АНАЛИЗ РАЗВИТИЯ СОЦИОИНЖЕНЕРНОЙ АТАКИ КАК СЛУЧАЙНОГО ПРОЦЕССА С ДИСКРЕТНЫМ ВРЕМЕНЕМ: ФОРМИРОВАНИЕ ПЕРЕЧНЯ НАИБОЛЕЕ УЯЗВИМЫХ ПОЛЬЗОВАТЕЛЕЙ[1]

Азаров А.А., ст. научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики СПИИРАН, заместитель директора по развитию информационных технологий ООО "Винета", artur-azarov@yandex.ru
Суворова А.В., доцент НИУ "ВШЭ", suvalv@mail.ru
Тулупьева Т.В., ст. научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики СПИИРАН, tvt100a@mail.ru
Васильева О.В., студент СПбГУ, vasiljevaa@mail.ru

Аннотация

В статье предлагается рассмотреть подход к анализу защищенности пользователей информационной системы к социоинженерным атакующим воздействиям злоумышленника. Предлагается рассмотреть изменения состояния информационной системы и пользователей этой системы, находящихся под воздействием социоинженерных атакующих воздействий злоумышленника, как случайный процесс с дискретным временем. Данный подход допускает моделирование изменения состояний системы с начального периода, когда система находится в состоянии покоя, то есть, не атакована злоумышленником. Моделирование с помощью Марковских сетей делает возможным выявление пользователей и их уязвимости, которые подвержены социоинженерным атакующим воздействиям в большей степени, чем все остальные. На основании этого анализа предлагается формировать перечень наиболее уязвимых пользователей и предполагаемый перечень мер, потенциально позволяющий повысить уровень защищенности как таких пользователей, так и информационной системы в целом.

[1] Работа проводилась при поддержке гранта РФФИ, проект №18-37-00340, и частичной поддержке по проекту по государственному заданию СПИИРАН № 0073-2019-0003

Введение

Расширение использования и, соответственно, влияния компьютерных технологий и информационных систем на большинство сфер жизни человека растет с каждым годом. Термины «цифровые технологии», «цифровая экономика» становятся неотъемлемой частью большинства новостей и используются постоянно. Такие изменения не могут не затрагивать вопросы повышения безопасности данных. Как следствие, повышаются и требования по защищенности информации; разрабатываются различные методы защиты, в основном уделяется внимание технической составляющей информационных систем [8]. Однако, показывают исследования, именно пользователи информационных систем могут стать первопричиной утечек конфиденциальной информации [6, 7, 9, 10–13].

Обилие исследований на тему защищенности пользователей информационных систем ставит крайне важную задачу осуществления своевременных действий по профилактике нежелательных последствий действий пользователей в информационных системах. Существует несколько причин утечки конфиденциальной информации от таких пользователей. Одной из причин является воздействие на пользователей извне, с целью получения конфиденциальной информации. Обобщением такого рода воздействий являются социоинженерные атакующие воздействия злоумышленника на пользователей информационных систем [1–4].

Данная статья посвящена рассмотрению подхода к анализу защищенности пользователей информационной системы к социоинженерным атакующим воздействиям злоумышленника. При этом, изменения состояния информационной системы, то есть получения злоумышленником доступа к тем или иным конфиденциальным данным, представлены в виде случайного процесса с дискретным временем. Данный подход допускает не только моделирование изменения состояний системы с начального периода, когда система находится в состоянии покоя, то есть не атакована злоумышленником, но и делает возможным выявление пользователей и их уязвимости, которые подвержены социоинженерным атакующим воздействиям в большей степени, чем все остальные. Последовательное моделирование шагов алгоритма позволит выявить состояния системы, в которых вероятности успеха социоинженерных атакующих воздействий выше определенного порогового значения, являющегося приемлемым уровнем защиты информационной системы.

Описание моделей и алгоритмов

В статье рассматриваются модели, ранее предложенные в работах [1–3]. В комплекс «критичные документы — информационная система — персонал — злоумышленник», подлежащий рассмотрению, входит набор моделей, отображающих пользователя и его поведение в информационной системе. Одним из важнейших элементов является профиль уязвимостей пользователя $\left(\left(V_1, V_1(\mathrm{D})\right),...,\left(V_k, V_k(\mathrm{D})\right)\right)$, где $V_1,...,V_k$ — уязвимости пользователя, $V_1(\mathrm{D}),...,V_k(\mathrm{D})$ — степень выраженности уязвимостей. В зависимости от степени выраженности может быть построена вероятность успеха социоинженерного атакующего воздействия $p_i = \dfrac{V_i(D)}{V_i(\max)}$.

