DOI 10.31891/2307-5732-2024-337-3-42
УДК 004

ЯРОВИЙ РОМАН
Приватний вищий навчальний заклад «Європейський університет»
https://orcid.org/0000-0001-8978-8137
e-mail: roman.yaroviy@e-u.edu.ua
УЛІЧЕВ ОЛЕКСАНДР
Приватний вищий навчальний заклад «Європейський університет»
https://orcid.org/0000-0003-3736-9613
e-mail: o.ulichev@e-u.edu.ua
СКЛЯРЕНКО ОЛЕНА
Приватний вищий навчальний заклад «Європейський університет»
https://orcid.org/0000-0001-6555-1223
e-mail: olena.skliarenko@e-u.edu.ua
ПАШОРІН ВАЛЕРІЙ
Приватний вищий навчальний заклад «Європейський університет»
https://orcid.org/0000-0001-6165-1147
e-mail: v.pashorin@e-u.edu.ua

МОДЕЛЮВАННЯ МУЛЬТИАГЕНТНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Традиційні централізовані системи захисту інформації не забезпечують належного рівня адаптивності та ефективності в умовах динамічно змінюваного середовища загроз. Мультиагентні системи, маючи розподілену архітектуру та можливість автономного прийняття рішень, представляють собою перспективний напрямок для вирішення задач інформаційної безпеки.

Новизна дослідження полягає у розробці мультиагентної системи захисту інформації з розширеними можливостями аналізу вразливостей та виявлення вторгнень. На відміну від існуючих рішень, запропонована система забезпечує активний аналіз загроз, зниження кількості хибних спрацювань, адаптацію до нових видів атак та мінімізацію впливу на цільовий трафік інформаційних потоків.

У запропонованій формальній моделі та прототипі агентно-орієнтованої системи моделювання атак (АСМА) розподілені скоординовані атаки на комп'ютерну мережу розглядаються як послідовність спільних дій агентів-хакерів, які виконуються з різних хостів. Передбачається, що хакери координують свої дії відповідно до деякого загального сценарію. На кожному кроці сценарію атаки вони намагаються реалізувати певну приватну підціль.

Ключові слова: мультиагентні, системи захисту, інформаційні ресурси

YAROVOY ROMAN, ULICHEV ALEXANDER, SKLYARENKO OLENA, PASHORIN VALERIY
Private higher educational institution "European University"

SIMULATION OF MULTI-AGENT INFORMATION RESOURCES PROTECTION SYSTEMS

Traditional centralized information protection systems do not provide an adequate level of adaptability and efficiency in a dynamically changing threat environment. Multi-agent systems, having a distributed architecture and the possibility of autonomous decision-making, represent a promising direction for solving information security problems.

The novelty of the research lies in the development of a multi-agent information protection system with enhanced capabilities for vulnerability analysis and intrusion detection. Unlike existing solutions, the proposed system provides active analysis of threats, reduction of the number of false positives, adaptation to new types of attacks, and minimization of the impact on the target traffic of information flows.

In the proposed formal model and prototype of the agent-oriented attack modeling system (ASMA), distributed coordinated attacks on a computer network are considered as a sequence of joint actions of hacker agents, which are performed from different hosts. Hackers are supposed to coordinate their actions according to some common script. At each step of the attack scenario, they try to implement a specific private subgoal.

The developed agent-oriented attack modeling system (ASMA) allows simulating distributed coordinated attacks on computer networks. It is based on a hierarchy of grammars, each of which is interpreted as a finite automaton. The system takes into account both macro- and micro-levels of attack description, providing detailed simulation of each stage of the attack. The use of KQML for communication between agents and XML for describing the content of messages allows effective coordination of agents' actions and ensures realistic simulation of attacks.

Keywords: multi-agent, protection systems, information resources

Вступ

У зв'язку зі стрімким розвитком задач розподіленої обробки інформації та використанням відкритих мереж (Інтернету), не пристосованих для захищеного обміну інформацією, питання захисту інформаційних ресурсів у комп'ютерних системах набули виключної актуальності. Однак, нинішній стан у сфері забезпечення безпеки цих систем, зокрема у сфері побудови засобів захисту комп'ютерних мереж, залишає бажати кращого. Існуючі системи захисту інформаційних ресурсів у комп'ютерних мережах, як правило, мають централізовану структуру, характеризуються нерозвиненими адаптаційними можливостями, пасивними механізмами виявлення атак, великим відсотком хибних спрацювань при виявленні вторгнень, значною деградацією трафіку цільових інформаційних потоків через великий обсяг ресурсів, виділених на захист, тощо.

