CPNTools Usage in Tasks of Information Security Risk Assessment

Nechypor Vitaliy

Information Security Department, Lviv Polytechnic National University, UKRAINE, Lviv, 12, S. Bandery Str.
E-mail: nechypor.vv@gmail.com

The work is devoted to research of simulation mathematical modeling methods concerning the application in problems of information security risk assessment of secure enterprise communication networks (ЗКМЗ, SECN - secure enterprise communication networks). The use of the mathematical apparatus for the tasks of analysis and examination of SECN allow to receive important information about the structure and investigate the dynamic behavior of the system, to identify dangerous areas, to study the potential consequences of attacker intervention.

The objective of the research is to investigate and selection of efficient simulative mathematical modeling, to present the possibilities of mathematical apparatus for the tasks of security and optimization SECN.

We conducted the simulation of malicious attack process on the communications center SECN (Fig. 1). To describe the behavior of the attacker and the evaluation of possible consequences effects as a result of the unauthorized intervention, we used method of attacks tree, which allows to can take into account the combined effect of the use of system vulnerabilities and their dependence on each other. On the basis of expert assessments of the security systems units (transitions in the theory of Petri nets) Time and financial costs of their overcoming were brought to conformity by means of simulation modeling CPNTools (Fig. 2).

Compatible using of the approach based on "the least resistance" together with methods for evaluating of susceptibility to threats allows to determine the most sensitive parts of system protection and predict the emergence of vulnerabilities in the future.

During the simulation modeling it was found that SECN with the default configuration of system security isn't safe, the information can be easily reached.

This approach to risk assessment of information system allows on the initial stages of projecting to determine the most vulnerable parts of the system and on the base of received information to develop an action plan to ensure the informational security of the assets.

*Переклад виконано Малиновською О. А., центр іноземних мов «Universal Talk», **www.utalk.com.ua***

Використання CPNTools в задачах оцінки ризиків інформаційної безпеки

Віталій Нечипор

Кафедра захисту інформації, Національний університет "Львівська політехніка", УКРАЇНА,
м.Львів, вул. Кн.Романа, 1,
E-mail: nechypor.vv@gmail.com

Робота присвячена дослідженню методів імітаційного математичного моделювання на предмет застосування в задачах оцінки ризиків інформаційної безпеки захищених корпоративних мереж зв'язку (ЗКМЗ).

Ключові слова – оцінка ризиків, імітаційне моделювання, мережі Петрі, CPNTools, дерево атак.

I. Вступ

Впровадження математичного апарату в задачах аналізу та дослідження моделі порушника (загроз) ЗКМЗ дає змогу детальніше проаналізувати потенційно небезпечні ділянки ЗКМЗ, отримати важливу інформацію про структуру та динамічну поведінку ЗКМЗ, виявити фактори, що зумовлюють реалізацію загроз, на основі кількісних оцінок співставити ризик дослідженої системи з ризиками альтернативних систем або технологій, розробити план технічних та організаційних заходів захисту. В статті визначено особливості основних математичних моделей поведінки порушника, представлено переваги системи імітаційного математичного моделювання CPNTools [http://cpntools.org/], для наочності проведено моделювання процесу атаки зловмисника на вузол зв'язку ЗКМЗ.

II. Виклад основного матеріалу

На сучасному етапі розвитку інформаційних систем важливою частиною заходів захисту при побудові та дослідженні моделі загроз постає завдання отримання кількісної оцінки ризиків, що здатна оцінити адекватність затрат на їх мінімізацію та продемонструвати керівництву організації процес та результат зниження ризиків інформаційної безпеки, порівняти поточний рівень захисту з попереднім.

Аналіз останніх досліджень і публікацій. Проблемі оптимізації побудови імітаційних моделей з метою динамічного дослідження реальних систем присвячені роботи таких вітчизняних і закордонних авторів: Девянин П.М., Дудикевич В.Б., Малюк А.А., Павлов В.А., Пятунин А.Н, Хорошко В.О. Дослідженням моделювання поведінки зловмисника у корпоративній мережі з використання апарату мереж Петрі-Маркова займаються науковці Цибулин А.М., Шипилева А.В.

Метою роботи є дослідження та вибір ефективної системи імітаційного математичного моделювання, представлення можливостей математичного апарату в задачах захисту та оптимізації КМЗ.

Дослідження динамічних процесів у ЗКМЗ проводять на її математичному еквіваленті – імітаційній

моделі. При побудові адекватної моделі використовується такий математичний апарат: теорія графів, теорія масового обслуговування, марківські процеси, теорія мереж Петрі, штучні нейронні мережі. Використання мереж Петрі дає змогу представити систему як чітку причинно-наслідкову послідовність. Чітка математична формалізація мереж дозволяє проводити моделювання на обчислювальній техніці, можливість моделювання паралельних непов'язаних між собою процесів зумовила широке застосування мереж Петрі при аналізі систем.