Другим элементом, который следует принять к рассмотрению, являются связи между пользователями, на основании которых может быть построен граф социальных связей пользователей с нагруженными двунаправленными дугами и нагруженными вершинами. Весами дуг являются вероятности перехода от пользователя к пользователю, сформированные на основании типа связей пользователей, а весом каждой вершины — вектор вероятностей успеха социоинженерного атакующего воздействия на отдельные уязвимости пользователя информационной системы [5].

Ранее были предложены подходы к анализу защищенности пользователей информационных систем через деревья атак [1–3], данный подход позволял выстраивать все возможные пути развития социоинженерной атаки среди пользователей информационной системы, при этом необходимо было задавать «точку входа», то есть пользователя, на которого совершается первое социоинженерное атакующее воздействие пользователя. Таким образом, вероятность успеха социоинженерного атакующего воздействия на первого пользователя имела существенное влияние на расчет вероятности доступа злоумышленника к определенной критичной информации через цепочку пользователей. Позднее был предложен подход к анализу графа социальных связей [4], который позволял проводить анализ графа различных конфигураций, производя расчет сразу ряда показателей; в данном подходе также предлагалось рассматривать определенные «точки входа», хотя предлагалось рассматривать сразу несколько таких точек. В качестве расширения предлагается подход к анализу защищенности пользователей информационных систем на основе случайного процесса с дискретным временем. Это делает возможным выявление пользователей, которые

подвержены социоинженерным атакующим воздействиям в большей степени чем все остальные. Последовательное моделирование шагов алгоритма позволит выявить состояния системы, в которых вероятности успеха социоинженерных атакующих воздействий выше определенного порогового значения, являющегося приемлемым уровнем защиты информационной системы.

При моделировании случайного процесса с дискретным временем, положим $S_1,...,S_n$ состояниями системы. Под состоянием системы мы будем понимать развитие социоинженерной атаки злоумышленника, т.е. реализацию того или иного социоинженерного атакующего воздействия. Состояниями системы, изменяющими ее конфигурацию, могут быть: успех определенного социоинженерного атакующего воздействия и переход по связи пользователь-пользователь, в случае если социоинженерная атака прошла успешно. Каждому из этих событий сопоставлена определенная вероятность, основанная на данных из графа социальных связей пользователей. В рассматриваемой парадигме, переходы между состояниями возможны только в строго определенный момент времени $t_1,...,t_n$. Данными моментам являются социоинженерные атакующие воздействия злоумышленника.

Будем рассматривать однородную марковскую цепь, т.е. подразумеваем, что переход алгоритма не зависит от номера шага. В таком случае, состояния системы и переходы между ними могут быть представлены в виде графа (рис.1)

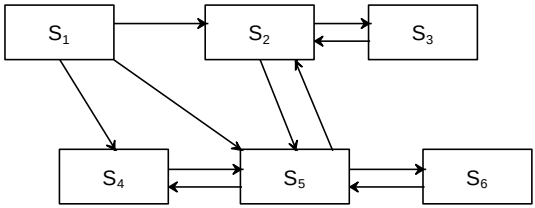

Рис.1. Граф состояний системы

Обозначим через p_{ij} вероятность перехода от одного состояния системы в другое. Как было обозначено, эти вероятности отражены в графе социальных связей. Таким образом, может быть получена матрица

$$\left\| P_{ij} \right\| = \begin{pmatrix} p_{11} p_{12} \cdots p_{1m} \\ \\ p_{n1} p_{n2} \cdots p_{nm} \end{pmatrix}$$

Каждая вероятность p_{ij} — это вероятность перехода системы в новое состояние. Не умаляя общности, на первом шаге работы алгоритма эта вероятность может быть представлена как вероятность поражения пользователя на прямую. Второй и последующий шаги — вероятность события, что пользователь будет поражен или через связи пользователь – пользователь, или напрямую. В данной статье рассмотрим вероятность успеха отдельного социоинженерного атакующего воздействия на отдельную уязвимость пользователя. Тогда вероятность p_{ij} может быть представлена в виде $p_{ij} = 1 - p_{u_j} \prod_{l=1}^{z} \left(1 - p_{lu_j} p_l\right)$, где p_{u_j} — вероятность поражения пользователя u_j определенным социоинженерным атакующим воздействием, p_{lu_j} — вероятности перехода по связям между пользователями l к пользователю u_j, p_l — вероятность поражения пользователя l, пораженного злоумышленником на предыдущем шаге атаки.