Перспективним підходом до побудови комплексних систем захисту інформації у комп'ютерних мережах, який дозволяє подолати деякі з перелічених недоліків, є використання інтелектуальних систем захисту інформації, що базуються на технології мультиагентних систем. Порівняно з традиційними методами, цей підхід дозволяє суттєво підвищити ефективність механізмів захисту інформації, зокрема їх оперативність, адекватність, відмовостійкість, стійкість до деструктивних дій, гнучкість тощо.

Ця робота присвячена розробці формальних моделей, архітектур та програмних реалізацій мультиагентних систем захисту інформації, які служать для аналізу вразливостей та виявлення вторгнень у комп'ютерні мережі. Розглянуто рішення щодо створення системи моделювання атак, призначеної для активного аналізу вразливостей комп'ютерних мереж, та системи виявлення вторгнень.

Цілі та задачі дослідження.

Метою даної роботи є розробка мультиагентної системи захисту інформації для комп'ютерних мереж, здатної ефективно виявляти та запобігати загрозам інформаційної безпеки. Для досягнення поставленої мети необхідно вирішити наступні задачі:

1. Провести аналіз існуючих методів та систем захисту інформації, виявити їх недоліки та переваги.
2. Розробити архітектуру мультиагентної системи захисту інформації, що включає модулі для аналізу вразливостей та виявлення вторгнень.
3. Розробити формальні моделі взаємодії агентів усередині системи, а також алгоритми прийняття рішень агентами.
4. Реалізувати програмне забезпечення для моделювання атак та виявлення вторгнень, основане на розробленій архітектурі та моделях.
5. Провести експериментальні дослідження розробленої системи, оцінити її ефективність та порівняти з існуючими рішеннями.

Актуальність та новизна дослідження

Актуальність дослідження обумовлена необхідністю підвищення рівня захищеності інформаційних ресурсів в умовах зростання кількості та складності кібератак. Традиційні централізовані системи захисту інформації не забезпечують належного рівня адаптивності та ефективності в умовах динамічно змінюваного середовища загроз. Мультиагентні системи, маючи розподілену архітектуру та можливість автономного прийняття рішень, представляють собою перспективний напрямок для вирішення задач інформаційної безпеки.

Новизна дослідження полягає у розробці мультиагентної системи захисту інформації з розширеними можливостями аналізу вразливостей та виявлення вторгнень. На відміну від існуючих рішень, запропонована система забезпечує активний аналіз загроз, зниження кількості хибних спрацювань, адаптацію до нових видів атак та мінімізацію впливу на цільовий трафік інформаційних потоків.

Загальне описання технології проектування, архітектури типового агента та схеми кооперації мультиагентних систем захисту інформації

Інтелектуальний агент – це програмно або апаратно реалізована система, яка має автономію, сукупність "ментальних властивостей" і здатна функціонувати в спільноті з іншими агентами. Виділяють наступні "ментальні властивості" агента:

Знання – постійна частина знань агента про себе, середовище та інших агентів, які не змінюються в процесі його функціонування.

Переконання – знання агента про середовище (зокрема, про інших агентів), які можуть змінюватися з часом і ставати неправильними.

Бажання – стани, досягнення яких з різних причин є бажаним для агента, однак вони можуть бути суперечливими, і тому агент не очікує, що всі вони будуть досягнуті.

Наміри – те, що агент або зобов'язаний зробити в силу своїх обов'язків по відношенню до інших агентів, або те, що випливає з його бажань (тобто несуперечлива підмножина бажань, обрана з тих чи інших причин і яка сумісна з прийнятими на себе зобов'язаннями).

Цілі – конкретне множина кінцевих і проміжних станів, досягнення яких агент прийняв як поточну стратегію поведінки.

Зобов'язання по відношенню до інших агентів – завдання, які агент бере на себе на прохання (доручення) інших агентів в рамках кооперативних цілей або цілей окремих агентів в рамках співробітництва.

Відповідно до розробленої в лабораторії інтелектуальних систем технології процес розробки мультиагентних систем для будь-якої предметної області, включаючи захист інформації в комп'ютерних мережах, передбачає вирішення двох високорівневих завдань:

1. Створення "Системного ядра" мультиагентної системи.
2. Клонування програмних агентів і відокремлення згенерованої мультиагентної системи від "Системного ядра".