В роботі проведено імітаційне математичне моделювання процесу отримання авторизації користувачем та процес атаки зловмисника на вузол зв'язку ЗКМЗ. В якості метода аналізу ланки інформаційної системи було використано метод дерева атак, перевагами якого є універсальність, наочність та гнучкість при побудові моделей захищених інформаційних систем.

Дерево атак представлене у вигляді дводольного графа (рис. 1), у вершини якого замикаються варіанти атак для досягнення поставленої зловмисником цілі. Для кожної загрози будується власне дерево, кожен вузол дерева є можливою проміжною ціллю зловмисника і згідно з синтаксисом мереж Петрі позначається як позиція, дії зловмисника відповідать переходам у теорії мереж Петрі [1]. Для отримання кількісної оцінки кожній ланці системи ставиться у відповідність еквівалент часових та фінансових ресурсів, які необхідно затратити для подолання системи захисту. На основі отриманих даних про можливу поведінку зловмисника визначаються найвразливіші місця та приймається рішення про проведення відповідних заходів захисту.

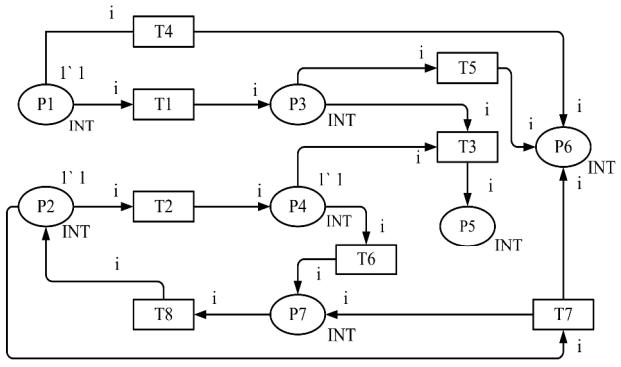

Рис. 1.Модель дерева атак

Замість ймовірності використання тої чи іншої вразливості зловмисником враховується вартість та час проходження з одного вузла в інший (рис. 2). Шляхом багаторазового моделювання визначається найкоротший шлях до поставленої цілі (підхід на основі «найменшого опору»), що дозволяє визначити пріорітетні напрямки захисту та передбачити можливі наслідки.

Система імітаційного моделювання CPNTools дає змогу службі захисту інформації поставити у відповідність кожному переходу власну затримку проходження. У випадку І, АБО декомпозицій дерева вразливостей використано логічні оператори з такими булевими операціями: not b, b1 orelse b2, b1 andelso b2 [2].

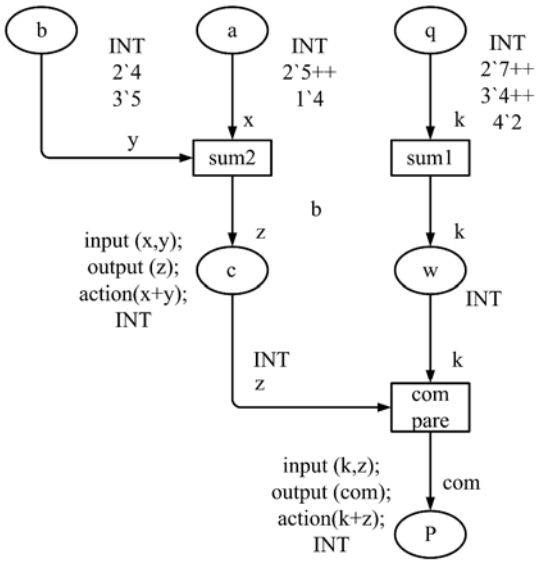

Рис. 2. Модель подолання зловмисником системи захисту

В процесі моделювання Було виявлено, що ЗКМЗ із заданою конфігурацією системи захисту не є безпечною, час проходження зловмисником системи захисту менший за час життя інформації, а отже мережа потребує вжиття додаткових заходів захисту. Запропоновано реалізувати систему-приманку (honeypot), яка забезпечує навчання ЗКМЗ за рахунок аналізу типових дій зловмисника та використання і впровадження відповідних методів та засобів захгшощисту.

Висновок

В роботі досліджено аспекти використання математичного апарату в задачах моделювання ЗКМЗ, наведено основні переваги теорії кольорових мереж Петрі та за допомогою програми імітаційного математичного моделювання CPNTools продемонстровано процес атаки зловмисника на захищений вузол зв'язку. Такий підхід, на відміну від інших (OCTAVE, ISO 13335, PCI DSS, Digital Security) до оцінки ризиків інформаційної безпеки дає змогу службі захисту інформації на етапі розроблення системи менеджменту інформаційної безпеки проводити динамічну ефективну оцінку активів, вразливостей, ризиків.

Література

[1] Moore A. P. Attack Modeling for Information Security and Survivability / A. P. Moore, R. J. Ellison, R. C. Linger. – Carnegie Mellon University, 2001.

[2] Зайцев Д. А. Моделирование телекоммуникационных систем в CPN Tools / Д. А. Зайцев, Т. Р. Шмелева. – Одесская национальная академия связи им. А. С. Поповы, 2008. – 68 с.