УДК 004.77.056

СИСТЕМАТИЗАЦІЯ ПІДХОДІВ ДО КІЛЬКІСНОЇ ОЦІНКИ МЕРЕЖЕВОЇ БЕЗПЕКИ З ВИКОРИСТАННЯМ ГРАФІВ АТАК

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

Attack graphs are widely used for modeling multi-step intrusions in computer networks and for developing quantitative security metrics. This paper proposes a taxonomy of approaches to the quantitative assessment of network security based on attack graphs, developed through the analysis of contemporary research. The taxonomy classifies existing approaches according to the type of attack graph model, the type of security metrics, the temporal aspect of assessment, and the intended purpose of the metrics. The proposed classification provides a systematic view of existing solutions and highlights directions for further research in quantitative network security analysis.

Сучасні комп'ютерні мережі є складними розподіленими системами, які постійно піддаються різноманітним кіберзагрозам. Значна частина атак реалізується у вигляді багатокрокових сценаріїв, що експлуатують комбінації вразливостей на різних вузлах мережі. Для формального моделювання таких сценаріїв широко використовуються графи атак, які дозволяють описувати можливі шляхи ескалації привілеїв з урахуванням топології мережі, конфігурації хостів та відомих вразливостей [1]. Важливим напрямом досліджень є розробка кількісних метрик мережевої безпеки на основі графів атак, які дають змогу оцінювати рівень захищеності системи, порівнювати різні конфігурації мережі та підтримувати прийняття рішень щодо впровадження контрзаходів [2].

Попри значну кількість досліджень, відсутня уніфікована систематизація кількісних підходів до оцінювання мережевої безпеки, що ускладнює їх практичне застосування. Тому актуальною є побудова таксономії таких підходів на основі графів атак [3].

На основі проведеного аналізу запропоновано таксономію підходів до кількісної оцінки мережевої безпеки, що ґрунтується на чотирьох ключових вимірах класифікації. Перший вимір визначає тип графової моделі, яка використовується, зокрема станові графи атак, експлойт-залежні графи, баєсівські графи та марковські моделі [1]. Окрему групу становлять атач-дерева та їх розширення, що поєднують графові структури з логічними операторами для моделювання взаємодії атак і контрзаходів.

Другий вимір таксономії пов'язаний із типом метрик безпеки, що обчислюються на графах атак. У дослідженнях використовуються структурні метрики, які базуються на топологічних характеристиках графа; ймовірнісні метрики, що враховують імовірність успішної експлуатації

вразливостей; економічні або ризик-орієнтовані метрики, які поєднують оцінки ймовірності атак із потенційними втратами та вартістю контрзаходів; а також комбіновані метрики мережевої безпеки.

Третій вимір таксономії пов'язаний із урахуванням часових аспектів у моделі оцінювання безпеки. Існуючі підходи можна умовно поділити на статичні та динамічні. Статичні метрики оцінюють безпеку для фіксованої конфігурації мережі, тоді як динамічні моделі враховують зміну стану вразливостей, появу експлойтів, а також еволюцію загроз у часі. До таких підходів належать моделі, що використовують розширення CVSS, марковські процеси з часовими параметрами та баєсівські моделі для динамічного аналізу сценаріїв атак.

Четвертий вимір таксономії визначається цільовим призначенням метрик безпеки. У цьому контексті метрики можуть застосовуватися для оцінювання загального рівня захищеності мережевої конфігурації, для підтримки вибору та оптимізації контрзаходів, а також для аналізу інцидентів і підвищення ситуаційної обізнаності у системах управління інформаційною безпекою.

Запропонована таксономія дозволяє систематизувати існуючі підходи до оцінювання мережевої безпеки. Встановлено, що структурні метрики є обчислювально простими, але не враховують реалістичні характеристики експлуатації вразливостей, тоді як ймовірнісні та марковські моделі забезпечують точнішу оцінку ризику, проте потребують надійних статистичних даних. Економічні моделі дозволяють враховувати бюджетні обмеження та оптимізувати вибір контрзаходів, а динамічні підходи – зміни стану мережі у часі. Водночас більшість існуючих моделей мають обмеження щодо масштабованості, якості вхідних даних та інтеграції з експлуатаційними характеристиками мережі [2-3]. Отримані результати можуть бути використані для розроблення комбінованих метрик безпеки та подальших досліджень у цій галузі.

Список використаних джерел:

1. Aslanyan L. H., Alipour D., Heidari M. Comparative analysis of attack graphs. *Mathematical problems of computer science*. 2013. Т. 40. С. 85–95.

2. Purboyo T. W. Attack graph based security metrics: state of the art. *International journal of science and engineering investigations*. 2012. Т. 1, № 7. С. 18–21.

3. Kaynar K. A taxonomy for attack graph generation and usage in network security. *Journal of information security and applications*. 2016. Т. 29. С. 27–56. URL: https://doi.org/10.1016/j.jisa.2016.02.001