Для специфікації "Системного ядра" використовуються два компоненти програмного інструментарію. Перший з них – це так званий "Типовий агент" ("Generic Agent"), який призначений для створення високорівневої специфікації класу агента. Другий компонент служить для формування

проблемно-орієнтованої архітектури застосування, заповнення даних, знань, а також визначення комунікаційного компонента.

Агенти, мають аналогічну архітектуру. Різниці відображаються у змісті даних і баз знань агентів. Кожен агент взаємодіє з іншими агентами, середовищем, яке сприймається і, можливо, змінюється агентами, а також користувачем, який спілкується з агентами через користувацький інтерфейс.

Архітектура типового агента

Архітектура типового агента включає наступні компоненти:

Буфер вхідних повідомлень – для фіксації отриманих повідомлень.

Буфер вихідних повідомлень – для фіксації відправлених повідомлень.

Процесор вхідного трафіку – для обробки отриманих повідомлень, синтаксичного аналізу, інтерпретації KQML-повідомлень та витягування змісту повідомлень.

База даних діалогів агента – зберігає атрибути кожного вхідного повідомлення (ідентифікатори, тип повідомлення, його джерело тощо).

Мета-автомат – керує семантичною обробкою вхідних повідомлень, направляючи їх для обробки відповідними автоматами. Крім того, цей компонент керує паралельним виконанням різних процесів в рамках агента.

Автомати – виконують базові обчислення агента, які визначені його роллю в мультиагентній системі, реалізуючи різні сценарії обробки вхідних повідомлень.

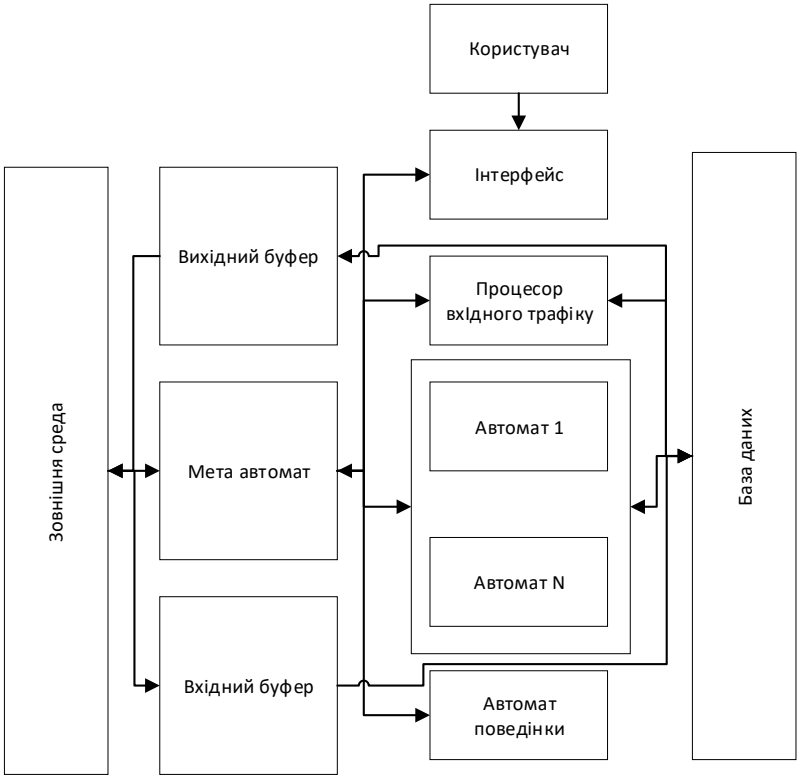

Рис 1. Архітектура типового агента

Кожен клас агентів має певний набір шаблонів повідомлень, визначених на мові KQML. Розробник виконує процедуру спеціалізації за допомогою компонента MASDK, званого Редактором шаблонів повідомлень, призначаючи кожному шаблону відповідний KQML-перформатив. Комунікаційний компонент кожного агента включає дані про потенційних адресатів повідомлень даного шаблону. Зміст повідомлень визначається на XML.

Схема кооперації мультиагентних систем захисту інформації

Програмний код мультиагентних систем захисту інформації, таких як агентно-орієнтована система моделювання атак (АСМА) та мультиагентна система виявлення вторгнень (МСОВ), написаний з використанням інструментарію MASDK, Visual C++, JAVA 2 та засобів розробки XML.

