УДК 004.891.3
DOI: 10.17586/0021-3454-2016-59-11-928-933

ПРИМЕНЕНИЕ МЕТОДА ПРЕОБРАЗОВАНИЯ СТОХАСТИЧЕСКИХ СЕТЕЙ ДЛЯ МОДЕЛИРОВАНИЯ МОБИЛЬНЫХ БАНКОВСКИХ АТАК

И. Б. САЕНКО[1,2], О. С. ЛАУТА[2], И. В. КОТЕНКО[1,3]

[1] *Санкт-Петербургский институт информатики и автоматизации РАН, 199178, Санкт-Петербург, Россия*
E-mail: ibsaen@comsec.spb.ru

[2] *Военная академия связи им. С. М. Буденного, 194064, Санкт-Петербург, Россия*

[3] *Университет ИТМО, 197101, Санкт-Петербург, Россия*

Предложен подход к моделированию мобильных банковских атак, основанный на методе преобразования стохастических сетей, достоинствами которого являются достаточно высокая скорость моделирования, а также высокая достоверность и чувствительность результатов к изменению исходных данных. Приведены результаты экспериментальной оценки, подтверждающие достаточно высокую эффективность метода.

Ключевые слова: *мобильная безопасность, моделирование атак, мобильные банковские атаки, стохастические сети, преобразование Лапласа*

Введение. В настоящее время участились атаки злоумышленников на мобильные устройства, при этом используются новые угрозы их безопасности. Известно более 650 тыс. отдельных образцов вредоносного программного обеспечения для платформы Android [1], среди которых наиболее распространенными являются SMS-трояны, рекламные модули и эксплойты для получения доступа root-уровня.

Многие коммерческие банки и платежные системы предлагают различные способы защиты мобильных финансовых операций пользователей. Тем не менее злоумышленниками разрабатываются новые программы, позволяющие обходить эти защитные меры. Примером является вредоносная программа ZitMo (Zeus-in-the-MObile), способная обходить двухфакторную проверку подлинности [2].

Для оценивания риска мобильных банковских атак необходимы аналитические модели, позволяющие исследовать вероятностные параметры атак. Среди различных подходов к построению вероятностных моделей атак в последнее время все большую популярность приобретает метод, основанный на преобразовании стохастических сетей [3], отличающийся высокой точностью и устойчивостью. Применение этого подхода для построения и исследования аналитической модели мобильной банковской атаки на примере программы ZitMo обсуждается в настоящей статье.

Обзор публикаций. Стохастическое аналитическое моделирование лежит в основе функционирования многих систем моделирования дискретных событий, например COMNET [4]. Однако эта система предназначена для моделирования сетей массового обслуживания, что требует значительных вычислительных затрат.

В работах [5, 6] рассмотрена система CAMIAC (Cyber Attack Modeling and Impact Assessment Component), основанная на анализе графов атак и стохастической имитации атак и контрмер. Моделирование в этой системе не позволяет, однако, получить функции распределения времени атаки. Такой же недостаток присущ и подходам, предложенным в работах [7, 8], в которых учитывается распространение атак по параллельным ветвям, рассматривают-

ся отдельные сценарии безопасности, но вычисления базируются только на применении основных теорем теории вероятности.

Стохастический симулятор атак, предложенный в работе [9], основан на исчислении ситуаций; в работе [10] рассмотрены стохастические модели для различных задач в компьютерной области, основанные на дискретных марковских цепях. Подход к классификации атак с использованием обобщенных стохастических сетей представлен в работе [11]. Эти работы показали, что стохастические сети являются достаточно мощным средством моделирования, однако сценарии, связанные с моделированием атак, в них не рассматривались.

Таким образом, анализ релевантных работ показывает, что стохастические модели, необходимые для выработки контрмер в современных системах защиты информации, должны обеспечивать получение функции распределения времени атаки и ее этапов с минимальными вычислительными затратами, а также обеспечивать высокую гибкость и возможность применения для анализа атак любого типа. Рассмотренные выше подходы не в полной мере отвечают этим требованиям. Метод, предложенный в настоящей статье, позволяет устранить этот недостаток.

Стохастическая сеть для атаки ZitMo. Стохастическая сеть является моделью процесса, реализуемого системой, и представляет собой совокупность взаимосвязанных вершин и ветвей, соединение которых соответствует алгоритму функционирования системы [12]. При этом процесс декомпозируется на подпроцессы, каждый из которых характеризуется функцией распределения, средним временем и его дисперсией.

