УДК 004.056(043.2)

ВИКОРИСТАННЯ ТЕОРІЇ ІГОР В ЗАДАЧАХ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Марченко Віталій Анатолійович
Інститут кібернетики ім. В.М. Глушкова НАНУ, http://www.icyb.kiev.ua, vmarchenko@gmail.com

В доповіді представлено підхід до вирішення задач захисту інформації в сучасних інформаційних системах з застосуванням теорії ігор. Наведено інтерпретацію базових понять теорії ігор в термінах захисту інформації в інформаційних системах.

Ключові слова – інформаційна безпека; захист інформації; теорія ігор.

ВСТУП

Сучасні інформаційні системи представляють собою набір програмних додатків розподілених в рамках великих географічних регіонів і пов'язаних між собою за допомогою загальнодоступної телекомунікаційної інфраструктури. В якості транспортної мережі в основному застосовується мережа Інтернет. Таким чином для організації захисту інформації в рамках інформаційної системи необхідно забезпечити ефективний захист на декількох рівнях:

- рівні транспортної інфраструктури;
- рівні інформаційної системи.

Для організації захисту на рівні транспортної інфраструктури використовуються загальновідомі засобі такі як VPN [1] та прикладні протоколи такі як HTTPS [2] для захисту виділеного сеансу зв'язку між серверним додатком та прикладною частиною користувача. Організація захисту в межах інформаційної системи забезпечуються тільки її власником.

Останнім часом інформаційні атаки спрямовуються на компрометацію саме інформаційних систем. За своїм принципом функціонування та побудови поділяються на дві категорії. Перша категорія це інформаційні атаки, які використовують особливості архітектури атакованої системи або сервісу (особливості протоколів, взаємозв'язків різних підсистем і т.п.). До другої категорії належать атаки спрямовані на використання помилок в реалізації конкретних алгоритмів нормального функціонування інформаційної системи. наприклад збереження оригінальної інформації після шифрування, відсутність фільтрування введених даних і т.п.

Для ефективної протидії атакам пов'язаним з помилками в реалізації досить ефективними виявилися методи аналізу і тестування вихідного коду системи, проведення навантажувальних випробувань і застосовуючи різні методи оптимізації та верифікації програмних комплексів.

При створенні методів протидії архітектурним атакам пропонується використовувати апарат теорії ігор. При цьому присутні два учасника гри:

- зловмисник, який намагається з компрометувати цільову систему;
- захисник, який представлений власником інформаційної системи.

У якості стратегій для зловмисника будуть використовуватися відомі вектори атак та окремі атаки, наприклад такі як описані в класифікаторі WASC [3]. Таким чином його ігрова стратегія буде полягати у спробах реалізації тієї чи іншої погрози з нобору відомих атак або привести наявну ігрову ситуацію до відомої стратегії з визначеним виграшем.

Ігрова стратегія захисника буде полягати у реалізації та використанні відомих методів захисту в рамках своєї інформаційної системи для протидії найбільш ймовірним атакам для даної інформаційної системи.

Виграшем у вказаній грі для зловмисника буде порушення цілісності, конфіденційності, доступності інформації що оброблюється у атакованій інформаційній системі, а виграшем для захисника буде недопущення вказаних дій. Відповідно гра буде з нульовою сумою, так як виграш зловмисника призводить до втрат захисника. Сама гра буде описуватися як гра в нормальній формі [4] для якої пара "інформаційна атака-метод захисту" буде представляти собою вмістом матриці платежів для даної гри.

ВИСНОВКИ

У цій доповіді увага приділяється особливостям застосування теорії ігор для дослідження та аналізу атак направлених на експлуатації архітектурних особливостей інформаційної системи. Пропонується використовувати матрицю поширених атак на веб-орієнтовані системи в якості стратегії зловмисників з подальшим дослідженням оптимальної стратегії захисника для мінімізації втрат (програшу в термінах гри) від проведення інформаційних атак.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Provider Provisioned Virtual Private Network (VPN) Terminology. L. Andersson, T. Madsen. Date, March 2005. http://www.ietf.org/rfc/rfc4026.txt.

2. Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000. http://www.ietf.org/rfc/rfc2818.txt

3. The WASC Threat Classification v2.0. 2010. 172p. http://projects.webappsec.org/f/WASC-TC-v2_0.pdf

4. Костевич Л.С., Лапко А.А, Теория игр. Исследование операций. – Минск: Вышэйшая школа, 1982. 229 с.