АСМА імітує вхідний трафік, тобто комбінацію потоків як нормальних, так і аномальних подій. Потік аномальних подій задає атаки на комп'ютерну мережу. Вхідний трафік аномальних подій відповідає послідовностям "однофазних" атак, які використовують різні хости як "точки входу ініціювання" атак.

МСОВ відповідає за виявлення атак на комп'ютерну мережу, сформованих АСМА. В експериментах з цими системами використовуються різні конфігурації комп'ютерної мережі. Ця мережа може включати кілька різних сегментів, і вхідний трафік може формуватися як всередині, так і ззовні захищеної мережі. Припускається, що зловмисники можуть знаходитися в різних точках мережі, як ззовні, так і всередині захищеного фрагмента мережі.

Таким чином, мультиагентні системи захисту інформації надають можливість більш ефективно виявляти та запобігати загрозам, завдяки розподіленій архітектурі, автономності агентів та їх здатності до кооперації та адаптації в динамічно змінюваних умовах.

Агентно-орієнтована система моделювання атак на комп'ютерні мережі

У запропонованій формальній моделі та прототипі агентно-орієнтованої системи моделювання атак (АСМА) розподілені скоординовані атаки на комп'ютерну мережу розглядаються як послідовність спільних дій агентів-хакерів, які виконуються з різних хостів. Передбачається, що хакери координують свої дії відповідно до деякого загального сценарію. На кожному кроці сценарію атаки вони намагаються реалізувати певну приватну підціль.

Таким чином, загальний сценарій розподіленої атаки задається як впорядкована у часі послідовність кроків, спрямованих на послідовне досягнення мети команди хакерів. При реалізації складних скоординованих атак, залежно від встановленої загальної мети атаки, спеціально призначений мета-агент (агент-лідер) обирає загальний сценарій атаки та призначає сфери відповідальності іншим агентам. Агенти, відповідальні за окремі фрагменти (кроки) загального сценарію, можуть, у свою чергу, "наймати" інших агентів або здійснювати реалізацію окремих дій самостійно. Для цього призначені спеціальні сценарії (плани) дій та протоколи обміну повідомленнями.

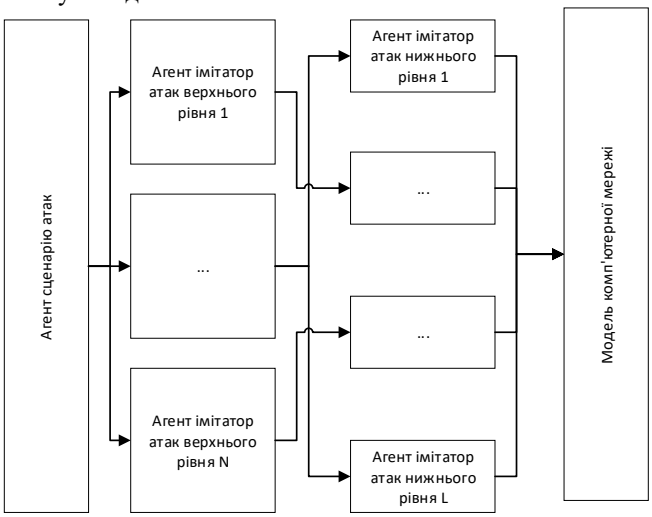

Рис2. Ієрархія атак

Сценарій задається у вигляді послідовності намірів (підцілей) і способів їх досягнення (дій), які можуть описуватись на різних рівнях деталізації. Намірі самого нижнього рівня реалізуються конкретними діями, які виражаються у вигляді мережевих пакетів, команд операційної системи або операцій з конкретним додатком.

Базові класи високорівневих намірів хакерів

Виділяються наступні базові класи високорівневих намірів хакерів:

1. Розвідка:
   - Визначення функціонуючих хостів
   - Ідентифікація служб хоста
   - Ідентифікація типу операційної системи хоста
   - Визначення спільних ресурсів
   - Визначення облікових записів користувачів і груп
   - Визначення додатків і заголовків
2. Внедрення та реалізація загрози:
   - Отримання доступу до ресурсів хоста
   - Отримання розширеного доступу до ресурсів хоста
   - Порушення конфіденційності
   - Порушення цілісності
   - Порушення доступності
   - Створення потайних ходів
   - Приклад сценарію атаки

Загальний сценарій атаки може включати наступні кроки

1. Розвідка:
   - Визначення працюючих хостів у цільовій мережі.
   - Ідентифікація служб, що працюють на визначених хостах.
2. Визначення операційних систем на хостах.
   - Внедрення загрози:

- Отримання початкового доступу до хоста через вразливу службу.
- Розширення доступу, отримання привілеїв адміністратора.
- Встановлення бекдорів для забезпечення постійного доступу.
- Викрадення конфіденційної інформації або її зміна.