Рассмотрим построение стохастической сети на примере атаки типа ZitMo. Реализация этой атаки содержит следующие этапы:

— злоумышленник направляет на мобильное устройство жертвы (пользователя) SMS-сообщение с просьбой выполнить „обновление банковского программного обеспечения безопасности“; положим, что длительность этого этапа имеет функцию распределения $W(t)$ и среднее время $\overline{t_W}$;

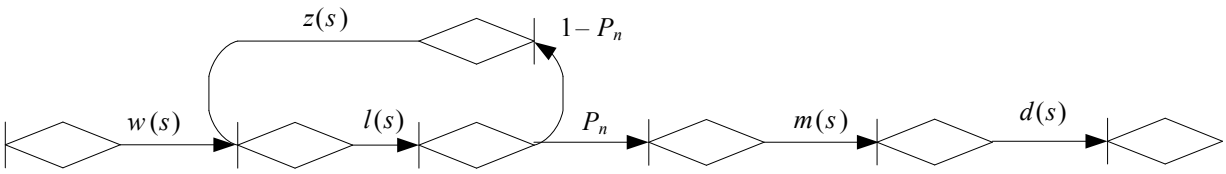
— пользователь с вероятностью P_n проходит по ссылке в сообщении, при этом мобильное устройство заражается программой ZitMo за среднее время $\overline{t_L}$ с функцией распределения времени $L(t)$;

— программа ZitMo перенаправляет злоумышленнику логин и пароль пользователя для перевода денег с его счета за среднее время $\overline{t_M}$ с функцией распределения времени $M(t)$;

— для авторизации банк отсылает пользователю SMS-сообщение с „номером авторизации“, а зараженное устройство пересылает его злоумышленнику за среднее время $\overline{t_D}$ с функцией распределения времени $D(t)$;

— если пользователь не перешел по ссылке в сообщении, то с вероятностью $(1 - P_n)$ злоумышленник повторно направляет это сообщение за среднее время $\overline{t_Z}$ с функцией распределения времени $Z(t)$.

Схема стохастической сети, отражающая этапы атаки ZitMo, представлена на рисунке. Функции $w(s)$, $l(s)$, $m(s)$, $d(s)$ и $z(s)$ на выходе узлов сети являются эквивалентными и формируются путем применения преобразования Лапласа к функциям $W(t)$, $L(t)$, $M(t)$, $D(t)$ и $Z(t)$ соответственно.



Метод преобразования стохастической сети для атаки ZitMo. Результатом преобразования стохастической сети является эквивалентная функция, позволяющая определить первые моменты случайного времени выполнения целевого процесса. Сущность метода заключается в замене множества элементарных ветвей сети одной эквивалентной и последующем определении эквивалентной функции сети, начальных моментов и функции распределения времени реализации анализируемого процесса. При этом эквивалентная функция петли k-го порядка определяется как

$$Q_k(s) = \prod_{i=1}^{k} Q_i(s), \tag{1}$$

где $Q_i(s)$ — эквивалентная функция i-й петли первого порядка, определяемая как произведение эквивалентных функций ветвей, входящих в эту петлю.

Замкнем условно выход сети на вход. Тогда для искомой эквивалентной функции $h(s)$ справедливо $h(s) = 1/Q_a(s)$, где $Q_a(s)$ — эквивалентная функция входа всей сети. При этом для определения эквивалентной функции исходной сети можно использовать уравнение Мейсона:

$$H = 1 + \sum_{k=1}^{K} (-1)^k Q_k(s) = 0, \tag{2}$$

где K — максимальный порядок петель, входящих в стохастическую сеть.

