УДК 004.94: 004.428

МОДЕЛЮВАННЯ ПОШИРЕННЯ КІБЕРАТАК В РОЗПОДІЛЕНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

В.В.Литвинов , І.В. Стеценко

Чернігівський національний технічний університет, Україна
Національний технічний університет України «Київський політехніч-ний інститут імені Ігоря Сікорського», Україна

Питання інформаційного захисту є надзвичайно актуальним в зв'язку зі зростанням кількості кіберзлочинів та масштабів шкоди, які спричиняють атаки, спрямовані на державні та фінансові установи, об'єкти енергетичної системи та об'єкти підвищеної небезпеки. Дослідження кіберзлочинів поступово переходять зі стану накопичення інформації у стан системної обробки накопиченої інформації та розробки методів її використання для попередження розповсюдження атак, аудиту інформаційних систем, збільшення рівня захищеності інформаційних систем (ІС).

Виконувати дослідження кібератак в реальних умовах, тобто штучно розповсюджуючи шкідливе програмне забезпечення за певним сценарієм надто дорого, а в умовах майже необмеженого поширення в кіберпросторі взагалі неможливо. Тому розробка моделей, на яких до-слідники можуть відпрацьовувати здійснення кібератак на ІС, є важли-вою задачею.

Для моделювання атак використовують дерева атак, які нада-ють уявлення про успішну послідовність кроків зловмисника [1]. Проте такі моделі не дають можливість дослідити динаміку атаки, не врахо-вують системи захисту, не дають можливість оцінити вплив часових характеристик елементів атаки. Аналітичні методи, які використову-ються для виявлення вторгнень в комп'ютерні мережі, розглядаються в [2]. Імітаційні методи генерування атак використовують для їх симу-ляції [3]. Система візуального контролю вразливостей ІС запропоно-вана в [4].

Найпростіша розподілена система складається з персональних комп'ютерів, файл-сервера та веб-сервера. Доступ до веб-сервера здійснюється після авторизації та успішного проходження мережевого екрану (firewall). Система контролю передбачає контрольний запуск тестового пакету. При успішному його запуску, приймається рішення про дієздатність системи, у противному випадку – про її ушкодження.

Дії зловмисника, який атакує розподілену ІС, можуть бути в за-гальному випадку описані таким чином. Він надсилає шкідливу про-граму, яка спрацьовує за наявності певного набору вразливостей в системі і

спричиняє ушкодження (повні або часткові) обчислювальних та/або інформаційних ресурсів системи. В противному випадку атака зловмисника – не успішна. Якщо мета зловмисником не досягнута, то з певною періодичністю він знову обирає для нападу шкідливу програ-му та надсилає її. Шкідливі програми відрізняються наборами вразли-востей, які необхідні для їх спрацювання та набором ушкоджень, які вони спричиняють. Окрім користувачів зі злісними намірами, ІС вико-нує завдання, що надходять від звичайних користувачів. У разі вияв-ленні ушкоджень в роботі системи користувачі повідомляють про це адміністратора.

Для побудови моделі використовується Петрі-об'єктна техноло-гія [5] та програмне забезпечення DESS (Discrete Event Simulation Sys-tem), що автоматизує розробку мереж Петрі об'єктів на основі графіч-ного редактора [6]. Структура Петрі-об'єктної моделі представлена на рисунку 1. Користувач (User) надсилає пакети запитів (Packet), які ви-конуються з використанням обчислювальних ресурсів ІС (System). Якщо користувач помічає надвелику тривалість виконання запиту, він надсилає адміністратору(Admin) тривожний сигнал. Користувач зі злісними намірами (Attack) надсилає пакети запитів (Packet), які вико-ристовують вразливості системи (System) для ураження шкідливим програмним забезпеченням (Malware).

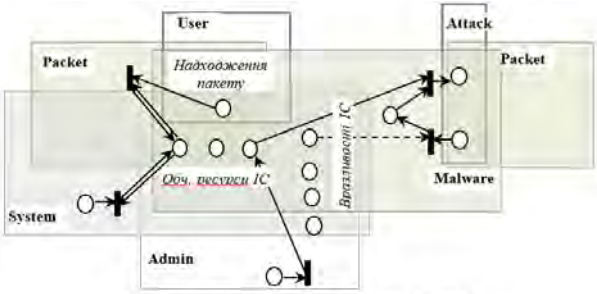

Рис. 1 Структура Петрі-об'єктної моделі розподіленої ІС

Звичайні пакети проходять мережевий екран, авторизацію, отримують доступ до веб-сервера, потім до файл-сервера і запуска-ються операційною системою персонального комп'ютера. Типи паке-тів можуть варіюватись в залежності від необхідності використання того чи іншого набору обчислювальних ресурсів системи. Шкідливе програмне забезпечення проходить ті ж етапи, але при наявності від-повідних вразливостей в системі. При успішному запуску шкідливого програмного забезпечення процес продовжується спричиненням ушкоджень операційній системі, файл-серверу та веб-серверу. Відпо-відно до цієї послідовності

подій складається мережа Петрі-об’єкта (рис. 2). Проникнення шкідливої програми в систему відбува-ється через вразливості ІС, тому з’єднання об’єкту класу Malware з об’єктом класу System здійснюється через відповідні спільні позиції.

