Метод тестування на проникнення як засіб забезпечення безпеки корпоративної мережі

Гавронський В.Є.[1], Муляр І.В.[1], Яцків В.В.[2]
Хмельницький національний університет [1]
Західноукраїнський національний університет[2]

Необхідним елементом безпеки корпоративної мережі є тестування її програмного забезпечення як на етапах розробки, так і його використання. Проте не існує єдиної ефективної методики тестування на проникнення. Наприклад, існують криптографічні методи, що базуються на математичних алгоритмах та використовуються для шифрування даних з подальшою передачею їх відкритими каналами зв'язку. Додатковим ступенем захисту є приховання самого факту передачі інформації, наприклад, за допомогою методів цифрової стеганографії [1]. Іншим підходом до вирішення цієї задачі є використання в якості носіїв інформації хаотичних сигналів, які характеризуються широким неперервним спектром та високою інформаційною ємністю [2].

Таким чином, розроблення методу тестування безпеки програмного забезпечення для захисту інформації в корпоративній мережі є актуальним науковим завданням.

Проведені дослідження існуючих методик тестування безпеки програмного забезпечення, факторів, що впливають на цей процес, а також технологій математичної формалізації дозволили виявити ряд недоліків і обмежень щодо їх використання в умовах підвищеної уваги до програмного забезпечення у зловмисників.

На основі аналізу сучасних методів забезпечення безпеки ПЗ та систематизації сучасних підходів у предметній галузі захисту даних сформульовано актуальне наукове завдання, що полягає в розробленні методу тестування безпеки програмного забезпечення для захисту інформації в корпоративній мережі. Для цього розроблено математичну модель початкової генерації коду кібератаки несанкціонованого доступу до інформаційних ресурсів та GERT-модель початкової генерації коду кібератаки несанкціонованого доступу до ресурсів корпоративної мережі. Спрощену GERT-мережу представлено у вигляді рис. 1.

На рис. 1 перехід (1,2) характеризує операції вибору обладнання-жертви для злому. Переходи (2,3) (2,4) описують процес вибору методу атаки з урахуванням визначення операційної системи на вузлі-жертві (Windows або Linux, відповідно).

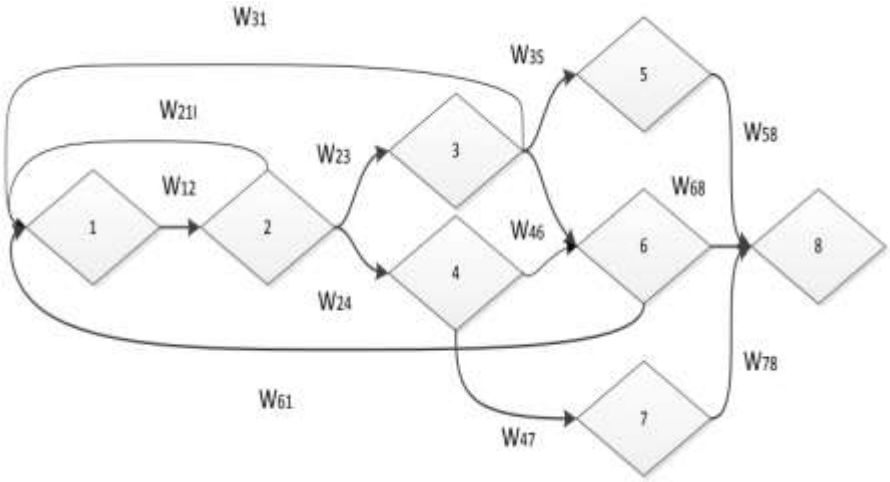

Рисунок 1 - GERT-мережа алгоритму генерації коду кібератаки несанкціонованого доступу

Переходи (2,1) і (3,1) наводять ситуацію, коли зловмисник, через певні причини, не зміг здійснити вибір методу атаки в межах заданого часу або характеристики знайденого шкідливого ПЗ, відповідно, не відповідають умовам і цілям кібератаки несанкціонованого доступу. Перехід (3,5) характеризує процеси пошуку ПЗ в глобальній мережі Інтернет, скачування та установлення ПЗ, що функціонує під OS Windows. Відповідно перехід (4,7) описує процес отримання вихідного коду в глобальній мережі Інтернет і компіляції ПЗ, яке функціонує під OS Linux.

Переходи (3,6) і (4,6) представляють процедури кодування та налагодження ПЗ під OS Windows і Linux, відповідно, за умови відсутності такого в глобальній мережі Інтернет. Перехід (6,1) характеризує ситуацію, коли зловмисник не зміг виконати операції кодування та налагодження шкідливого ПЗ в заданий для атаки час. Переходи (5,8), (6,8) і (7,8) описують процедури запуску шкідливого ПЗ і введення первинних параметрів IP-сервера вузла-жертви.

Проведені дослідження показали, що в складних GERT-мережах з можливими циклами відсутні прості методи знаходження особливих точок функції. Це пов'язано з тим, що для знаходження особливих точок необхідно вирішувати нелінійні рівняння, і чим складнішою є структура GERT-мережі, тим складнішим є і вихідне рівняння [3].