Теперь определим все петли в стохастической сети, используя выражение (1). В сети имеется две петли первого порядка. Первая петля имеет эквивалентную функцию $w(s)m(s)l(s)P_n d(s)/h(s)$, вторая — $(1-P_n)z(s)l(s)$. Петель второго и более высоких порядков нет. Эквивалентная функция всей сети в этом случае имеет следующий вид:

$$h(s) = \frac{w(s)m(s)l(s)P_n d(s)}{1-(1-P_n)z(s)l(s)}. \tag{3}$$

Используя преобразование Лапласа и разложение Хевисайда, для функции $F(t)$ распределения вероятности времени реализации атаки ZitMo и среднего времени $\overline{T}$ ее реализации можно записать следующие выражения:

$$F(t) = \sum_{k=1}^{5} \frac{wlP_n md(z+s_k)}{\varphi(s_k)} \frac{1-\exp[s_k t]}{-s_k}; \tag{4}$$

$$\overline{T} = \sum_{k=1}^{5} \frac{wlP_n md(z+s_k)}{\varphi(s_k)(-s_k)^2}, \tag{5}$$

где s_k — полюс разложения Хевисайда k-го порядка; $w = 1/\overline{t_W}$; $l = 1/\overline{t_L}$; $m = 1/\overline{t_M}$; $d = 1/\overline{t_D}$; $z = 1/\overline{t_Z}$, а функция $\varphi(s_k)$ имеет вид

$$\varphi(s_k) = (w+s_k)(d+s_k)(m+s_k)\left[(l+s_k)(z+s_k) - (1-P_n)zl\right]. \tag{6}$$

Экспериментальные результаты. Было проведено сравнение результатов расчета величины $\overline{T}_{\text{ан}}$, полученных при аналитическом моделировании с помощью уравнения (5), с результатами имитационного моделирования ($\overline{T}_{\text{им}}$) на вероятностном стенде (см. таблицу). При

этом использовались следующие исходные данные: $\overline{t_W} = 5$ с, $\overline{t_L} = 10$ с, $\overline{t_M} = 5$ с, $\overline{t_D} = 40$ с, $\overline{t_Z} = 4$ с, $P_n = 0{,}1 \ldots 0{,}9$.

P_n	$\overline{T}_{\text{ан}}$, с	$\overline{T}_{\text{им}}$, с	Погрешность, %
0,2	250	261	4,4
0,3	140	139	0,7
0,4	118	123	4,2
0,5	97	101	4,1
0,6	76	75	1,3
0,7	68	67	1,5
0,8	60	62	3,3
0,9	55	54	1,8

Анализ полученных результатов позволяет сделать следующие выводы:

— среднее время реализации атаки ZitMo при вероятности перехода пользователя по ссылке в сообщении $P_n = 0{,}8$ составляет 60 с;

— уменьшение вероятности перехода значительно увеличивает среднее время реализации вредоносной программы;

— погрешность оценки времени реализации атаки не превышает 5 %, что подтверждает корректность предложенной аналитической модели и метода ее формирования.

Заключение. Предложен новый подход к аналитическому моделированию компьютерных атак, основанный на методе преобразования стохастических сетей. Сущность данного метода заключается в замене множества элементарных ветвей стохастической сети одной эквивалентной ветвью и последующем определении эквивалентной функции сети, а также начальных моментов и функции распределения случайного времени реализации компьютерной атаки. Проверка подхода была произведена при моделирования атаки ZitMo, которая является наиболее характерной и опасной мобильной банковской атакой.

Полученные аналитические выражения позволяют использовать результаты моделирования для выявления причин низкой защищенности элементов мобильных сетей и обоснования мер противодействия мобильным атакам.

Перспективные исследования связаны с применением предложенного метода для моделирования целевых атак.

Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, государственной финансовой поддержке ведущих университетов Российской Федерации (субсидия 074-U01), а также Российского научного фонда (грант 15-11-30029).

СПИСОК ЛИТЕРАТУРЫ

1. *Svajcer V*. Sophos mobile security threat report // Mobile World Congress. SophosLabs, 2014.
2. *Dmitrenko A., Liebchen Ch., Rossow Ch., Sadeghi A.-R.* Security analysis of mobile two-factor authentication schemes // Intel Technology Journal. 2014. Vol. 18(4). P. 138—161.
3. *Привалов А. А.* Метод топологического преобразования стохастических сетей и его использование для анализа сетей связи ВМФ. СПб: ВМА, 2000.
4. *Ahuja S. P.* COMNET III: A network simulation laboratory environment for a course in communications networks // 28th Annual Frontiers in Education: Conf. Proc. (FIE '98). 1998. Vol. 3. P. 1085—1088.
5. *Kotenko I., Chechulin A.* A Cyber attack modeling and impact assessment framework // Proc. of the 5th IEEE Intern. Conf. on Cyber Conflict (CyCon). 2013. P. 1—24.

