ВЫБОР СТРАТЕГИИ ЛОЖНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ МОДЕЛИ ТЕОРИИ ИГР

Шматова Е.С[1].

В настоящей статье рассмотрена технология обнаружения атак на основе ложных информационных систем (ЛИС), в англоязычной терминологии – технология Honeypot («ловушка»). Данная технология является системой пассивного сбора событий сетевых атак и имеет ряд немаловажных преимуществ. Одним из них является возможность регистрации только реальных попыток зондирования или атак, так как ЛИС не используется санкционированными пользователями сети. Проблема состоит в том, что с развитием практики применения ЛИС, злоумышленники стали активно искать пути обхода «ловушек». Помимо этого, в случае обнаружения ЛИС она может быть использована против других информационных систем. Следовательно, ЛИС должна быть не только хорошо замаскирована, но и обеспечивать максимальную вероятность того, что злоумышленник будет выбирать в качестве атакуемой цели «ловушку», а не реальную систему. Для решения данных вопросов возможно использовать математический аппарат теории игр. В настоящей работе приведены статьи последних лет, подтверждающие актуальность теоретико-игрового подхода при рассмотрении взаимодействия между ЛИС и стороной нападения. Также в статье предложена постановка задачи выбора моделируемых в ЛИС информационных ресурсов на основе теоретико-игрового подхода. Выбор оптимальной стратегии ЛИС позволит эффективно использовать технологию в целях информационной безопасности.

***Ключевые слова**: информационная безопасность, информационный ресурс, ложная информационная система, теория игр*

Введение

Одной из задач, решаемых специалистами по информационной безопасности, является сбор сведений, позволяющих обнаружить атаки, и анализ действий злоумышленника. Обнаружение атак на основе ложных информационных систем, иначе технология Honeypot («ловушка»), позволяет на более ранней стадии обнаружить факт подготовки атаки, изучить поведение ее инициатора при попытке проникновения и управления уже захваченным ресурсом, получить информацию о ранее неизвестных методах атак, дезинформировать злоумышленника, а также обнаружить «дыры» в безопасности и своевременно применить меры по их устранению. Honeypot является ложным ресурсом информационной системы (ИС), не используемым санкционированными пользователями сети и находящимся под полным контролем специалистов по информационной безопасности. Это позволяет сократить число ложных тревог и объем обрабатываемых событий безопасности, поскольку в системе регистрируется только реальные попытки зондирования или атаки. Однако следует отметить, что необходимы обоснованные подходы и рекомендации к процессу проектирования таких «ловушек», так как в случае обнаружения злоумышленником ЛИС она может быть использована для организации атак на другие системы [11]. Таким образом, исследование и разработка научно обоснованных решений для проектирования ЛИС в реальных автоматизированных системах (АС) представляет собой актуальную проблему в сфере информационной безопасности.

ЛИС может представлять собой как отдельный хост сети, так и сеть, наполненную разного рода объектами: маршрутизаторами, серверами, рабочими станциями, реальными или виртуальными. Следует отметить, что развитию практики применения ЛИС способствует активное внедрение технологии виртуализации, появление программных средств виртуализации, позволяющих создать виртуальную инфраструктуру и управлять ею [1]. Однако с увеличением степени использования рассматриваемой технологии злоумышленники принимают во внимание возможность существования ЛИС в атакуемой сети и пытаются обойти «ловушки». Следовательно, такие ИР должны быть достаточно замаскированы и не очевидны, ЛИС не должна представлять из себя наиболее уязвимую цель для злоумышленника (при этом должна быть обеспечена высокая вероятность выбора злоумышленником в каче-

1 Шматова Елена Сергеевна, МГТУ им. Н.Э. Баумана, Москва, elena_shmatova.92@mail.ru.

стве цели ложной ИС, а не реальной системы) [2]. Это приводит к рассмотрению некоторой состязательности между злоумышленником и ЛИС, анализу стратегий взаимодействующих сторон. С этой задачей может справиться математический аппарат теории игр.