Синтез трас – це наступний етап розробленого методу. Вихідними даними для алгоритму синтезу трас «Синтез» виступає набір графів $\Gamma=\{G1,G2,...,GM\}$, таких, що всі вони споріднені до деякої траси *t*.

Алгоритм складається з двох кроків. На першому кроці виконується розбиття та синтез базових блоків (алгоритм «Базовий блок»). На другому кроці новостворені базові блоки з'єднуються ребрами (алгоритм «Синтез ребер»).

Спочатку враховуються внутрішні команди управління, обумовлені операторами BRANCH. Прямим проходом по операторах цього блоку будується орієнтований ациклічний граф, що описує вирази, які зустрічаються в цьому базовому блоці. Листові вершини в такому графі відповідають операторам INIT.

При побудові такого графа паралельно підтримується хеш-таблиця, ключі в якій відповідають виразам. Під час підрахунку хешу враховується код операції, а також хеші підвиразів. Тоді доповнення графа при перегляді чергового оператора зводиться до перевірки знаходження еквівалентного виразу в хеш-таблиці. Якщо такий вираз знайдено, то нові вершини не створюються. В іншому випадку необхідно створити нову вершину та додати вихідні ребра підвиразів, якщо такі в даному операторі є.

Після того, як граф побудовано, можна виключити повторне обчислення підвиразів: послідовно проглядаються оператори та виключаються ті, які обчислюють підвирази повторно. Слід зазначити, що додатково необхідно враховувати залежності, які проходять через біти слова стану: якщо будь-яка операція виставляє деякий біт, а інша операція, розташована далі, його читає, то першу з них виключати не можна.

У сукупності з уже наявними в середовищі можливостями реалізовані програмні компоненти дозволили повною мірою проводити запропоновану процедуру виділення алгоритму, у тому числі й ітеративно, з поповненням набору розглянутих трас в процесі аналізу.

Основною відмінністю розробленого методу є можливість його використання в ітеративному сценарії, коли в розгляд додаються нові траси за умови відсутності обмежень на природу аналізованого коду. Це дає можливість отримати уявлення про природу динамічної модифікації коду програми за допомогою побудови її еволюційного графа, розміри якого можуть розглядатися як одна з метрик складності програми.

Таким чином, розроблено математичну GERT-модель процесу генерації коду кібератаки несанкціонованого доступу. Запропонована математична модель відрізняється від відомих урахуванням у процесі математичної формалізації GERTмережі основних етапів генерації коду для операційних систем Windows або Linux з можливістю пошуку сучасних рішень у мережі Інтернет. Модель може бути використано для дослідження основних етапів генерації коду кібератаки з метою вироблення практичних рекомендацій протидії процесу несанкціонованого доступу до ресурсів корпоративної мережі.

Перелік посилань

1.Абазина Е.С. Цифровая стеганография: состояние и перспективы / Е.С. Абазина, А.А. Ерунов // Системы управления, связи и безопасности. – 2016. – № 2. – С. 182–201.

2.Колесов В.В. Применение дискретных хаотических алгоритмов в широкополосных телекоммуникационных системах / В.В. Колесов, А.И. Полубехин, Е.П. Чигин, А.Д. Юрин // Вестник СибГУТИ. – 2016. – № 3. – С. 77–92.

3.Барабаш О. В. Методи пошуку оптимальних маршрутів графа структури розгалуженої інформаційної мережі за заданим критерієм оптимальності при різних обмеженнях / О. В. Барабаш, І. П. Саланда, А. П. Мусієнко // Наукові записки Українського науково-дослідного інституту зв'язку. -К.: УНДІЗ, 2016. - №2 (42). - С 99-106.

Оптимальне кодування як засіб підвищення захищеності передачі шифрованих даних

Гончар Р. М., Нагребецький О.В., Орленко В.С., Чешун В.М.
Хмельницький національний університет

Постійне збільшення обсягів інформації в кіберпросторі і зростання її цінності зумовлює зацікавленість конкуруючих сторін і зловмисників у незаконному заволодінні нею, що створює постійну появу нових загроз щодо цілісності і конфіденційності інформації і актуальність заходів її захисту. Одним із основних способів захисту даних є шифрування, про що свідчить поява великої кількості методів та алгоритмів шифрування з різними функціональними можливостями і принципами дії (алгоритми DES-базовий, подвійний і потрійний DES, IDEA, ГОСТ 28147, Діффі-Хелмана, RSA тощо [1]) та тенденція до їх постійного вдосконалення.

Підвищення криптостійкості алгоритмів шифрування досягається як розробкою нових їх реалізацій, так і модернізацією-вдосконаленням існуючих або їх комбінуванням.

Проведені дослідження показують, що підвищення криптостійкості алгоритмів шифрування можна досягти попередньою підготовкою вхідних даних, в ході якого забезпечується порушення статистичних даних повторюваності символів вхідного тексту, тобто, збільшення характеристик його ентропії. Одним із варіантів такої підготовки вхідного тексту може бути застування методів оптимального нерівномірного кодування.

Для демонстрації можливості збільшення криптостійкості алгоритмів шифрування попередньою підготовкою вхідних даних оптимальним кодуванням обрано два класичних методи:

– кодування Хаффмена як класичний метод оптимального