6. *Kotenko I., Polubelova O., Saenko I.* The ontological approach for SIEM data repository implementation // Proc. of 2012 IEEE Intern. Conf. on Green Computing and Communications. 2012. С. 761—766.

7. *Goldman R. P.* A stochastic model for intrusions // Proc. of the 5th Intern. Symp. (RAID 2002). 2002. P. 199—218.

8. *Gorodetski V., Kotenko I.* Attacks against computer network: formal grammar-based framework and simulation tool // Lecture Notes in Computer Science. 2002. Vol. 2516. P.219—238.

9. *Dudorov D., Stupples D., Newby M.* Probability analysis of cyber attack paths against business and commercial enterprise systems // Proc. of 2013 European Intelligence and Security Informatics Conf. 2013. P. 38—44.

10. *Matlof N.* From Algorithms to Z-Scores: Probabilistic and Statistical Modeling in Computer Science [Электронный ресурс]: <htttp://heather.cs.ucdavis.edu/probstatbook>.

11. *Zöhrer M., Pernkopf F.* General stochastic networks for classification // Advances in Neural Information Processing Systems. 2014. Vol. 27. P. 2015—2023.

12. *Serfozo R. F.* Introduction to stochastic networks // Applications of Mathematics. 1999. Vol. 44.

Сведения об авторах

Игорь Борисович Саенко — д-р техн. наук, профессор; СПИИРАН, лаборатория проблем компьютерной безопасности; Военная академия связи им. С. М. Буденного, кафедра автоматизированных систем специального назначения; E-mail: ibsaen@ comsec.spb.ru

Олег Сергеевич Лаута — канд. техн. наук; Военная академия связи им. С. М. Буденного, кафедра безопасности информационно-телекоммуникационных систем специального назначения; E-mail: laos_82@yandex.ru

Игорь Витальевич Котенко — д-р техн. наук, профессор; СПИИРАН, лаборатория проблем компьютерной безопасности; Университет ИТМО, кафедра информационных систем; E-mail: ivkote@comsec.spb.ru

Рекомендована СПИИРАН

Поступила в редакцию
01.06.16 г.

Ссылка для цитирования: *Саенко И. Б., Лаута О. С., Котенко И. В.* Применение метода преобразования стохастических сетей для моделирования мобильных банковских атак // Изв. вузов. Приборостроение. 2016. Т. 59, № 11. С. 928—933.

APPLICATION OF STOCHASTIC NETWORKS CONVERSION TECHNIQUE FOR SIMULATION OF MOBILE BANKING ATTACKS

I. B. Saenko[1,2], O. S. Lauta[2], I. V. Kotenko[1,3]

[1] *St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, 199178, St. Petersburg, Russia*
E-mail: ibsaen@comsec.spb.ru

[2] *Marshal S. M. Budyonny Military Academy of Telecommunications, 194064, St. Petersburg, Russia*

[3] *ITMO University, 197101, St. Petersburg, Russia*

An approach to modeling mobile banking attacks is proposed. The approach is based on stochastic network conversion technique providing a high speed of modeling, high reliability, and high sensitivity of results to change in initial data. Results of experimental assessment of the proposed method are presented to confirm efficiency of the developed approach.

Keywords: mobile security, attack modeling, mobile banking attack, stochastic networks, Laplace transform

Data on authors

Igor B. Saenko — Dr. Sci., Professor; SPIIRAS, Laboratory of Computer Security Problems; Marshal S.M. Budyonny Military Academy of Telecommunications, Department of Automated Systems for Special Purposes; E-mail: ibsaen@mail.ru

Oleg S. Lauta — PhD; Marshal S. M. Budyonny Military Academy of Telecommunications, Department of the Security of Information-Telecommunication Systems for Special Purposes; E-mail: laos_82@yandex.ru

Igor V. Kotenko — Dr. Sci., Professor; SPIIRAS, Laboratory of Computer Security Problems; ITMO University, Department of Information Systems; E-mail: ivkote@comsec.spb.ru

For citation: *Saenko I. B., Lauta O. S., Kotenko I. V.* Application of stochastic networks conversion technique for simulation of mobile banking attacks // Izv. vuzov. Priborostroenie. 2016. Vol. 59, N 11. P. 928—933 (in Russian).

DOI: 10.17586/0021-3454-2016-59-11-928-933