1. Ложные информационные системы и теория игр

В настоящее время предложено немало решений, в том числе открытых реализаций, для проектирования ЛИС, однако меньше известно о том, как разработать стратегию «ловушки» в защищаемой сети [2].

При решении задач, связанных с обеспечением информационной безопасности, широкое применение находит математический аппарат теории игр [3]. Теория игр является формальным подходом, предназначенным для анализа взаимодействий между несколькими участниками игры, принимающими решения. В области защиты информации присутствуют две стороны: сторона нападения и сторона защиты, в качестве которой выступают системы защиты информации.

Рассмотрим примеры использования теории игр. В работе [4] предложена математическая модель антагонистической игры и алгоритмы, позволяющие решить задачу выбора средств защиты информации в АС. Методы теории игр используют и для выбора средств защиты от конкретных сетевых атак. Например, в [5] разработана матричная игра двух игроков с нулевой суммой для выбора эффективного средства защиты от DoS/DDoS-атак. В работе [6] рассмотрено взаимодействие узловой системы обнаружения вторжений и нарушителя информационной безопасности с помощью некооперативной игры с ненулевой суммой, где оптимальные стратегии игроков выбираются согласно равновесию Нэша. Математический аппарат теории игр находит свое применение и в технологии ЛИС.

Имеющиеся на данный момент работы, исследующие взаимодействие злоумышленника и ЛИС (сторона защиты) с помощью теории игр, можно разделить на две категории: моделирование взаимодействия сторон для конкретной атаки и моделирование взаимодействия до проведения атаки, когда злоумышленник, анализируя сеть, выбирает цель нападения [2]. Во втором случае рассматривается проблема повышения вероятности выбора злоумышленником ложной ИС для проведения атаки. Так в работе [2] представлены две теоретико-игровые модели с нулевой суммой, позволяющие понять, какой должна быть «ловушка», чтобы максимизировать вероятность проведения атаки на ЛИС, а не на реальную систему. Первая модель позволяет определить число приманок, размещаемых в ЛИС, и их конфигурацию. Вторая модель включает в рассмотрение стратегию зондирования, целью которой является обнаружение ЛИС в реальной сети. В [7] посредством некооперативной игры с ненулевой суммой рассмотрено взаимодействие между ЛИС и бот-сетью (от англ. botnet; от слов robot и network). При моделировании большое внимание уделяется проблеме обнаружения ЛИС ботами. Следует отметить, что в поиске уязвимых мест ложной ИС заинтересованы как злоумышленники, так специалисты по информационной безопасности. Не менее интересным является решение, предложенное в работе [8], где для построения игровой модели используются графы атак, а оптимальная стратегия игроков определяется равновесием Штакельберга.

Таким образом, можно сделать вывод, что теория игр – это математическая теория, которая способна вырабатывать и находить оптимальные стратегии и инструкции по организации систем информационной безопасности. Ниже будет предложена постановка задачи выбора ресурсов сети, моделируемых в ЛИС, на основе теоретико-игрового подхода.

2. Постановка задачи выбора ресурсов сети, моделируемых в ЛИС

Рассмотрим постановку задачи выбора ресурсов сети для их моделирования в ЛИС.

Подобная постановка была представлена в [9].

2.1. Исходные данные

$S = \{s_1, s_2, \ldots, s_n\}$ – множество защищаемых ИР,

$N = \{1, 2, \ldots, n\}$ – множество индексов ресурсов.

$w_i > 0, \forall\, i \in N$ – стоимость защищаемых ресурсов (возможный ущерб при нарушении требований безопасности).

$c_{зi} > 0, \forall\, i \in N$ – стоимость защиты ИР посредством технологии ЛИС.

$c_{нi} > 0, \forall\, i \in N$ – стоимость проведения атаки на ИР.

$p_{лi} > 0, \forall\, i \in N$ – вероятность выбора *i*-го ложного ИР злоумышленником для проведения атаки.

