторгнень зменшує кількість помилкових позитивних результатів.

Методи обману відігравали помітну роль у багатьох людських конфліктах протягом усієї історії [32]. Цифрові конфлікти не відрізняються, оскільки використання обману знайшло свій шлях до обчислення. У роботі [32] представлено модель, яка може бути використана для планування та інтеграції обману в захисні сили комп'ютерної безпеки. Обман як стратегія оборони проти зловмисників має заслугу [56 і може бути привабливою новою здатністю для більш великих організацій, які бажають підвищити виявлення загроз та оборонних рішень. Обман, як автоматизований реагуючий механізм, представляє собою зміну в можливостях IT-безпеки. Обман [33] може відігравати значну роль в покращенні безпеки сучасних комп'ютерних систем. Розроблений фреймворк [34] дає змогу включати інтегровану обманну технологію в захист комп'ютерної системи. В роботі [35] запропоновано обманну гру, яка використовується для оцінювання прийняття зловмисником рішення за наявності обману. В експерименті проаналізовано вплив двох факторів на рішення зловмисника атакувати комп'ютерну мережу: обсяг використаного обману; час обману. В роботі [36] проведено огляд 24 робіт 2008-2018 років, які використовують теорію ігор для моделювання захисного обману для кібербезпеки та приватності. Запропонована класифікація виділяє шість типів обману: збурення; захист рухомої цілі; заплутування; змішування; привабливість; залучення зловмисника. Ці типи характеризуються своїми інформаційними структурами, діями і тривалістю, та концепцією теорії ігор.

Обманні рішення [37] можуть виявляти, аналізувати та захищати веб застосунки від вдосконалених атак, від яких не можуть захистити існуючі рішення на основі пошуку аномалій та методи запобігання атакам.

В роботі [38] досліджено методи на основі кіберобману та розроблено нову концептуальну модель гібридних загроз, що включає методи обману. Більшість програм захисту сфокусовані на стратегії запобігання та стримування зловмисників від потрапляння в мережу. Елементи керування виявленням зловмисних дій зазвичай використовують для посилення запобігання потрапляння в мережу, а не для виявлення загрозу в мережі. Це залишає прогалини у виявленні, які важко заповнити існуючими засобами кібербезпеки. Доцільно використовувати більш збалансовану стратегію, яка включає як виявлення, так і реагування. Більшість організацій розгортають системи виявлення вторгнень, які мають певні обмеження. Індустрія захисту сфокусована на знаходженні більш точних шляхів розпізнавання зловмисних дій із використанням таких технологій, як поведінкова аналітика, великі данні, штучний інтелект та обман.

В роботі [39] представлено нову теоретику-ігрову модель оманливої взаємодії між засобом захисту та зловмисником, яку в роботі названо кібер обман. Розглянуто випадки потужного зловмисника, якому відомо про обманну стратегію засобу захисту, та наївного зловмисника, якому це невідомо. Необхідність зв'язку та передачі даних між споживачами (інтелектуальними лічильниками) та комунальними службами робить інфораструктуру вразливою до атак. Робота [40] сфокусована на розподілених атаках відмови в

обслуговуванні в мережі. В мережу вводять приманки як систему-пастку для виявлення та збору інформації про атаку.

Активні хибні об'єкти цифрових даних розміщені серед реальних об'єктів даних і використовуються для виявлення зловмисного використання даних [42]. В роботі [43] визначено мережевий обман для захисної розвідки та розроблено систему розвідувального обману, яка грунтується на програмно-конфігурованій мережі, щоб досягти обману шляхом імітаці віртуальних топологій.

У роботі [44] розроблено механізми орієнтації на користувачів, які надають мінімальну втрату корисності для гарантування конфіденційності користувача.

Таким чином, для забезпечення безпеки та захисту інформації корпоративних мереж можуть бути застосовані обманні технології для зловмисників. Обман зловмисників, які можуть діяти ззовні та зсередини периметру корпоративної мережі, може бути базований на збуренні, захисті рухомою цілю, заплутуванні, змішуванні, привабливості, залучення зловмисника. Переважно для аналізу та побудови моделей обманних технологій використовують теорію ігор. Крім того, реалізацію обманних технологій здійснюють переважно окремими засобами-приманками або системами з приманками, причому вони можуть бути спрямовані під різні типи ресурсів корпоративних мереж. В процесі реалізації обманних технологій потрібно вирішувати завдання щодо нерозрізнюваності та секретності обманних об’єктів, суть яких полягає в тому що повинен бути забезпечений секрет щодо обману. При цьому в частині завдань обманні об’єкти повинні бути максимально подібні до реальних об’єктів в мережах і видимі для зловмисників, а в частині завдань вони мають бути приховані, тобто перебувати в тіні.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Метод організації функціонування контролеру прийняття рішень

Функціонування контролеру прийняття рішень в архітектурі систем класу [4] є визначальним саме для цього класу систем і потребує розроблення методу організації такого функціонування, яке включатиме безпосередньо внутрішні дії в ньому, взаємодію з центром системи та взаємодію із елементами та компонентами систем. Розглянемо місце контролеру прийняття рішень в архітектурі систем класу та його завдання.

