НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
сентябрь–октябрь 2016 Том 16 № 5 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
September–October 2016 Vol. 16 No 5 ISSN 2226-1494 http://ntv.ifmo.ru/en
УНИВЕРСИТЕТ ИТМО

УДК 004.056

РАЗРАБОТКА ВЕРОЯТНОСТНОЙ ПОВЕДЕНЧЕСКОЙ МОДЕЛИ ДЛЯ ЗАЩИТЫ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ ДЕРЕВЬЕВ АТАК

Н.А. Дородников[a], С.А. Арустамов[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: nucleofag@gmail.com

Информация о статье
Поступила в редакцию 02.08.16, принята к печати 30.08.16
doi: 10.17586/2226-1494-2016-16-5-960-962
Язык статьи – русский

Ссылка для цитирования: Дородников Н.А., Арустамов С.А. Разработка вероятностной поведенческой модели для защиты вычислительной сети с использованием деревьев атак // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 5. С. 960–962. doi: 10.17586/2226-1494-2016-16-5-960-962

Аннотация

Приведены результаты разработки вероятностной поведенческой модели вычислительной сети. Представлен способ моделирования состояния системы, начиная непосредственно с момента атаки. Для описания угроз подобран набор из соответствующих типов математических моделей процессов. Предложена модификация теории деревьев атак – вероятностные деревья атак, описывающие пути достижения целей злоумышленниками и позволяющие вычислять вероятности реализации различных угроз. Предложенный метод позволяет с помощью моделирования поведения системы производить оценку уровней рисков и защищенности исследуемых вычислительных сетей.

Ключевые слова

вероятностные деревья атак, поведенческая модель вычислительной сети, вероятность реализации угрозы, оценка уровня защищенности, моделирование атаки

PROBABILISTIC BEHAVIORAL MODEL FOR COMPUTER NETWORK PROTECTION BASED ON ATTACK TREES

N.A. Dorodnikov[a], S.A.Arustamov[a]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: nucleofag@gmail.com

Article info
Received 02.08.16, accepted 30.08.16
doi: 10.17586/2226-1494-2016-16-5-960-962
Article in Russian

For citation: Dorodnikov N.A., Arustamov S.A. Probabilistic behavioral model for computer network protection based on attack trees. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2016, vol. 16, no. 5, pp. 960–962. doi: 10.17586/2226-1494-2016-16-5-960-962

Abstract

The paper deals with the results of probabilistic model development for behavioral computer network. We present a method for the system state simulation immediately after the attack. To describe the threats we have selected an appropriate set of mathematical models for processes. The authors have proposed a modification of the attack trees theory including probabilistic attack trees, describing the ways to achieve objectives by illegal intruders and calculating the probability of the various types of threats. The proposed method enables to assess the levels of risks and vulnerability of the studied networks with the aid of the system behavior simulation.

Keywords

probabilistic attack trees, computer network behavioral model, threat probability, vulnerability level assessment, attack simulation

На сегодняшний день при растущих потоках данных и повсеместном использовании автоматизированных систем проблема обеспечения информационной безопасности локальных сетей является очень актуальной. Для решения данной задачи обычно предлагается использовать какую-либо из существующих методик оценки риска, однако их пригодность для использования в вычислительных сетях вызывает

сомнения, так как они, как правило, направлены на оценку рисков финансовых параметров организаций и не учитывают структурно-технологические особенности вычислительных сетей. К тому же для анализа защищенности вычислительных сетей важно наблюдать динамику распространения угроз в них.

При этом возникает проблема построения эффективной имитационной и математической моделей, с достаточной полнотой описывающих поведение сети в момент проведения на нее атаки, оценка изменения состояния ее узлов и элементов, учитывающая возможные источники и пути распространения атак, особенности построения исследуемой сети, наличие резервирования функционала. Эти факторы позволяют оценить устойчивость к атакам каждого элемента сети в отдельности.

Для описания вычислительных сетей ранее [1] было предложено понятие квазиподсети как средства описания защищаемой сети. Корнем квазиподсети является маршрутизирующий элемент, а ее элементами являются маршрутизирующие и коммутирующие элементы, оборудование провайдера, группы пользователей с указанием VLAN (виртуальных групп устройств), серверы, конечные узлы, виртуальные серверы, вложенные квазиподсети. Каждому типу узла соответствует свой набор определенных параметров оборудования.

Деревья атак для анализа воздействий на информационные системы начали применяться достаточно давно. В литературе [2–5] также встречаются «графы атак», «деревья ошибок», «деревья риска» – по сути, синонимы.

Дерево атак представляется последовательностью действий, которые должен совершить злоумышленник, чтобы достичь определенной цели. В качестве корневого узла (вершины дерева) выступает основная цель, которую предполагает достичь нарушитель. Каждый узел в дереве представляет промежуточную цель, достижение которой позволяет нарушителю перейти на более «высокий» уровень по отношению к достижению основной цели. Достижение корня означает, что злоумышленник успешно реализовал задуманную атаку.

Поведение системы в момент атаки является вероятностным процессом. Иными словами, нельзя точно утверждать, что система будет скомпрометирована за определенное время. С увеличением интервала времени вероятность компрометации стремится к единице. Однако можно оценить вероятность того, что система будет скомпрометирована за определенное время, т.е. определить некоторый вероятностный интервал (например, 0,4–0,6), соответствующий заданному времени. С учетом этого обстоятельства вводится понятие функции вероятности реализации угрозы, зависящей от заданного времени $P(t)$:

$P(t) \in [0;1]$, $t = [0;+\infty)$.

Моделирование состояния системы производится непосредственно с момента атаки, т.е. момент при $t = 0$ является моментом начала атаки. Время t здесь выступает в роли бесконечного счетчика, т.е. представляет собой дискретную бесконечную временную модель.