2.2 Показатели игроков

Для стороны защиты введем переменную $p_i \in [0,1], \forall\, i \in N$, имеющую содержательный смысл вероятности конфигурации *i*-го реального ИР в системе ЛИС, переменные образуют вектор $\vec{P}$. Для стороны нападения введем переменную $q_i \in [0,1], \forall\, i \in N$, имеющую содержательный смысл вероятности атаки на i-ый ИР переменные образуют вектор $\vec{Q}$. Векторы $\vec{P}$ и $\vec{Q}$ определяют стратегии игроков.

В отношении каждого объекта для сторон защиты и нападения возможны две стратегии: сторона защиты моделирует ИР в ЛИС или не моделирует, сторона нападения проводит атаку на ресурс сети или нет. Матрицы игры для отдельного ИР в рамках взаимодействующих сторон могут быть построены аналогично тем, что приведены в [9].

После исключения компонент показателей, определяющих затраты игроков, и их переноса в ограничения, как это было сделано в [10], была получена модель игры с нулевой суммой. Таким образом, выигрыш стороны нападения, который можно рассматривать как результат игры «атакующих» отдельные ИР, определяется максимальным ущербом, который может быть нанесен стороной нападения при атаке на реальные ИР, минус предотвращенный ущерб стороной защиты:

$$F_н(\vec{P},\vec{Q}) = \sum_{i \in N}[q_i w_i - p_i q_i p_{лi} w_i] .$$

Т.к. была получена игра с нулевой суммой, то выигрыш стороны защиты в целом, который можно рассматривать как результат игры всех моделируемых (ложных) информационных ресурсов ЛИС, имеет следующий вид:

$$F_з(\vec{P},\vec{Q}) = -F_н(\vec{P},\vec{Q}) = \sum_{i \in N}[\, p_i q_i p_{лi} w_i - q_i w_i].$$

2.3 Ограничения

Для стороны защиты ограничения на ресурсы, выделяемые на защиту:

$$\sum_{i \in N} c_{зi} p_i \le C_з^{max} ,$$

где $C_з^{max}$ – максимальный размер ресурсов, выделенных на ЛИС.

Аналогично для стороны нападения:

$$\sum_{i \in N} c_{нi} q_i \le C_н^{max} ,$$

где $C_н^{max}$ – максимальный размер ресурсов, выделенных на проведение атак.

Каждая из сторон стремится выбрать такую стратегию, чтобы максимизировать свой показатель (выигрыш). Решением подобной игры может стать поиск седловой точкой, т.е. пары $(\vec{P}_0, \vec{Q}_0) \in M_p \times M_q$, где M_p, M_q – множество допустимых векторов $\vec{P}$, $\vec{Q}$, соответственно, при которой игрокам не выгодно отклоняться от выбранных стратегий. Компоненты вектора-стратегии $\vec{P}_0$, имеющие содержательный смысл вероятности моделирования *i*-го реального ресурса в ЛИС, определяют ИР, которые будут играть роль «ловушек». Для решения данной задачи можно предложить алгоритм, основанный на игровой модели и принципе равномерной защищенности объектов, предложенный в [10].

Выводы

В настоящей статье была рассмотрена технология ложных информационных систем, используемая для привлечения злоумышленника и дальнейшего исследования его действий. Так как ЛИС не используется санкционированными пользователями сети, поведение нарушителя в «ловушке» своевременно регистрируется и не влияет на функционирование реальной системы. Однако активное внедрение рассматриваемой технологии способствует развитию методов, позволяющих злоумышленникам определять наличие ЛИС в атакуемой сети и обойти их. Это может привести к использованию ЛИС против других ИС, следовательно, к ее неэффективности. Таким образом, ЛИС должна быть не только хорошо замаскирована, но и обеспечивать максимальную вероятность того, что злоумышленник будет выбирать в качестве цели «ловушку», а не реальную систему. Данная проблема несет состязательный характер между нарушителем и ЛИС, что позволяет задействовать математический аппарат теории игр. В статье рассмотрены работы, использующие теоретико-игровые модели для определения оптимальных стратегий участников игры. Также в работе была предложена постановка задачи выбора моделируемых в ЛИС информационных ресурсов на основе теоретико-игрового подхода и алгоритм, который может быть использован для ее решения. Работа алгоритма была продемонстрирована в [10]. Выбор оптимальной стратегии ЛИС позволит эффективно использовать технологию в целях информационной безопасности.