Центр системи готує для визначених завдань, які може розв’язувати в системі, від трьох до п’яти варіантів відповідей з урахуванням попереднього досвіду функціонування системи, зокрема і можливості повторення певних варіантів та їх урізноманітнення. Контролер прийняття рішень отримує від центру системи запропоновані ним варіанти відповідей для виконання завдань, які виникли під час функціонування системи. Подальші дії контролеру прийняття рішень полягають у визначенні лише одного варіанту для використання в системі при виконанні завдання. При цьому вибір єдиного варіанту здійснюється з врахуванням попереднього досвіду функціонування системи з використанням цього варіанту, якщо він вже був раніше, та решти варіантів. Контролер прийняття рішень, також, незалежно від центру системи враховує кількість активних компонент систем та їх розміщення у вузлах в комп’ютерних мережах, значення критеріїв оцінювання варіантів та цільової функції. Після затвердження єдиного варіанту, тобто наступних кроків системи для виконання завдання, контролер передає результат центру системи для фіксування і використання на наступному кроці підготовки варіантів виконання такого ж завдання. Центр системи після отримання відповіді від контролеру запускає процес виконання завдання. Центр системи взаємодіє з контролером прийняття рішень згідно схеми зображеної на рис. 1.

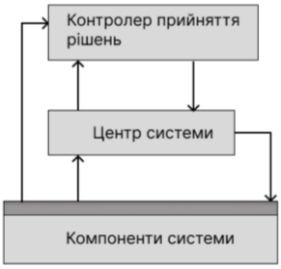

Рис. 1.Схема взаємодії контролеру прийняття рішень та центру системи

Задамо метод організації функціонування контролеру прийняття рішень основними кроками з урахуванням вхідних даних для опрацювання та правил так:

1) формування контролеру прийняття рішень у визначених компонентах системи;

2) перебудова архітектури контролеру прийняття рішень;

3) переміщення контролеру прийняття рішень до визначених компонент системи;

4) встановлення зв'язку між компонентами, що містять поточний контролер прийняття рішень та рештою компонент системи;

5) отримання вхідних даних від центру системи та решти компонент системи;

6) вибір випадковим чином та застосування одного з правил формування стратегії вибору наступного варіанту виконання завдання контролером прийняття рішень;

7) передавання результату з вибору наступного варіанту виконання завдання до центру системи та решти компонент системи.

Таким чином, розроблено метод організації функціонування контролеру прийняття рішень, суть якого полягає у забезпеченні вибору одного варіанту виконання завдання із підготовлених та пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи із застосування варіантів виконання завдання, рівнів безпеки компонент системи, кількості компонент та зв'язків між ними, що дає змогу сформувати поліморфну відповідь системи на подію, яка викликана зовнішніми та внутрішніми впливами в корпоративних мережах.

Метод організації функціонування мультикомп'ютерних систем

Концептуальна модель $\mathfrak{A}_{\mathfrak{M},\mathfrak{S}}$ систем класу $\mathfrak{S}$ [4] враховує множинність елементів, які знаходяться у відносинах та зв'язках один з одним і утворюють певну цілісність та єдність частин. Задані взаємозв'язки між частинами системи та її внутрішня організованість мають конкретні властивості, які змінюються відповідно до зовнішніх і внутрішніх впливів та мети використання систем класу $\mathfrak{S}$. Для організації функціонування таких систем потрібно врахувати не тільки правила внутрішньої організації між елементами та компонентами і правила взаємодії між ними, але потрібно забезпечити зміну їх визначальних властивостей. Тобто, в процесі функціонування системи класу $\mathfrak{S}$ повинні змінювати набір визначальних характеристик. Ці набори визначальних характеристик визначені множинами [4] і допускають велику кількість варіантів. Таким чином, системи класу $\mathfrak{S}$ в процесі свого функціонування в корпоративних мережах багатократно змінюють свої властивості і, тому, з врахування таких особливостей потрібно розробити метод організації функціонування систем, особливістю якого були б можливості систем до самостійної зміни своїх властивостей, організації елементів та компонентів і встановлення зв'язків між ними. Організація централізації в системах класу $\mathfrak{S}$ та наявність контролеру прийняття рішень деталізовані і задані відповідними методами. При цьому, вони є невід'ємними частинами систем класу $\mathfrak{S}$ і, тому, повинні бути враховані при організації взаємодії всіх частин систем.

Для організації функціонування мультикомп'ютерних систем з урахуванням визначених в них компонентів та зв'язків між ними задамо основні кроки методу так:

1) поточне формування системи з активних компонент, які знаходяться в щойно увімкнених комп'ютерних станціях або знаходились в увімкнених раніше комп'ютерних станціях;

2) постійне отримання даних щодо часу функціонування системи та її компонент для формування вектору;

3) отримання даних на виконання вказівок від центру системи та контролеру прийняття рішень для формування вектору врахування поточного часу від початку функціонування системи та значення рівнів функційної та кібербезпеки комп'ютерних станцій компонент системи та вектору стану функційної та кібербезпеки системи;

4) отримання даних на виконання вказівок від центру системи та контролеру прийняття рішень для формування вектору подання зв'язків для кожної компоненти, вектору повноти зв'язків;