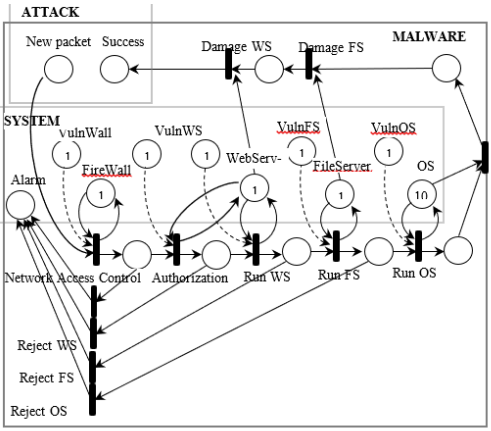

Рис.2 Петрі-об’єкт Malware

Ресурси міжмережевий екран, веб та файл-сервери є спільними для робочих станцій ІС, тому наявність пошкодження в одному з цих ресурсів спричиняє збій в роботі усіх станцій, які їх використовують. З’єднуючи кілька об’єктів System по спільних ресурсах веб-сервер та міжмережевий екран, отримаємо об’єкт Обчислювальний кластер. Пошкодження файл-серверу спричинить припинення роботи з файла-ми усіх робочих станцій (користувачів), які працюють з його використанням. Аналогічно спрацює пошкодження веб-сервера. У РІС з бага-тьма серверами окремі сервери виконують роль маршрутизаторів. Ко-жний маршрутизатор з’єднаний з кількома кластерами, які, в свою чер-гу, з’єднані з іншими маршрутизаторами.

Зловмисник здійснює атаку, повторюючи запуск шкідливого програмного забезпечення до успішного його проходження в систему. У загальному випадку зловмисник обирає для запуску одну чи декіль-ка шкідливих програм та запускає їх за певним сценарієм з урахуван-ням усіх доступних кластерів. Такий сценарій можна відтворити, з’єднуючи відповідним чином об’єкти Атака. За результатами моде-лювання системи визначається середній час, за який ресурси системи будуть пошкоджені для даної інтенсивності атак, а також відсоток ча-су працездатності системи, обумовлений її засобами захисту та інтен-сивністю відновлення.

Таким чином, розглянута формалізована модель кібератак у ви-гляді Петрі-об'єктної моделі. Побудована імітаційна модель кібератак розподіленої інформаційної системи з урахуванням таких деталей як наявні вразливості інформаційної системи, часові характеристики об-робки запитів, ймовірні характеристики системи захисту, індивідуальні характеристики зловмисника (набір використовуваних шкідливих про-грам, навички, обмеженість на витрати часу при повторних запусках). Моделі кібератак є важливим інструментом для дослідження впливу системи захисту на час розповсюдження атаки.

Література

1. P. Wang, J. Liu Threat Analysis of Cyber Attacks with Attack Tree+ // Journal of Information Hiding and Multimedia Signal Processing. – Vol. 5, N. 4. - 2014. – P.778-788.

2. Литвинов В.В. Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі / В.В. Литвинов, Н. Стоянов, І.С. Скітер, О.В. Трунова, А.Г. Гребенник // Математичні машини і системи. – 2018. – № 1. – С. 31-40.

3. Bryan K. Fite Simulating Cyber Operations: A Cyber Security Training Framework // The SANS Institute, 2014 – 36 p.

4. SkyBox Security [Електронний ресурс]. – Режим доступу: https://www.skyboxsecurity.com/solutions/attack-simulation

5. Стеценко И. В. Теоретические основы Петри-объектного моделиро-вания систем / И.В. Стеценко // Математичні машини і системи. – 2011. – № 4. – С. 136-148.

6. Stetsenko I.V. Petri-Object Simulation: Software Package and Complexi-ty / I. Stetsenko, V. Dorosh, A. Dyfuchyn // Proceedings of the 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. – Warsaw, 2015. – P. 381-385.

УДК 004.7; 004.056

МОДЕЛЮВАННЯ РОБОТИ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Є.В. Риндич, В.В. Коняшин

Чернігівський національний технологічний університет

Програмно-апаратні компоненти є частиною майже кожної системи виявлення вторгнень (Intrusion Detection System, IDS), яка здатна кон-