Кожен крок реалізується через послідовність дій агентів, які координуються мета-агентом. Це дозволяє моделювати складні атаки і визначати ефективні стратегії захисту.

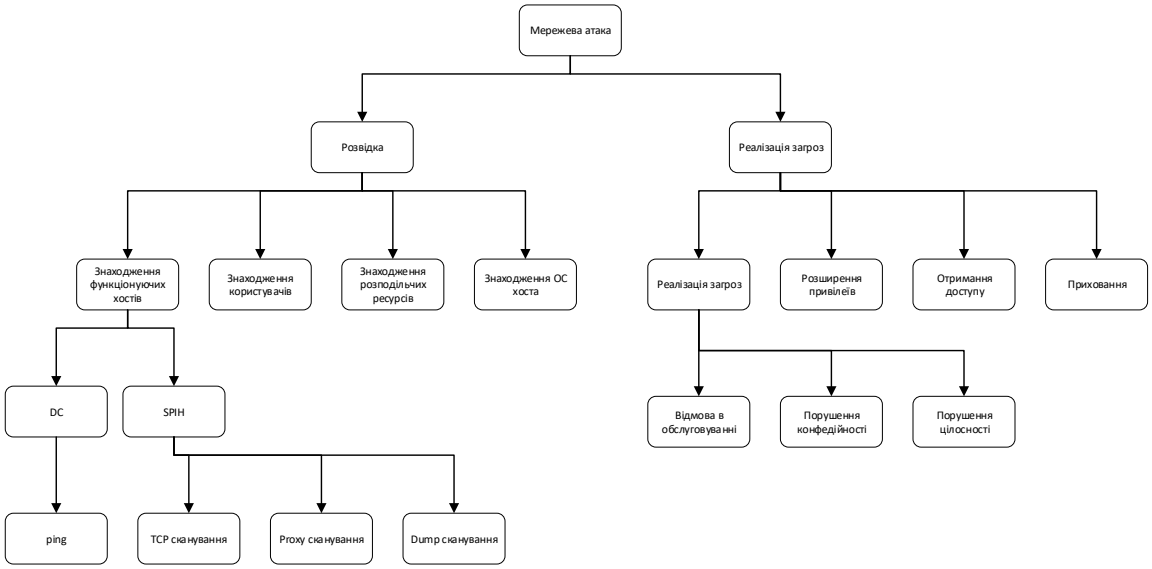

Рис 3. Фрагмент мережевої атаки

Використання у експериментах

Використовується для імітації вхідного трафіку, що включає як нормальні, так і аномальні події. Аномальні події представляють собою атаки на комп'ютерну мережу. Вхідний трафік формується як всередині, так і ззовні захищеної мережі, що дозволяє моделювати різні сценарії атак і тестувати ефективність захисних механізмів.

Таким чином, агентно-орієнтована система моделювання атак (АСМА) забезпечує гнучке і потужне середовище для дослідження, тестування і вдосконалення методів захисту інформації в комп'ютерних мережах.

Агентно-орієнтована система моделювання атак на комп'ютерні мережі

В агентно-орієнтованій системі моделювання атак (АСМА) розподілені скоординовані атаки на комп'ютерну мережу розглядаються як послідовність спільних дій агентів-хакерів, які виконуються з різних хостів. Хакери координують свої дії відповідно до загального сценарію, на кожному кроці якого вони намагаються досягти певної підцілі.

Специфікація задачі зловмисника

Задача зловмисника (або групи зловмисників), що визначає підмножину сценаріїв, які ведуть до досягнення мети атаки, специфікується наступною четвіркою:

1. Адреса мережі (хоста) – ціль атаки.
2. Намір.
3. Параметри мережі (хоста), відомі зловмисникам.
4. Об'єкт атаки.

Специфікації атак зберігаються в розподіленій базі знань агентів, яка спільно використовується агентами та структурована відповідно до розробленої онтології предметної області «Атаки на комп'ютерні мережі».