5) виявлення події в корпоративній мережі, яка викликана зовнішніми і внутрішніми впливами, її ідентифікація та здійснення вибору завдань з множини завдань системи для відповіді на подію;

6) запуск центру системи для підготовки варіантів відповідей для виконання завдання щодо події з п. 5;

7) запуск контролеру прийняття рішень для затвердження варіанту виконання завдання з п. 6;

8) передача на виконання та виконання затвердженого варіанту виконання завдання з п. 7;

9) вилучення системою частини компонент, в яких значення рівнів функційної та кібербезпеки комп'ютерних станцій компонент системи та стану функційної та кібербезпеки системи перевищує допустимі значення;

10) виконання п. 1-п. 9 для кожної незв'язної частини системи при її поділі;

11) повторне виконання п.6-п.8 у випадку невиконання п. 8;

12) виконання п. 1-п. 4 у випадку успішного виконання п. 8.

Таким чином, розроблено метод організації функціонування мультикомп'ютерних систем, особливістю якого стало забезпечення можливості систем до самостійної зміни своїх властивостей, організації елементів та компонентів і встановлення зв'язків між ними з урахуванням стану функційної та кібербезпеки, а також виокремлення контролеру прийняття рішень та центру системи, що дало змогу забезпечити багатоваріантність при опрацюванні відповіді на подію, яка викликана зовнішніми та внутрішніми впливами на систему в корпоративній мережі.

ЕКСПЕРИМЕНТ

Оскільки метою роботи було покращення прийняття рішень мультикомп'ютерними системами з комбінованими антивірусними приманками та пастками щодо подальших кроків за рахунок формування поліморфних відповідей на події з урахуванням попереднього досвіду застосування варіантів відповідей та функціонування систем, то сфокусуємо постановку експерименту щодо таких показників:

1) врахування попереднього досвіду функціонування системи та застосування варіантів виконання при формуванні поліморфних відповідей на події;

2) стійкість системи;

3) оперативність системи;

4) цілісність системи;

5) безпека системи;

6) оцінювання прийнятих рішень.

В табл. 1 подано дані фрагментом результатів експерименту та загальним підсумком в останніх двох рядках таблиці.

Таблиця 1

Фрагмент результатів експерименту для першого випадку

№	Час вибору варіантів виконання завдань	Час завершення виконання завдань	Номер завдання	Варіанти виконання завдання	Критерій $f_{j,kr}^{m_{pz,i}^{\Theta}}$				Значення цільової функції оцінювання $F_{kr}^{m_{pz,i}^{\Theta}}$	Номер варіанту 1-5	Номер повтору варіанту	Попереднє значення цільової функції
					с	о	ц	б				
1	1,54E-01	5,99E-01	1	1	0,0618	0,0605	0,0641	0,0581	0,0611			
	1,90E-01	3,46E-01		2	0,0577	0,0622	0,0627	0,0620	0,0611	2		
	1,56E-01	5,68E-01		3	0,0624	0,0610	0,0583	0,0588	0,0601			
	1,68E-01	3,63E-01		4	0,0646	0,0604	0,0558	0,0568	0,0594			
	1,53E-01	3,50E-01		5	0,0575	0,0592	0,0591	0,0552	0,0578			
…	…	…	…	…	…	…	…	…	…	…	…	…
100	1,43E-01	5,45E-01	5	1	0,0616	0,0578	0,0602	0,0645	0,0610	1		0,0613
	1,02E-01	4,60E-01		2	0,0579	0,0588	0,0591	0,0623	0,0595			0,0575
	1,66E-01	5,49E-01		3	0,0612	0,0568	0,0576	0,0575	0,0583		3	0,0616
	1,04E-01	3,67E-01		4	0,0593	0,0629	0,0627	0,0571	0,0605			0,0588
	1,34E-01	4,35E-01		5	0,0564	0,0556	0,0596	0,0602	0,0579			0,0604
Разом			1-10 2-19 3-12 4-21 5-16 6-13 7-9									
Середнє значення					0,0605	0,0599	0,0600	0,0602	0,0602			

За результатами експерименту встановлено покращення функціонування мультикомп'ютерної системи при використанні контролеру прийняття рішень (перший випадок). Це підтверджено значеннями результатів обчислення цільової функції оцінювання варіантів виконання завдань. Значення цільової функції для першого випадку знаходяться в межах інтервалу [0;0,07], що відповідають її цільовій меті. В другому випадку (без використання контролеру прийняття рішень) значення цільової функції, які обчислені без врахування попереднього досвіду функціонування системи, для варіантів виконання завдань без вибору з них знаходяться в інтервалі [0,12;0,27]. Такі значення суттєво відхиляються від цільової значення, яке повинно бути близьким до нуля. Також, ці значення суттєво відрізняються від значень для першого випадку, що становить приблизно 15 відсотків. Це впливає на стабільність функціонування системи в другому випадку. Стабільність системи в другому випадку є кращою.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Розроблено метод організації функціонування контролеру прийняття рішень. Його особливістю є забезпечення вибору одного варіанту виконання завдання із підготовлених та пропонованих до розгляду варіантів центром системи з урахуванням попереднього досвіду системи із застосування варіантів виконання завдання, рівнів безпеки компонент системи, кількості компонент та зв'язків між ними. Це дало змогу формувати поліморфні відповіді системи на події, які викликані зовнішніми та внутрішніми впливами в корпоративних мережах.

