2, Еремеев А.П. Некоторых формальные построения на таблицах решений. – Программирование,1972,№4, с.16-22.

Лановий О.Ф.

ПРО ОДИН ПІДХІД ДО ЗАСТОСУВАННЯ МЕТОДІВ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ ПРИ ДОСЛІДЖЕННІ КІБЕРАТАК

Сучасне суспільство неможливе без використання досягнень науково-технічного прогресу. Швидке поширення інформаційно-телекомунікаційних систем виводить питання забезпечення інформаційної безпеки на передій план. Зростаюча кількість кібератак приводить до необхідності їх детального вивчення та розуміння. Однак вивчення фактів нападу в реальному середовищі їх скоєння у своїй більшості неможливе в силу його активної динаміки, що призводить до необхідності застосування інших методів досліджень.

Одним з варіантів вивчення комп'ютерних атак є моделювання. Моделювання кібератак в інформаційному середовищі, що контролюється дослідником, дозволяє деталізувати процес атаки на окремі служби операційних систем, шляхи поширення вторгнення у мережу тощо. З метою підвищення адекватності імітаційних моделей реальним умовам, валідності системи моделювання сформулюємо ряд вимог, яким вона повинна задовольняти.

Вимоги, *пов'язані з архітектурою мережі,* визначають властивості системи моделювання симулювати та керувати мережею будь-якої топології, не залежно від складності мережі. Система повинна надавати дослідникам інструментарій для повного контролю над моделлю мережі. Крім того, система повинна забезпечувати моделювання - різних типів мережевого обладнання – від комп'ютерів, роутерів, ADSL-модемів до мобільних пристроїв; надавати можливість оперативної зміни суттєвих властивостей мережі – обмеження смуги пропускання сигналів, введення затримок, втрат пакетів або відмови каналів зв'язку; підтримку сценаріїв, які потребують зв'язків з реальними Інтернет-серверами.

Вимоги, що *пов'язані з методами управління в мережі,* визначаються можливостями системи щодо побудови моделей з різної конфігурацією хостів, які, у свою чергу, можуть різнитися операційними системами та апаратною платформою.

Для забезпечення *надійного управління* система моделювання повинна надавати можливість контролювати зв'язки в мережі між будь-якими вузлами в конкретній топології та забезпечувати запис інформації щодо потоків даних між ними та у мережі загалом.

Вимоги до контролю за моделлю в основному визначають простоту побудови моделі, легкість її створення та зміни, управління її складовими та властивостями за допомогою користувальницького інтерфейсу. Система моделювання повинна надавати можливість виконувати визначений набір операцій як в режимі реального, так і прискореного або уповільненого часу, враховувати можливість інтерактивного втручання або перехоплення управління над системою, поведінка якої моделюється.

Виходячи з наведеного вище, архітектура системи складається з 5 шарів: реалізація моделі, транзактори, операції, аналіз та управління (рис.1).

Шар транзакторів включає компоненти, що містять два інтерфейси: інтерфейс зв'язку з моделлю та внутрішній інтерфейс системи. *Драйвери* (*drivers*), *відповідачі* (*responders*), *монітори* (*monitors*) реалізують функції перетворення даних між поданням їх в моделі та тим, як вони використовуються всередині системи моделювання.

Шар операцій містить компоненти, що імітують оточення моделі. *Генератор стимулів* (*stimulus generator*) використовується для створення потоку тестових впливів, а *головні* (*master*) та *другорядні* (*slave*) модулі розширюють його можливості для підтримки операцій зі зворотним зв'язком.

Шар аналізу поєднує компоненти, що реалізують обробку інформації, яка надходить від нижчих шарів системи. *Компоненти перевірки* (*scoreboard*) порівнюють поведінку моделі з еталоном, а *збирач покриття* (*coverage collector*) зберігає інформацію про досягнутий рівень тестового покриття.

Шар управління містить особливий компонент – *контролер моделі*, який здійснює запуск та припинення тестування у залежності від інформації, що надходить від моделі, та відповідно до сценарію моделювання.

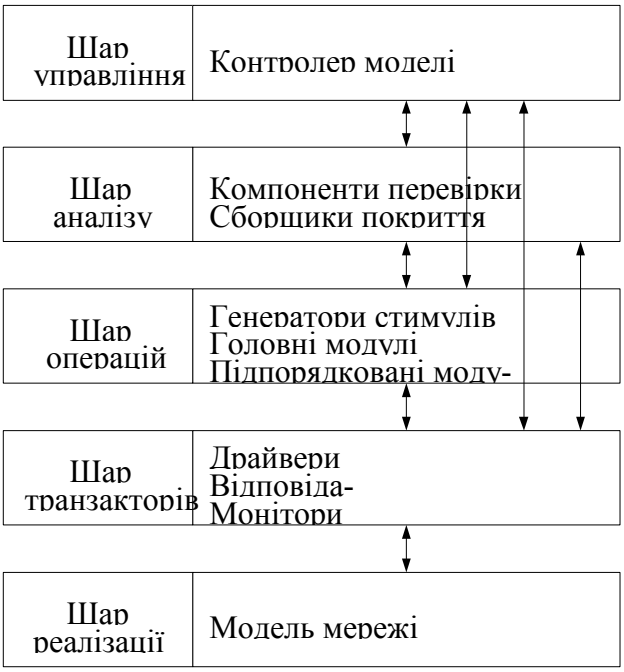

Рис. 1. Структура системи моделювання

Застосування системи моделювання для детального вивчення вже відомих фактів кібератак дозволить полегшити не лише створення нових методів їх виявлення, але і дасть розуміння можливих шляхів їх поширення. Архітектура системи моделювання повинна забезпечувати відбиття реальних явищ, зберігаючи при цьому повний контроль над усіма діями, що виконуються в межах інфраструктур що моделюються. Використання системи імітаційного моделювання дозволить досліджувати різні види атак на безпеку інформаційно-комунікаційних систем, оцінити результати їх впливу.

Перелік використаних джерел

1. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. [Электронный ресурс}. Режим доступа: http://www.crime.vl.ru.
2. EDURange Project, (2013). EDURange: A Cybersecurity Competition Platform to Enhance Undergraduate Security Analysis Skills. [Электронный ресурс}. Режим доступа: http://blogs.evergreen.edu/edurange.
3. A. C. Kim, W. H. Park and D. H. Lee, "A Study on the Live Forensic Techniques for Anomaly Detection in User Terminals", International Journal of Network Security, vol. 7, no. 1, (2013), pp. 181-188. [Электронный ресурс}. Режим доступа: http://www.sersc.org/journals/IJSIA/vol7_no1_2013/17.pdf.

Сєвєрінов О.В., Хрєнов А.Г., Загайнов С.О.

СИСТЕМИ ТА МЕТОДИ ВИЯВЛЕННЯ ВТОРГНЕНЬ В СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ З'ЄДНАНЬ ТА ЧАСТИН ЗС УКРАЇНИ

Система виявлення вторгнень (СВВ, IDS – IntrusionDetectionSystem) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу (вторгнення або мережевої атаки) в комп'ютерну систему або мережу.