Научный руководитель: Шеремет Игорь Анатольевич, доктор технических наук, профессор, i.a.sher@yandex.ru.

Литература:

1. Язов Ю.К., Сердечный А.Л., Шаров И.А. Методический подход к оцениванию эффективности ложных информационных систем // Вопросы кибербезопасности. 2014. № 1(2). С. 55-60.
2. Píbil R., Lisý V., Kiekintveld C., Bošanský B., Pěchouček M. Game theoretic model of strategic honeypot selection in computer networks // GameSec. 2012. LNCS. Vol. 7638. 2012. P. 201-220. DOI = 10.1007/978-3-642-34266-0_12
3. Белый А.Ф. Компьютерные игры для выбора методов и средств защиты информации в автоматизированных система // Известия ЮФУ. Технические науки. 2008. № 8 (85). С. 172-176.
4. Быков А.Ю., Алтухов Н.О., Сосенко А.С. Задача выбора средств защиты информации в автоматизированных системах на основе модели антагонистической игры // Инженерный вестник. 2014. № 4. С. 5.
5. Абденов А.Ж., Заркумова Р.Н. Выбор средства эффективной защиты с помощью методов теории игр // Вопросы защиты информации. 2010. № 2. С. 26-31.
6. Лаврентьев А.В., Зязин В.П. О применении методов теории игр для решения задач компьютерной безопасности // Безопасность информационных технологий. 2013. № 3. С. 19-24.
7. Osama Hayatle, Hadi Otrok, Amr Youssef. A game theoretic investigation for high interaction honeypots // Communications (ICC), 2012 IEEE International Conference on. 2012. P. 6662-6667. DOI = 10.1109/ICC.2012.6364760.
8. Durkota K., Lisý V., Bošanský B., Kiekintveld C. Optimal network security hardening using attack graph games // Proceedings of IJCAI. 2015. P. 7-14. URL: http://ijcai.org/papers15/Papers/IJCAI15-080.pdf
9. Быков А.Ю., Шматова Е.С. Задача выбора контролируемых узлов в системе обнаружения вторжений для информационной системы на основе модели биматричной игры // Пятая Всероссийская научно-техническая конференция «Безопасные информационные технологии». Сборник трудов конференции. М.: НИИ РЛ МГТУ им. Н.Э. Баумана. 2015. С. 41-43.
10. Быков А.Ю., Шматова Е.С. Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равномерной защищенности объектов // Наука и образование. [Электронный ресурс]. М.: МГТУ им. Н.Э. Баумана. 2015. №9. С. 160-187. Режим доступа: http://technomag.bmstu.ru/doc/812283.html.
11. Шеремет И.А. Угрозы техносфере России и противодействие им в современных условиях // Вестник академии военных наук. 2014. № 1 (46). С. 27-34.

THE CHOICE OF STRATEGY FOR THE SPURIOUS INFORMATION SYSTEM ON THE BASIS OF THE GAME THEORY MODEL

***Shmatova E.S.*[2]**

The paper touches upon the technology of attack detection on the basis of spurious information systems (SIS), in English – a Honeypot technology («trap»). This technology is a system of passive collection of network attacks events and has several significant advantages. One of them is the ability to record only real attempts of probes or attacks, as the SIS is not used by authorized users of the network. The problem consists in the following: with the development of SIS, adversaries are beginning to search for the backdoors to bypass the «traps». Moreover, in case the SIS is detected, it can be used against other information systems. Hence the SIS should not only be well hidden but it should also provide the maximum probability that the adversary chooses the «trap» and not the real system as his target. The mathematical tool of game theory may be used to resolve such problems. The paper contains recent researches proving the relevance of the game–theoretic approach to the examination of interaction between the SIS and the adversary. The paper also presents a formulation of the problem for the choice of simulated information resources in the SIS on the basis of the game–theoretic approach. The optimal strategy of the SIS allows to effectively use the technology for the purposes of information security.