Розроблено метод організації функціонування мультикомп'ютерних систем, який дає змогу забезпечити можливості систем до самостійної зміни своїх властивостей, організації елементів та компонентів і встановлення зв'язків між ними з урахуванням стану функційної та кібербезпеки. В ньому враховано виокремлення контролеру прийняття рішень та центру системи. Це забезпечило багатоваріантність при опрацюванні відповіді на подію, яка викликана зовнішніми та внутрішніми впливами на систему в корпоративній мережі.

Література

1. Lysenko S, Bobrovnikova K, Kharchenko V, Savenko O. (2022). IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency. Algorithms, 15(7):239.

2. Nicheporuk, A., Savenko, O., Nicheporuk A., Nicheporuk Y. 2020. An android malware detection method based on CNN mixed-data model CEUR Workshop Proceedings Kharkiv, Ukraine. 2732:198–213.

3. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами. *АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ*. НАКАЗ № 463 від 29.05.2023. URL: https://zakon.rada.gov.ua/rada/show/v0463519-23#Text

4. Kashtalian, A., Lysenko, S., Savenko, O., Nicheporuk, A., Sochor, T., & Avsiyevych, V. (2024). Multi-computer malware detection systems with metamorphic functionality. Radioelectronic and Computer Systems, 2024(1), 152-175.

5. ДСТУ ISO/IEC 15026-4:2018 Інженерія систем і програмних засобів. Гарантії стосовно систем і програмних засобів. Частина 4. Гарантування в життєвому циклі (ISO/IEC 15026-4:2012, IDT)

6. ДСТУ ISO/IEC 15026-3:2018 Інженерія систем і програмних засобів. Гарантії стосовно систем і програмних засобів. Частина 3. Рівні цілісності системи (ISO/IEC 15026-3:2015, IDT)

7. ДСТУ ISO/IEC 15026-2:2018 Інженерія систем і програмних засобів. Гарантії стосовно систем і програмних засобів. Частина 2. Сценарій гарантування (ISO/IEC 15026-2:2011, IDT)

8. B. Savenko, A. Kashtalian, S. Lysenko and O. Savenko. (2023). Malware Detection By Distributed Systems with Partial Centralization," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 265-270.

9. D. Denysiuk, O. Savenko, S. Lysenko, B. Savenko and A. Kashtalian. (2023). Method for Detecting Steganographic Changes in Images Using Machine Learning. 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 1-6.

10. Bringer M., Chelmecki C. A Survey: Recent Advances and Future Trends in Honeypot Research. *International Journal of Computer Network and Information Security*. 2012. № 4. DOI: https://doi.org/10.5815/ijcnis.2012.10.07

11. K. G. Anagnostakis, S. Sidiroglou, P. Akritidis, K. Xinidis, E. Markatos, and A. D. Keromytis ―Detecting Targeted Attacks Using Shadow Honeypots,‖ Proceedings of the Conference on USENIX Security Symposium, August 2005, pp. 9-23.

12. Lin Chen, Zhitang Li, Cuixia Gao, and Lan Liu, ―Dynamic Forensics based on Intrusion Tolerance,‖ Proceedings of IEEE International Symposium on Parallel and Distributed Processing with Applications, August 2009, pp. 469-473.

13. Oliver Thonnard and Marc Dadier, ―A Framework for Attack Pattern's Discovery in Honeynet Data,‖ Digital Investigation, vol. 5, no. 1, September 2008, pp. 128-139.

14. Steve Webb, James Caverlee, and Calton Pu,―Social Honeypots: Making Friends with a Spammer Near You,‖ Proceedings of the Conference on Email and Anti-Spam, August 2008. Available: http://citeseerx.ist.psu.edu/ viewdoc/summary?doi=10.1.1.150.588 (last accessed: August 17, 2012).

15. Anoosha Prathapani, Lakshmi Santhanam, and Dharma P Agrawal. Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks. Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems, October 2009, pp. 753-758. URL: https://www.scirp.org/reference/referencespapers?referenceid=794111

16. Bedratyuk L., Savenko O. *MATCH Commun. Math. Comput. Chem.* 2018. № 79. Pp. 407–414.

17. A. H. Anwar, C. A. Kamhoua, N. O. Leslie and C. Kiekintveld, "Honeypot Allocation for Cyber Deception Under Uncertainty," in IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 3438-3452, Sept. 2022, doi: 10.1109/TNSM.2022.3179965.

18. Md Abu Sayed. Honeypot Allocation for Cyber Deception in Dynamic Tactical Networks: A Game Theoretic Approach/ Md Abu Sayed, Ahmed H. Anwar, Christopher Kiekintveld, Charles Kamhoua// arXiv:2308.11817v2 [cs.GT] 5 Sep 2023 https://doi.org/10.48550/arXiv.2308.11817

19. A. H. Anwar and C. A. Kamhoua, "Cyber Deception using Honeypot Allocation and Diversity: A Game Theoretic Approach," 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2022, pp. 543-549 doi: 10.1109/CCNC49033.2022.9700616.