Онтологія атак на комп'ютерні мережі

Онтологія являє собою ієрархію взаємопов'язаних понять, що описують дії хакерів з реалізації мережевих атак різних класів на різних рівнях деталізації та відносин між такими поняттями. Ієрархія узлів (понять) онтології поділяється на два підмножини відповідно до макро- та мікрорівневого опису атак.

На макрорівні загальний сценарій атаки моделюється множиною допустимих послідовностей скоординованих дій одного або декількох хакерів. На мікрорівні детально описується атака, де кожен крок макрорівневого сценарію представлений послідовністю подій на мікрорівні.

Кожному узлу онтології відповідає або підціль, яку намагається досягти хакер (його намір), або набір дій, за допомогою яких певна підціль може бути досягнута.

Приклад онтології макрорівня

Розглянемо фрагмент розробленої онтології, описуючи поняття макрорівня. На макрорівні поняття онтології вищого рівня пов'язані з відповідними поняттями суміжного нижчого рівня через три види відносин:

1. Part of – відношення декомпозиції («Ціле – частина»).
2. Kind of – відношення спеціалізації («Поняття – клас поняття»).
3. Seq of – відношення порядку виконання («Операція – етап реалізації»).

Специфікація планів реалізації розподілених атак

Специфікація планів реалізації розподілених атак задається з використанням контекстно-вільних атрибутних стохастичних граматик, пов'язаних між собою операцією підстановки. Послідовності символів, що виводяться в кожній із таких граматик, відповідають або опису множини сценаріїв атаки, що ведуть до досягнення заданої кінцевої мети хакера, або опису певного типу атаки.

Приклад граматики для опису атак

Кожна граматика задається у вигляді п'ятірки:

$G(C)$={VN,VT,S,P,A}G(C)={VN,VT,S,P,A},

де:

C – ім'я граматики.

VN – нетермінальні символи.

VT – термінальні символи.

S – початковий нетермінальний символ (аксіома).

P – продукції граматики.

A – атрибути та правила їх обчислення.

Кожна продукція з P задається у вигляді:

[(U)]$X\rightarrow\alpha$($Prob$)[(U)]X→α(Prob)

де:

U – умова застосовності продукції залежно від передісторії атаки до поточного кроку.

[] – позначають необов'язковість елемента U.

X – нетермінальний символ.

α – послідовність термінальних і нетермінальних символів.

Prob – початкова ймовірність вибору правила.

Атрибути граматики

Атрибутний компонент A граматики служить для завдання ймовірностей вибору чергової підстановки і умов застосовності продукцій залежно від передісторії атаки. Ймовірності, призначені продукціям, забезпечують необхідне різноманіття генерованих атак і керують вибором чергової підстановки в разі неоднозначності вибору.

Таким чином, операція підстановки граматик реалізує механізм багаторівневого опису атаки, дозволяючи ефективно моделювати та аналізувати складні сценарії атак на комп'ютерні мережі.

Агентно-орієнтована система моделювання атак на комп'ютерні мережі

Основні компоненти та їх функції

У розробленій системі моделювання атак (АСМА) кожній граматиці відповідає кінцевий автомат, що є основою алгоритмічної інтерпретації процедур генерації атак. Основні елементи автомата включають:

Стан: початкові, проміжні та кінцеві (з міткою "End").

- Дуги переходів: відповідають правилам підстановки граматик.
- Параметри та умови переходів.
- Скрипти дій: реалізують конкретні дії.

Стан кожного автомата поділяється на три типи:

- Початкові.
- Проміжні:
- Нетермінальні: ініціюють роботу вкладених автоматів.

Термінальні: взаємодіють з моделлю хоста.

- Абстрактні (вспомогательні): не ініціюють роботу інших автоматів і не взаємодіють з моделлю хоста.
- Кінцеві.

Взаємодія агентів у системі

Агенти-хакери функціонують в антагоністичній середовищі, де підсистеми захисту атакованої мережі намагаються перешкодити атаці, виявити її та нейтралізувати діяльність агентів-хакерів. Розвиток атаки залежить від результатів кожного кроку атаки, зібраної інформації про об'єкт атаки, та успіху чи неуспіху попередніх дій.

Компоненти АСМА

Програмний прототип АСМА складається з наступних компонентів:

- Множина агентів-хакерів: кожен агент моделює окремого атакуючого.
- Агент-модель атакованої комп'ютерної мережі.
- Генератор фонових «нормальних» трафіків.