***Keywords**: information security, information resource, spurious information system, game theory.*

References:

1. Yazov Yu.K., Serdechnyy A.L., Sharov I.A. Metodicheskiy podkhod k otsenivaniyu effektivnosti lozhnykh informatsionnykh system, Voprosy kiberbezopasnosti. 2014. No 1(2), pp. 55-60.

2 Elena Shmatova, Bauman Moscow State Technical University, Moscow, elena_shmatova.92@mail.ru.

2. Píbil R., Lisý V., Kiekintveld C., Bošanský B., Pěchouček M. Game theoretic model of strategic honeypot selection in computer networks, GameSec. 2012. LNCS. Vol. 7638. 2012, pp. 201-220. DOI: 10.1007/978-3-642-34266-0_12
3. Belyy A.F. Komp'yuternye igry dlya vybora metodov i sredstv zashchity informatsii v avtomatizirovannykh Sistema, Izvestiya YuFU. Tekhnicheskie nauki. 2008. No 8 (85), pp. 172-176.
4. Bykov A.Yu., Altukhov N.O., Sosenko A.S. Zadacha vybora sredstv zashchity informatsii v avtomatizirovannykh sistemakh na osnove modeli antagonisticheskoy igry, Inzhenernyy vestnik. 2014. № 4. S. 5.
5. Abdenov A.Zh., Zarkumova R.N. Vybor sredstva effektivnoy zashchity s pomoshch'yu metodov teorii igr, Voprosy zashchity informatsii. 2010. No 2, pp. 26-31.
6. Lavrent'yev A.V., Zyazin V.P. O primenenii metodov teorii igr dlya resheniya zadach komp'yuternoy bezopasnosti // Bezopasnost' informatsionnykh tekhnologiy. 2013. No 3, pp. 19-24.
7. Osama Hayatle, Hadi Otrok, Amr Youssef. A game theoretic investigation for high interaction honeypots // Communications (ICC), 2012 IEEE International Conference on. 2012, pp. 6662-6667. DOI: 10.1109/ICC.2012.6364760.
8. Durkota K., Lisý V., Bošanský B., Kiekintveld C. Optimal network security hardening using attack graph games, Proceedings of IJCAI. 2015, pp. 7-14. URL: http://ijcai.org/papers15/Papers/IJCAI15-080.pdf
9. Bykov A.Yu., Shmatova E.S. Zadacha vybora kontroliruemykh uzlov v sisteme obnaruzheniya vtorzheniy dlya informatsionnoy sistemy na osnove modeli bimatrichnoy igry, Pyataya Vserossiyskaya nauchno-tekhnicheskaya konferentsiya «Bezopasnye informatsionnye tekhnologii». Sbornik trudov konferentsii. M.: NII RL MGTU im. N.E. Baumana. 2015, pp. 41-43.
10. Bykov A.Yu., Shmatova E.S. Algoritmy raspredeleniya resursov dlya zashchity informatsii mezhdu ob"ektami informatsionnoy sistemy na osnove igrovoy modeli i printsipa ravnomernoy zashchishchennosti ob"ektov, Nauka i obrazovanie. [Elektronnyy resurs]. M.: MGTU im. N.E. Baumana. 2015. No 9, pp. 160-187. Rezhim dostupa: http://technomag.bmstu.ru/doc/812283.html.
11. Sheremet I.A. Ugrozy tekhnosfere Rossii i protivodeystvie im v sovremennykh usloviyakh // Vestnik akademii voennykh nauk. 2014. No 1 (46), pp. 27-34.