20. A. H. Anwar, C. Kamhoua and N. Leslie, "Honeypot Allocation over Attack Graphs in Cyber Deception Games," 2020 International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, 2020, pp. 502-506 doi: 10.1109/ICNC47757.2020.9049764.

21. L. Huang and Q. Zhu, "Duplicity Games for Deception Design With an Application to Insider Threat Mitigation," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4843-4856, 2021 doi: 10.1109/TIFS.2021.3118886.

22. Ehab Al-Shaer. Autonomous Cyber Deception. Reasoning, Adaptive Planning, and Evaluation of HoneyThings/ Ehab Al-Shaer, Jinpeng Wei, Kevin W. Hamlen, Cliff Wang// Springer Nature Switzerland AG 2019 (eBook) https://doi.org/10.1007/978-3-030-02110-8

23. Almeshekah, M.H., Spafford, E.H. (2016). Cyber Security Deception. In: Jajodia, S., Subrahmanian, V., Swarup, V., Wang, C. (eds) Cyber Deception. Springer, Cham. https://doi.org/10.1007/978-3-319-32699-3_2

24. Q. D. La, T. Q. S. Quek, J. Lee, S. Jin and H. Zhu, "Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 1025-1035, Dec. 2016 doi: 10.1109/JIOT.2016.2547994

25. Çeker, H., Zhuang, J., Upadhyaya, S., La, Q.D., Soong, BH. (2016). Deception-Based Game Theoretical Approach to Mitigate DoS Attacks. In: Zhu, Q., Alpcan, T., Panaousis, E., Tambe, M., Casey, W. (eds) Decision and Game Theory for Security. GameSec 2016. Lecture Notes in Computer Science(), vol 9996. Springer, Cham. https://doi.org/10.1007/978-3-319-47413-7_2

26. Aggarwal, P., Du, Y., Singh, K., & González, C. (2021). Decoys in Cybersecurity: An Exploratory Study to Test the Effectiveness of 2-sided Deception. ArXiv, abs/2108.11037.

27. Rowe, N.C. (2019). Honeypot Deception Tactics. In: Al-Shaer, E., Wei, J., Hamlen, K., Wang, C. (eds) Autonomous Cyber Deception. Springer, Cham. https://doi.org/10.1007/978-3-030-02110-8_3

28. Valero, J.M., Pérez, M.G., Celdrán, A.H., & Pérez, G.M. (2020). Identification and Classification of Cyber Threats Through SSH Honeypot Systems. https://www.semanticscholar.org/paper/Identification-and-Classification-of-Cyber-Threats-Valero-P%C3%A9rez/f561f1122402acfc3bd01c33edbc6490125ef14a

29. Biswas J. Analysis of Client Honeypots. (IJCSIT) International Journal of Computer Science and Information Technologies. 2014. Vol. 5 (4). P. 5776-5780. https://ijcsit.com/docs/Volume%205/vol5issue04/ijcsit20140504209.pdf

30. Mukti, Fransiska Sisilia & Sukmawan, R.. (2021). Integration of Low Interaction Honeypot and ELK Stack as Attack Detection Systems on Servers. Jurnal Penelitian Pos dan Informatika. 11. 10.17933/jppi.v11i1.336.

31. Yamin, M.M., Katt, B., Sattar, K., & Ahmad, M.B. (2019). Implementation of Insider Threat Detection System Using Honeypot Based Sensors and Threat Analytics. Lecture Notes in Networks and Systems. https://www.semanticscholar.org/paper/Implementation-of-Insider-Threat-Detection-System-Yamin-Katt/67ebef836b3993a68f81840fd65ed0b37a9e5d6e

32. Mohammadzadeh, Hamid, Roza Honarbakhsh and Omar Bin Zakaria. "A Survey on Dynamic Honeypots." International Journal of Information Engineering and Electronic Business (2012): n. pag. https://www.semanticscholar.org/paper/A-Survey-on-Dynamic-Honeypots-Mohammadzadeh-Honarbakhsh/137a32a02099f767414b852b9fbecec7c15ddf75

33. Mohammed H. Almeshekah and Eugene H. Spafford. 2014. Planning and Integrating Deception into Computer Security Defenses. In Proceedings of the 2014 New Security Paradigms Workshop (NSPW '14). Association for Computing Machinery, New York, NY, USA, 127–138. https://doi.org/10.1145/2683467.2683482

34. Pingree, L. (2016). Emerging Technology Analysis : Deception Techniques and Technologies Create Security Technology Business Opportunities. https://www.semanticscholar.org/paper/Emerging-Technology-Analysis-%3A-Deception-Techniques-Pingree/945207097007a80c321277c903401c633e7b5fcd

35. Almeshekah, M.H., & Spafford, E.H. (2016). Cyber Security Deception. Cyber Deception. p. 25-52. https://www.semanticscholar.org/paper/Cyber-Security-Deception-Almeshekah-Spafford/101feca00418270ffbb5cda4884dc24ab0aaab22