Комунікація агентів

Агенти обмінюються повідомленнями для координації дій. Мовою обміну повідомленнями є KQML, а зміст повідомлень задається в термінах XML. Приклад реалізації дії "отримання доступу до

ресурсів хоста" (GAR) на етапі розвідки після виконання дії EUE ("Визначення записів користувачів та груп утилітою enum") представлено на рисунку.

Дані про реалізовану атаку розбиваються на чотири групи:

- Ліва верхня частина екрана: елементи специфікації задачі атакуючого.
- Права частина екрану: візуалізується дерево генерації атаки.
- Ліва частина екрану нижче специфікації задачі: рядки згенерованих дій зловмисника.
- Права частина екрану: ознака успіху (неуспіху) у вигляді зеленого (чорного) квадрата і дані, отримані від атакованого хоста.

Невизначеність у виборі сценарію атаки

Вибір продовження атаки зазвичай недетермінований, тобто сценарій атаки не може бути визначений заздалегідь. Це означає, що розвиток атаки змінюється в залежності від зібраної інформації та результатів попередніх дій.

Висновок

Розроблена агентно-орієнтована система моделювання атак (ACMA) дозволяє моделювати розподілені скоординовані атаки на комп'ютерні мережі. Вона базується на ієрархії граматик, кожна з яких інтерпретується у вигляді кінцевого автомата. Система враховує як макро-, так і мікрорівні опису атак, забезпечуючи детальне моделювання кожного етапу атаки. Використання KQML для комунікації між агентами та XML для опису змісту повідомлень дозволяє ефективно координувати дії агентів і забезпечувати реалістичність моделювання атак.

Література

1. Lakhno, V.A., Kasatkin, D.Y., Skliarenko, O.V., Kolodinska, Y.O. Modeling and Optimization of Discrete Evolutionary Systems of İnformation Security Management in a Random Environment // Machine Learning and Autonomous Systems. Smart Innovation, Systems and Technologies, vol 269. Springer, Singapore. – 2022 – p. 9-22.

2. Невзоров А.В., Скляренко О.В., Колодінська Я.О., Яровий Р.О. Особливості аналітичного забезпечення експлуатації інформаційних систем та обладнання у сучасних умовах. Прикладні питання математичного моделювання. Т.6.№ 1. 2023. DOI: https://doi.org/10.32782/mathematical-modelling/2023-6-1-13

3. Невзоров А.В. Моделі оцінки структурної живучості та надійності комп'ютерних мереж/ А.В. Невзоров, О.В. Скляренко, Я.О. Колодінська, О.Ю. Ніколаєвський// Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах», № 3, 2023. – с. 164-169.

4. Скляренко О. В. Економіко-математичне моделювання: Навч. посібник / О. В. Скляренко, Г. М. Терещук, Я. О. Колодінська. – К.:: Вид-во Європейського університету, 2024. – 200 с.

References

1. Lakhno, V.A., Kasatkin, D.Y., Skliarenko, O.V., Kolodinska, Y.O. Modeling and Optimization of Discrete Evolutionary Systems of İnformation Security Management in a Random Environment // Machine Learning and Autonomous Systems. Smart Innovation, Systems and Technologies, vol 269. Springer, Singapore. – 2022 – p. 9-22.

2. Nevzorov A.V., Skliarenko O.V., Kolodinska Ya.O., Yarovyi R.O. Osoblyvosti analitychnoho zabezpechennia ekspluatatsii informatsiinykh system ta obladnannia u suchasnykh umovakh. Prykladni pytannia matematychnoho modeliuvannia. T.6.№ 1. 2023. DOI: https://doi.org/10.32782/mathematical-modelling/2023-6-1-13

1. Nevzorov A.V. Modeli otsinky strukturnoï zhyvuchosti ta nadiĭnosti komp'iuternykh merezh/ A.V. Nevzorov, O.V. Skliarenko, Ya.O. Kolodinska, O.Iu. Nikolaievskyi// Mizhnarodnyi naukovo-tekhnichnyi zhurnal «Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh», № 3, 2023. – s. 164-169.

2. Skliarenko O. V. Ekonomiko-matematychne modeliuvannia: Navch. posibnyk / O. V. Skliarenko, H. M. Tereshchuk, Ya. O. Kolodinska. – K.:: Vyd-vo Yevropeiskoho universytetu, 2024. – 200 s.