УДК 004.056.53:621.391

ДОСЛІДЖЕННЯ ПІДХОДІВ ДО ВІЗУАЛІЗАЦІЇ І СТРУКТУРИЗАЦІЇ АТАК У КОНТЕКСТІ МОДЕЛЮВАННЯ ДІЙ ЗЛОВМИСНИКІВ В ІНФОКОМУНІКАЦІЙНІЙ МЕРЕЖІ

Фукс М.А.
e-mail: maksymillian.fuks@nure.ua
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського
м. Харків, Україна

This work is devoted to analyzing modern approaches to representing attacks for the purpose of modeling adversarial actions and assessing system security. It is vital to adopt robust models for analyzing potential scenarios, identifying system vulnerabilities, and effectively prioritizing countermeasures. This work focuses on three primary approaches to representing attacks: attack trees, attack graphs, and matrix-based models. By examining each model's capabilities, the paper highlights the importance of selecting or combining appropriate approaches to gain insights into attacker behavior and enhance security posture.

У результаті проведеного аналізу сучасних підходів до представлення атак для моделювання дій зловмисників та аналізу захищеності систем було визначено три основні види: дерева атак, класичні графи атак та матричне представлення.

У деревах атак забезпечується доволі високий ступінь деталізації та можливість введення оцінок за деякими критеріями, але ця структура не може бути використана для моделювання атак, оскільки не надає засобів динамічного моделювання, введення у модель умов зовнішнього впливу та не забезпечує вибору наступного етапу на підставі результатів попереднього [1]. Згідно з визначенням, одне дерево спроможне моделювати один конкретний сценарій атаки або загрозу у структурований і зрозумілий спосіб, фокусуючись на досягненні визначеної цілі.

На відміну від дерев, граф атак є більш загальною, мережевою моделлю, що відображає всі можливі шляхи багатоетапної атаки в межах складної системи або мережі. Аналіз показав, що можна виділити декілька видів графів атак, кожен із цих видів відрізняється способом представлення взаємозв'язків між атаками та їхніми наслідками: state enumeration graph, condition-oriented dependency graph, exploit dependency graph.

Таким чином прослідковується відмінності між графами атак та деревами атак: перші охоплюють багато цілей і шляхів одночасно, з можливістю комбінації вразливостей, відображаючи загальний стан мережевої безпеки і можливі ланцюжки атак, у тому числі каскадні ефекти та можливі побічні шляхи, однак дерева атак, у свою чергу, фокусуються на одному сценарії або вразливості, не здатні моделювати динамічні зміни мережі, забезпечують більш чіткий, проте локальний аналіз загрози.

Проведене дослідження за критерієм аналізу дерева і графу та можливістю застосування кількісної оцінки ризиків, показало, що дерева атак зручно доповнювати логікою AND/OR, вводити ймовірності чи надавати ваги ребрам. Графи атак дають можливість оцінювати глобальну безпеку мережі, виявляти усі потенційні шляхи компрометації, проте для кількісної оцінки застосовують більш складні алгоритми: байєсівські мережі, марковські процеси, методи пошуку у графах, теорію ігор тощо.

Ще один спосіб організувати знання про атаки – матричне представлення у вигляді двовимірної матриці. Найвідомішим прикладом може слугувати матриця MITRE ATT&CK [2] і модель Cyber Kill Chain [3] від Lockheed Martin, що лінійно зображує етапи атаки. Проведений аналіз показав, що матричні моделі не відображають конкретних шляхів або послідовностей атак, а скоріше каталогізують можливі дії зловмисника, тому їх зручно використовувати для класифікації спостережуваної активності та співвіднесення її з відомими використовуваними зловмисниками методами. Доречним є моделювання повних послідовностей атак у вигляді графів щоб врахувати взаємозв'язки між кроками, що розглядаються, а не просто каталогування технік матричними моделями.

Згадані вище підходи слід адаптувати з урахуванням динамічного характеру інфокомунікаційних мереж. Наприклад, графи атак можуть ефективно використовуватися для глобальної оцінки безпеки мережевих інфраструктур, де одночасно існують різноманітні вразливості і потенційні вектори атак, а матриця ATT&CK спроможна допомогти систематизувати відомі методи нападу на різних рівнях мережевої взаємодії.

Отже, кожен із проаналізованих підходів візуалізації і структуризації дій зловмисників має власну структуру та призначення: дерева атак ефективні для деталізації певного сценарію й простої кількісної оцінки ризику, а матричні моделі систематизують і класифікують відомі техніки, тож їх варто використовувати як доповнення при моделюванні реальних послідовностей атак графами, які дають найбільш цілісне охоплення безпеки мережі та спроможні виявляти всі потенційні вектори уразливості.

Список використаних джерел:

1. Толюпа С., Пархоменко І., Штаненко С. Модель системи протидії вторгненням в інформаційних системах. *Інфокомунікаційні технології та електронна інженерія*. 2021. Т. 1, № 1. С. 39–50. URL: https://science.lpnu.ua/sites/default/files/journalpaper/2021/dec/25671/statya4stolyupaiparhomenkosshtanenko.pdf (дата звернення: 26.02.2025).

2. MITRE ATT&CK®. *MITRE ATT&CK®*. URL: https://attack.mitre.org(дата звернення: 02.03.2025).