36. Aggarwal, P., Gonzalez, C., Dutt, V. (2016). Cyber-Security: Role of Deception in Cyber-Attack Detection. In: Nicholson, D. (eds) Advances in Human Factors in Cybersecurity. Advances in Intelligent Systems and Computing, vol 501. Springer, Cham. https://doi.org/10.1007/978-3-319-41932-9_8

37. Pawlick, J., Colbert, E., & Zhu, Q. (2017). A Game-theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy. ACM Computing Surveys (CSUR), 52, 1 - 28. https://www.semanticscholar.org/paper/A-Game-theoretic-Taxonomy-and-Survey-of-Defensive-Pawlick-Colbert/47e558cd6c72e7292d7d686cdffaefe0e6e5fba2

37. Efendi, M.A., Ibrahim, Z.B., Zawawi, M.N., Rahim, F.A., Pahri, N.A., & Ismail, A. (2019). A Survey on Deception Techniques for Securing Web Application. 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), 328-331. https://www.semanticscholar.org/paper/A-Survey-on-Deception-Techniques-for-Securing-Web-Efendi-Ibrahim/d2c9acbda2145fe8860e81cdcc870486a560a3e6

38. Steingartner W, Galinec D, Kozina A. Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. Symmetry. 2021; 13(4):597. https://doi.org/10.3390/sym13040597

39. Li Y, Shi L, Feng H. A Game-Theoretic Analysis for Distributed Honeypots. Future Internet. 2019; 11(3):65. https://doi.org/10.3390/fi11030065

40. Aaron Schlenker, Omkar Thakoor, Haifeng Xu, Fei Fang, Milind Tambe, Long Tran-Thanh, Phebe Vayanos, and Yevgeniy Vorobeychik. 2018. Deceiving Cyber Adversaries: A Game Theoretic Approach. In Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS '18). International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 892–900. https://dl.acm.org/doi/10.5555/3237383.3237833

41. K. Wang, M. Du, S. Maharjan and Y. Sun, "Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid," in IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2474-2482, Sept. 2017, doi: 10.1109/TSG.2017.2670144.

42. Asaf Shabtai, Maya Bercovitch, Lior Rokach, Ya'akov (Kobi) Gal, Yuval Elovici, and Erez Shmueli. 2016. Behavioral Study of Users When Interacting with Active Honeytokens. ACM Trans. Inf. Syst. Secur. 18, 3, Article 9 (April 2016), 21 pages. https://doi.org/10.1145/2854152

43. S. Achleitner, T. F. La Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy and R. Chadha, "Deceiving Network Reconnaissance Using SDN-Based Virtual Topologies," in IEEE Transactions on Network and Service Management, vol. 14, no. 4, pp. 1098-1112, Dec. 2017, doi: 10.1109/TNSM.2017.2724239.

44. Reza Shokri. 2015. Privacy games: Optimal user-centric data obfuscation. Proc. Privacy Enhancing Technologies 2 (2015), 299–315. https://petsymposium.org/popets/2015/popets-2015-0024.pdf

References

1. Lysenko S, Bobrovnikova K, Kharchenko V, Savenko O. (2022). IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency. Algorithms, 15(7):239.

2. Nicheporuk, A., Savenko, O., Nicheporuk A., Nicheporuk Y. 2020. An android malware detection method based on CNN mixed-data model CEUR Workshop Proceedings Kharkiv, Ukraine. 2732:198–213.

3. Methodical recommendations for providing cyber defense of automated technological process management systems. Administration of the State Service of Special Communication and Information Protection of Ukraine. Order No. 463 dated 29.05.2023. URL: https://zakon.rada.gov.ua/rada/show/v0463519-23#Text

4. Kashtalian, A., Lysenko, S., Savenko, O., Nicheporuk, A., Sochor, T., & Avsiyevych, V. (2024). Multi-computer malware detection systems with metamorphic functionality. Radioelectronic and Computer Systems, 2024(1), 152-175.

5. DSTU ISO/IEC 15026-4: 2018 Engineering of systems and software. Guarantees on systems and software. Part 4. Guarantee in the life cycle (ISO/IEC 15026-4:2012, IDT)

6. DSTU ISO/IEC 15026-3: 2018 Engineering of systems and software. Guarantees on systems and software. Part 3. Levels of system integrity (ISO/IEC 15026-3:2015, IDT)

7. DSTU ISO/IEC 15026-2: 2018 Engineering of systems and software. Guarantees on systems and software. Part 2. Guarantee Scenario (ISO/IEC 15026-2:2011, IDT)

8. B. Savenko, A. Kashtalian, S. Lysenko and O. Savenko. (2023). Malware Detection By Distributed Systems with Partial Centralization," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 265-270.

9. D. Denysiuk, O. Savenko, S. Lysenko, B. Savenko and A. Kashtalian. (2023). Method for Detecting Steganographic Changes in Images Using Machine Learning. 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 1-6.

10. Bringer M., Chelmecki C. A Survey: Recent Advances and Future Trends in Honeypot Research. *International Journal of Computer Network and Information Security*. 2012. № 4. DOI: https://doi.org/10.5815/ijcnis.2012.10.07

11. K. G. Anagnostakis, S. Sidiroglou, P. Akritidis, K. Xinidis, E. Markatos, and A. D. Keromytis ―Detecting Targeted Attacks Using Shadow Honeypots,‖ Proceedings of the Conference on USENIX Security Symposium, August 2005, pp. 9-23.