Для описания угроз на основе теории вероятностей и математической статистики задается набор из различных типов математических моделей процессов, таких как:

- процесс с постоянной интенсивностью;
- процесс с промежуточным элементом;
- процесс с использованием резервирования при постоянной интенсивности;
- процесс с накапливаемым действием;
- процесс с замедленным действием;
- процесс со ступенчатыми потерями работоспособности;
- процесс без восстановления состояния;
- процесс с восстановлением состояния.

Каждый из процессов используется при описании атакующих действий в деревьях атак. Различные коэффициенты в моделях процессов зависят от параметров оборудования элементов квазиподсети.

Для описания предложенной модели используется модификация теории деревьев атак – вероятностные деревья атак, описывающие пути достижения целей злоумышленниками и включающих в себя введение композиции «УИ» (Упорядоченное И), функции вероятности $P(t)$, возможность указания временного интервала атакующего действия для каждого из поддеревьев и возможность указания уровня сложности атакующего действия для злоумышленника.

Каждый листовой узел (элементарная угроза) каждого дерева атак описывается функцией $P(t)$, вид которой зависит от математической модели реализации конкретной угрозы. Для вычисления $P(t)$ для подцелей и непосредственно целей деревьев атак приводятся соответствующие формулы (в зависимости от композиции: «И», «ИЛИ», «УИ», их комбинации, вложенность и прочее), с учетом временных интервалов и уровней сложности атакующих действий.

Для заданной квазиподсети автоматически генерируются несколько деревьев атак.

1. Выбираются все варианты целей атаки (все узлы).
2. Для каждой цели строятся два дерева атак (дерево атак на доступность и дерево атак на конфиденциальность).
3. Учитываются узлы, с которых может происходить атака на конкретную цель.

4. Получаются по два дерева для каждой цели, и каждый узел снабжен функцией вероятности $P(t)$ реализации конкретной угрозы.
5. Для внутренних атак листья дерева находятся внутри сети, а для внешней – корневой маршрутизатор.

Таким образом, предложенная модель позволяет оценить вероятности $P(t)$ каждого дерева атак с течением времени, которые, в свою очередь, позволят произвести количественную оценку уровней рисков информационной безопасности и уровня защищенности вычислительной сети [6].

Литература

1. Дородников Н.А., Безбородов Л.А., Арустамов С.А., Дородникова И.М. Разработка математической модели универсальной ЛВС с учетом требований информационной безопасности // Научно-технический вестник Поволжья. 2015. №2. С. 115–118.
2. Chechulin A., Kotenko I. Attack tree-based approach for real-time security event processing // Automatic Control and Computer Sciences. 2015. V. 49. N 8. P. 701–704. doi: 10.3103/S0146411615080052
3. Opdahl L., Sindre G. Experimental comparison of attack trees and misuse cases for security threat identification // Information and Software Technology. 2009. V. 51. N 5. P. 916–932. doi: 10.1016/j.infsof.2008.05.013
4. Zhao J.J., Zhao S.Y. Opportunities and threats: a security assessment of state e-government websites // Government Information Quarterly. 2010. V. 27. N 1. P. 49–56. doi: 10.1016/j.giq.2009.07.004
5. Kotenko I., Doynikova E., Chechulin A. Security metrics based on attack graphs for the Olympic Games scenario // Proc. 22th Euromicro Int. Conf. on Parallel, Distributed, and Network-Based Processing (PDP 2014). Turin, Italy, 2014. P. 561–568. doi: 10.1109/PDP.2014.113
6. Дородников Н.А. Реализация генетического алгоритма расчета параметров модели универсальной ЛВС в момент противодействия угрозам информационной безопасности // Научно-технический вестник Поволжья. 2015. №3. С. 126–128.

References

1. Dorodnikov N.A., Bezborodov L.A., Arustamov S.A., Dorodnikova I.M. Development of a mathematical model of a universal LAN based on requirements information security. *Scientific and Technical Volga region Bulletin*, 2015, no. 2, pp. 115–118.
2. Chechulin A., Kotenko I. Attack tree-based approach for real-time security event processing. *Automatic Control and Computer Sciences*, 2015, vol. 49, no. 8, pp. 701–704. doi: 10.3103/S0146411615080052
3. Opdahl L., Sindre G. Experimental comparison of attack trees and misuse cases for security threat identification. *Information and Software Technology*, 2009, vol. 51, no. 5, pp. 916–932. doi: 10.1016/j.infsof.2008.05.013
4. Zhao J.J., Zhao S.Y. Opportunities and threats: a security assessment of state e-government websites. *Government Information Quarterly*, 2010, vol. 27, no. 1, pp. 49–56. doi: 10.1016/j.giq.2009.07.004
5. Kotenko I., Doynikova E., Chechulin A. Security metrics based on attack graphs for the Olympic Games scenario. *Proc. 22th Euromicro Int. Conf. on Parallel, Distributed, and Network-Based Processing, PDP 2014*. Turin, Italy, 2014, pp. 561–568. doi: 10.1109/PDP.2014.113
6. Dorodnikov N.A. Realizing genetic algorithms calculating the parameters of the model of universal LAN while counteract information security threats. *Scientific and Technical Volga region Bulletin*, 2015, no. 3, pp. 126–128.

Авторы

Дородников Николай Александрович – аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, nucleofag@gmail.com

Арустамов Сергей Аркадьевич – доктор технических наук, профессор, профессор, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, sergey.arustamov@gmail.com

Authors

Nickolay A. Dorodnikov – postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, nucleofag@gmail.com

Sergey A. Arustamov – D.Sc., Professor, Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, sergey.arustamov@gmail.com