МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
ОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. Ф.М. ДОСТОЕВСКОГО

ОМСКИЕ НАУЧНЫЕ ЧТЕНИЯ – 2018

Материалы Второй Всероссийской научной конференции

(Омск, 10–15 декабря 2018 г.)

ISBN 978-5-7779-2339-4

Омск

ИЗДАТЕЛЬСТВО ОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

2018

ИЕРАРХИЧЕСКИЕ ИГРЫ И ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ

Т.В. Вахний, А.К. Гуц

Омский государственный университет им. Ф.М. Достоевского, г. Омск, Россия
E-mail: vahniytv@mail.ru; guts@omsu.ru

HIERARCHICAL GAMES AND DEFENSE OF COMPUTER SYSTEMS

T.V. Vahniy, A.K. Guts

Dostoevsky Omsk State University, Omsk, Russia

В докладе обсуждаются теоретико-игровые моменты проблемы описания защиты компьютерной системы в случае, когда ведущая роль принадлежит злоумышленнику, а ведомая − администратору безопасности. Предлагается для решения данной проблемы использовать теорию иерархических игр.

In the report we discuss the game-theoretic moments of the problem of describing the protection of a computer system in the case when the leading role belongs to the attacker, and the led role to the security administrator. It is proposed to solve this problem using the theory of hierarchical games.

Ключевые слова: иерархические игры, защита компьютерной системы.

Keywords: hierarchical games, defense of computer systems.

1. Поведение хакера и администратора

Теория игр в последнее десятилетие активно используется для организации защиты компьютерных систем [1]. Однако хотя при этом обращаются как стратегическим играм, так и к позиционным и даже к стохастическим играм, мало обращается внимание на иерархическое неравенство в этом противостоянии хакера и администратора. Взаимодействие хакера и администратора характеризуется тем, что ведущая роль принадлежит хакеру. Именно он организует атаку на компьютерную систему, ему принадлежит инициатива в противостоянии «Нападение – защита». Более того, опытный хакер прекрасно осведомлен о всех способах защиты информационного ресурса, которыми располагает администратор. Напротив, администратор часто уступает хакеру не только в инициативе, но и в знаниях наличевствующих «дыр» в защищаемой им системе. Иначе говоря поведение администратора следует описать словом «ведомый». Наконец, хакер действует первым, раньше администратора. С точки зрения теории игр следует говорить об игре с фиксированной последовательностью ходов.

Учет психологических моментов в поведении хакеров и администратора может быть произведен посредством рефлексивных игр [2]. Но принятие во внимания отношения типа «Ведущий – ведомый» возможно только в рамках так называемой теории иерархических игр. Рассмотрим как может быть описана такая игра (в нормальной форме) на примере игры Γ_1.

2. Атаки хакера с точки зрения иерархических игр

Пусть хакер имеет в своем распоряжении стратегии x из множества стратегий X, а администратор – стратегии y из множества стратегий Y. Рассмотрим игру в *нормальной форме.* В такой игре каждый участник выбирает стратегию, не зная выбора партнера. Пара стратегий (x,y) называется *ситуацией* игры. Интересы хакера характеризует функция выигрыша $F(x,y)$ – наносимый ущерб (в рублях), а администратора – функция выигрыша $G(x,y)$ – объем сохраненной информации, определенные на множестве всех ситуаций $X \times Y$. Каждый игрок стремится, по возможности, максимизировать свою функцию выигрыша. Таким образом, игра двух лиц в нормальной форме задается совокупностью $\Gamma = \{X, Y, F(x, y), G(x, y)\}$.

Игра Γ_1. Хакер выбирает стратегию $x \in X$ и начинает атаку. Для опытного администратора нетрудно понять, какая атака предпринята хакером. Поэтому фактически это означает – в терминах теории иерархических игр, – что хакер сообщает свою стратегию администратору. Затем администратор, зная x, выбирает стратегию $y \in Y$.

Игра Γ_1 является одношаговой игрой с полной информацией. Найдем наилучший *гарантированный результат* F_1 хакера игрока в игре Γ_1. Другими словами, мы пытаемся оценить неизбежный ущерб, который принесет атака хакера. Предположим, что администратор, зная *x*, выбирает

$$y \in Y(x) = Arg \max_{y \in Y} G(x, y),$$

т. е. максимизирует свою функцию выигрыша *G*(*x,y*), поскольку его задача максимально сохранить информацию. Будем считать, что хакер обладает полной информацией о важнейших ресурсах атакуемой системы. Хакер, предпринимая атаку *x,* знает, какие при этом информационные ресурсы им будут незатронутыми. Поэтому можно считать, что функция выигрыша администратора ему также известна, и ему также понятно, что администратор будет выбирать стратегию из множества *Y*(*x*). Но он не знает конкретного выбора $y \in Y(x)$.

Величина $W(x) = \min_{y \in Y} F(x, y)$ называется *оценкой эффективности* (гарантированным результатом) стратегии *x*. Поэтому наилучший гарантированный результат хакера – ущерб, который нанесет хакер – имеет вид: $F_1 = \sup_{x \in X} \min_{y \in Y} F(x, y)$.

Пусть задано $e > 0$. Стратегия хакера x_ε называется e-*оптимальной* в игре Γ_1, если $W(x_\varepsilon) > F_1 - \varepsilon$. Решить игру Γ_1 – это значит найти величину F_1 и *e*-оптимальную стратегию x_ε при заданном $e > 0$.

Мы видим, что чтобы лишить хакера наилучшего гарантированный результата от атаки, необходимо не допускать знания хакером функции *G*(*x,y*) и скрывать данные о важнейших ресурсах компьютерной системы. Теория иерархических игр, тем самым, математически подтверждает действенность известных принятых инструкций по соблюдению режима безопасности информационных ресурсов, их перечня, серверов хранения данных и т. д.

Можно рассматривать и другие типы задач с различными оптимизационными критериями. Например, в статьях [3; 4] с целью защиты компьютерных сетей рассматривается игра с критерием оптимальности Штакельберга, устанавливающее некоторое *щадящее* для участников игры равновесие.

---

1. *Гуц А.К., Вахний Т.В.* Теория игр и защита компьютерных систем. Омск, 2013.

2. *Гуц А.К.* Выявление цены психологической ошибки администратора компьютерной сети в оценке квалификации злоумышленников // Омские научные чтения [Электронный ресурс]: материалы Всерос. науч.-практ. конф. (Омск, 11–16 декабря 2017 г.). Омск, 2017.

3. *Damjanovic-Behrendt V.* Stackelberg Security Game for Optimizing Security of Federated Internet of Things Platform Instances // World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering. 2017. Vol. 11. № 5. P. 529–534.

4. *Lee P., Clark A., Alomair B., Bushnell L., Poovendran R.* Passivity-Based Distributed Strategies for Stochastic Stackelberg Security Games // Proceedings of 6th International Conference «GameSec 2015». UK, November 4–5. London, 2015. P. 113–129.