12. Lin Chen, Zhitang Li, Cuixia Gao, and Lan Liu, ―Dynamic Forensics based on Intrusion Tolerance,‖ Proceedings of IEEE International Symposium on Parallel and Distributed Processing with Applications, August 2009, pp. 469-473.

13. Oliver Thonnard and Marc Dadier, ―A Framework for Attack Pattern's Discovery in Honeynet Data,‖ Digital Investigation, vol. 5, no. 1, September 2008, pp. 128-139.

14. Steve Webb, James Caverlee, and Calton Pu,―Social Honeypots: Making Friends with a Spammer Near You,‖ Proceedings of the Conference on Email and Anti-Spam, August 2008. Available: http://citeseerx.ist.psu.edu/ viewdoc/summary?doi=10.1.1.150.588 (last accessed: August 17, 2012).

15. Anoosha Prathapani, Lakshmi Santhanam, and Dharma P Agrawal. Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks. Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems, October 2009, pp. 753-758. URL: https://www.scirp.org/reference/referencespapers?referenceid=794111

16. Bedratyuk L., Savenko O. *MATCH Commun. Math. Comput. Chem.* 2018. № 79. Pp. 407–414.

17. A. H. Anwar, C. A. Kamhoua, N. O. Leslie and C. Kiekintveld, "Honeypot Allocation for Cyber Deception Under Uncertainty," in IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 3438-3452, Sept. 2022, doi: 10.1109/TNSM.2022.3179965.

18. Md Abu Sayed. Honeypot Allocation for Cyber Deception in Dynamic Tactical Networks: A Game Theoretic Approach/ Md Abu Sayed, Ahmed H. Anwar, Christopher Kiekintveld, Charles Kamhoua// arXiv:2308.11817v2 [cs.GT] 5 Sep 2023 https://doi.org/10.48550/arXiv.2308.11817

19. A. H. Anwar and C. A. Kamhoua, "Cyber Deception using Honeypot Allocation and Diversity: A Game Theoretic Approach," 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2022, pp. 543-549 doi: 10.1109/CCNC49033.2022.9700616.

20. A. H. Anwar, C. Kamhoua and N. Leslie, "Honeypot Allocation over Attack Graphs in Cyber Deception Games," 2020 International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, 2020, pp. 502-506 doi: 10.1109/ICNC47757.2020.9049764.

21. L. Huang and Q. Zhu, "Duplicity Games for Deception Design With an Application to Insider Threat Mitigation," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4843-4856, 2021 doi: 10.1109/TIFS.2021.3118886.

22. Ehab Al-Shaer. Autonomous Cyber Deception. Reasoning, Adaptive Planning, and Evaluation of HoneyThings/ Ehab Al-Shaer, Jinpeng Wei, Kevin W. Hamlen, Cliff Wang// Springer Nature Switzerland AG 2019 (eBook) https://doi.org/10.1007/978-3-030-02110-8

23. Almeshekah, M.H., Spafford, E.H. (2016). Cyber Security Deception. In: Jajodia, S., Subrahmanian, V., Swarup, V., Wang, C. (eds) Cyber Deception. Springer, Cham. https://doi.org/10.1007/978-3-319-32699-3_2

24. Q. D. La, T. Q. S. Quek, J. Lee, S. Jin and H. Zhu, "Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 1025-1035, Dec. 2016 doi: 10.1109/JIOT.2016.2547994

25. Çeker, H., Zhuang, J., Upadhyaya, S., La, Q.D., Soong, BH. (2016). Deception-Based Game Theoretical Approach to Mitigate DoS Attacks. In: Zhu, Q., Alpcan, T., Panaousis, E., Tambe, M., Casey, W. (eds) Decision and Game Theory for Security. GameSec 2016. Lecture Notes in Computer Science(), vol 9996. Springer, Cham. https://doi.org/10.1007/978-3-319-47413-7_2

26. Aggarwal, P., Du, Y., Singh, K., & González, C. (2021). Decoys in Cybersecurity: An Exploratory Study to Test the Effectiveness of 2-sided Deception. ArXiv, abs/2108.11037.

27. Rowe, N.C. (2019). Honeypot Deception Tactics. In: Al-Shaer, E., Wei, J., Hamlen, K., Wang, C. (eds) Autonomous Cyber Deception. Springer, Cham. https://doi.org/10.1007/978-3-030-02110-8_3

28. Valero, J.M., Pérez, M.G., Celdrán, A.H., & Pérez, G.M. (2020). Identification and Classification of Cyber Threats Through SSH Honeypot Systems. https://www.semanticscholar.org/paper/Identification-and-Classification-of-Cyber-Threats-Valero-P%C3%A9rez/f561f1122402acfc3bd01c33edbc6490125ef14a

29. Biswas J. Analysis of Client Honeypots. (IJCSIT) International Journal of Computer Science and Information Technologies. 2014. Vol. 5 (4). P. 5776-5780. https://ijcsit.com/docs/Volume%205/vol5issue04/ijcsit20140504209.pdf

30. Mukti, Fransiska Sisilia & Sukmawan, R.. (2021). Integration of Low Interaction Honeypot and ELK Stack as Attack Detection Systems on Servers. Jurnal Penelitian Pos dan Informatika. 11. 10.17933/jppi.v11i1.336.

