Тесленко О. К., канд. техн. наук, доцент кафедри,
Перегудов М. С., магістрант
КПІ ім. Ігоря Сікорського

МЕТОД ОЦІНКИ АНТРОПОГЕННОГО ВПЛИВУ В ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ

За останні кілька років технологія програмно-конфігурованих мереж (ПКМ, *англ.*: SDN) пройшла шлях від ідеї до реальних технічних рішень [1]. По суті у даній технології рівень керування відділено від пристроїв передачі даних і реалізовано програмними засобами, що дозволяє динамічно розподіляти ресурси, підтримувати обробку величезних обсягів інформації та віртуалізацію, яка необхідна для автоматизованого та безпечного хмарного середовища. Архітектура ПКМ суттєво змінює структуру мережі, отже, виникають нові загрози безпеки. Крім того, більшість загроз, характерних для традиційних систем передачі даних, є критичними також і для ПКМ. Як показує аналіз, усі джерела загроз безпеці інформації, що циркулює в мережі, можна розділити на три основні групи: антропогенні, техногенні та природні.

Причому з точки зору захисту інформації перша група найбільш цікава, оскільки дії суб'єкта завжди можна спрогнозувати. Проте методи такого оцінювання антропогенного впливу не завжди формалізовані. Тому розробка методів оцінки антропогенного впливу на програмні комплекси, зокрема ПКМ, є актуальною задачею.

Однією із завдань захисту інформації, як відомо, є цілісність переданих даних, що у свою чергу залежить від надійності комп'ютерних систем. І якщо для апаратної частини, зокрема ПКМ, розроблено потужний арсенал методів її оцінки, то стосовно програмного забезпечення результати є більш скромними. Однією з причиною цього є суттєве зростання впливу антропогенного чиннику, до якого відносяться також атаки. У свою чергу проблема захисту від атак пов'язана з інформаційної стійкістю програмних систем, під якою розуміють гарантоване забезпечення сервісів та протидію їх використанню за недекларованим призначенням. Таке визначення є досить загальним і дозволяє включати в себе цілий ряд проблем від питань надійності апаратних засобів та програмного забезпечення до методів протидії хакерським атакам. Зокрема наявність централізованого мережного контролера, який є критичним для нормального функціонування мережі, породжує вразливість до DoS-атак, які можуть привести до відмови всієї інфраструктури ПКМ. Крім цього, атаки сканування, які часто є попередниками DoS-атак, також можуть спричинити використання специфічних вразливостей програмного забезпечення контролера. Для систем критичного застосування прийнято застосовувати терміни «гарантоздатність» («dependability»). Результати розробки принципів гарантоздатності комп'ютерних систем узагальнені в праці [2]. До ключових з них можна віднести пошук можливих критичних ділянок. Зазвичай таке тестування програм виконується для перевірки відповідності поведінки сервісу до сценаріїв, зазначених у специфікаціях.

Проте антропогенний вплив на ПКМ не завжди спричиняє порушення інформаційної безпеки. Таким порушенням слід вважати лише збій у роботі, який породжує можливість віддаленого виконання програмного коду, обходу політики безпеки; ініціювання відмови в обслуговуванні, що впливає на інформаційно-технічний стан ПКМ. Це можна розглядати як перехід системи у несправний, непрацездатний, частково працездатний або небезпечний стан залежно від впливу.

На основі проведеного аналізу можна виділити такі методи дослідження інформаційної стійкості ПКМ і оцінки антропогенного впливу.

1. Ручний пошук, що базується на пошуку функцій, вхідні дані для яких можна змінити з метою отримання незапланованого результату.

2. Пошук за шаблонами – автоматизований метод пошуку типових не стійких сценаріїв на основі сигнатур, причому такі сигнатури можна доповнити набором евристичних правил.

3. Fuzzing – автоматизований метод пошуку на основі динамічного синтезу вхідних даних (повного або часткового) [3]. При цьому можуть використовуватись заздалегідь підготовлені дані, зміна структурованих даних протоколу, порушення формату даних в бінарних протоколах, а також повним перебір мутацій даних.

Як показує проведений аналіз, факт антропогенного впливу на ПКМ доцільніше оцінювати за допомогою автоматизованого методу пошуку на основі динамічної зміни вхідних даних, оскільки через різноманітність функцій окремих компонентів мережі ручний пошук або автоматизований пошук на основі сигнатур суттєво ускладнені.

Література

1. A survey of network update in SDN / Li D., Wang S., Zhu K., Xia S. // Frontiers of computer science. – 2017. – № 1. – P. 4-12.

2. Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avizienis, J.C. Laprie, B. Randell, C. Landwehr // IEEE Trans. On Dependable and Secure Computing. – 2004. – Vol.1. – №1. – P. 11-33.

3. Sutton M. Fuzzing: Brute Force Vulnerability Discovery / M. Sutton, A. Greene, P. Amini. – Addison Wesley, 2007.– 517 p.