31. Yamin, M.M., Katt, B., Sattar, K., & Ahmad, M.B. (2019). Implementation of Insider Threat Detection System Using Honeypot Based Sensors and Threat Analytics. Lecture Notes in Networks and Systems. https://www.semanticscholar.org/paper/Implementation-of-Insider-Threat-Detection-System-Yamin-Katt/67ebef836b3993a68f81840fd65ed0b37a9e5d6e

32. Mohammadzadeh, Hamid, Roza Honarbakhsh and Omar Bin Zakaria. "A Survey on Dynamic Honeypots." International Journal of Information Engineering and Electronic Business (2012): n. pag. https://www.semanticscholar.org/paper/A-Survey-on-Dynamic-Honeypots-Mohammadzadeh-Honarbakhsh/137a32a02099f767414b852b9fbecec7c15ddf75

33. Mohammed H. Almeshekah and Eugene H. Spafford. 2014. Planning and Integrating Deception into Computer Security Defenses. In Proceedings of the 2014 New Security Paradigms Workshop (NSPW '14). Association for Computing Machinery, New York, NY, USA, 127–138. https://doi.org/10.1145/2683467.2683482

34. Pingree, L. (2016). Emerging Technology Analysis : Deception Techniques and Technologies Create Security Technology Business Opportunities. https://www.semanticscholar.org/paper/Emerging-Technology-Analysis-%3A-Deception-Techniques-Pingree/945207097007a80c321277c903401c633e7b5fcd

35. Almeshekah, M.H., & Spafford, E.H. (2016). Cyber Security Deception. Cyber Deception. p. 25-52. https://www.semanticscholar.org/paper/Cyber-Security-Deception-Almeshekah-Spafford/101feca00418270ffbb5cda4884dc24ab0aaab22

36. Aggarwal, P., Gonzalez, C., Dutt, V. (2016). Cyber-Security: Role of Deception in Cyber-Attack Detection. In: Nicholson, D. (eds) Advances in Human Factors in Cybersecurity. Advances in Intelligent Systems and Computing, vol 501. Springer, Cham. https://doi.org/10.1007/978-3-319-41932-9_8

37. Pawlick, J., Colbert, E., & Zhu, Q. (2017). A Game-theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy. ACM Computing Surveys (CSUR), 52, 1 - 28. https://www.semanticscholar.org/paper/A-Game-theoretic-Taxonomy-and-Survey-of-Defensive-Pawlick-Colbert/47e558cd6c72e7292d7d686cdffaefe0e6e5fba2

37. Efendi, M.A., Ibrahim, Z.B., Zawawi, M.N., Rahim, F.A., Pahri, N.A., & Ismail, A. (2019). A Survey on Deception Techniques for Securing Web Application. 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), 328-331. https://www.semanticscholar.org/paper/A-Survey-on-Deception-Techniques-for-Securing-Web-Efendi-Ibrahim/d2c9acbda2145fe8860e81cdcc870486a560a3e6

38. Steingartner W, Galinec D, Kozina A. Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. Symmetry. 2021; 13(4):597. https://doi.org/10.3390/sym13040597

39. Li Y, Shi L, Feng H. A Game-Theoretic Analysis for Distributed Honeypots. Future Internet. 2019; 11(3):65. https://doi.org/10.3390/fi11030065

40. Aaron Schlenker, Omkar Thakoor, Haifeng Xu, Fei Fang, Milind Tambe, Long Tran-Thanh, Phebe Vayanos, and Yevgeniy Vorobeychik. 2018. Deceiving Cyber Adversaries: A Game Theoretic Approach. In Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS '18). International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 892–900. https://dl.acm.org/doi/10.5555/3237383.3237833

41. K. Wang, M. Du, S. Maharjan and Y. Sun, "Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid," in IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2474-2482, Sept. 2017, doi: 10.1109/TSG.2017.2670144.

42. Asaf Shabtai, Maya Bercovitch, Lior Rokach, Ya'akov (Kobi) Gal, Yuval Elovici, and Erez Shmueli. 2016. Behavioral Study of Users When Interacting with Active Honeytokens. ACM Trans. Inf. Syst. Secur. 18, 3, Article 9 (April 2016), 21 pages. https://doi.org/10.1145/2854152

43. S. Achleitner, T. F. La Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy and R. Chadha, "Deceiving Network Reconnaissance Using SDN-Based Virtual Topologies," in IEEE Transactions on Network and Service Management, vol. 14, no. 4, pp. 1098-1112, Dec. 2017, doi: 10.1109/TNSM.2017.2724239.

44. Reza Shokri. 2015. Privacy games: Optimal user-centric data obfuscation. Proc. Privacy Enhancing Technologies 2 (2015), 299–315. https://petsymposium.org/popets/2015/popets-2015-0024.pdf