Далее может быть произведен расчет вероятностей того, что злоумышленника за k шагов получит конфиденциальную информацию от определенных пользователей. В зависимости от решаемой задачи, могут быть поставлены и другие исследовательские вопросы, как то: за какое минимальное количество шагов вероятность успеха социоинженерного атакующего воздействия перейдет за пороговые значения, какие пользователи будут наиболее подвержены социоинженерным атакующим воздействиям злоумышленника за определенное число шагов и другие.

Вычислительный эксперимент

Разберем пример анализа защищенности пользователей информационной системы на основе графа социальных связей (рис. 2):

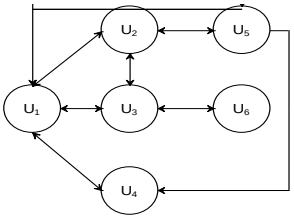

Рис. 2. Пример графа социальных связей между пользователями

Вероятностные оценки нагрузки вершин и дуг данного графа могут быть представлены в виде матрицы $\|P\|$. Она представима в виде:

$$\|P\| = \begin{pmatrix} 0,1 & 0,06 & 0,07 & 0,08 & 0 & 0 \\ 0,04 & 0,15 & 0,01 & 0 & 0,07 & 0 \\ 0,05 & 0,09 & 0,2 & 0 & 0 & 0,03 \\ 0,08 & 0 & 0 & 0,11 & 0 & 0 \\ 0,03 & 0,09 & 0 & 0,07 & 0,19 & 0 \\ 0 & 0 & 0,04 & 0 & 0 & 0,2 \end{pmatrix}$$

По диагонали в данной матрице стоят вероятности успешного социоинженерного атакующего воздействия на пользователей информационной системы, а на других позициях матрицы стоят вероятности перехода от пользователя к пользователю.

На основании рассматриваемого графа социальных связей пользователей может быть построен набор состояний информационной системы. Отдельное состояние — состояние системы в котором поражено какое-то количество пользователей. В рассматриваемом случае таких состояний будет 64. Состояния могут быть представлены в виде графа. Приведем фрагмент данного графа (рис. 3).

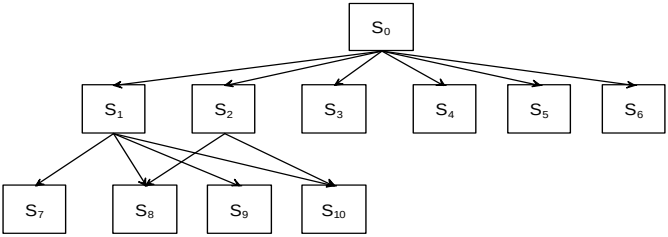

Рис. 3. Фрагмент графа состояний для системы из шести пользователей

Состояние S_0 — это начальное состояние системы, состояния $S_1, \dots, S_6$— состояния системы, когда атакован один из пользователей. Состояния $S_7, \dots, S_{10}$ — состояния системы, когда атакованными являются два пользователя, эти состояния возникают из предыдущих состояний системы, т.е. уже известно какой пользователь был атакован ранее. Построение матрицы переходов системы из состояния в состояние было описано выше.

Результаты представлены в таблице 1.

Таблица 1

Изменение степеней проявления уязвимости при распространении атаки

Пользователь	шаг1	шаг2	шаг3	швг4	шаг5	шаг6	шаг7	шаг8	шаг9	шаг10
user1	0.100	0.103	0.106	0.109	0.112	0.114	0.118	0.121	0.124	0.127
user2	0.150	0.152	0.155	0.157	0.160	0.163	0.165	0.168	0.171	0.174
user3	0.200	0.204	0.208	0.212	0.216	0.220	0.224	0.228	0.232	0.237
user4	0.110	0.111	0.112	0.112	0.113	0.114	0.115	0.116	0.117	0.118
user5	0.190	0.194	0.197	0.201	0.205	0.209	0.213	0.217	0.221	0.225
user6	0.200	0.201	0.203	0.204	0.205	0.207	0.208	0.209	0.211	0.212

Вероятность поражения системы на первом шаге 0.65, на третьем 0.66, на 10 – 0.70, на 30 – 0.82. Также из представленной таблицы могут быть выделены пользователи с наихудшими оценками защищенности.

Заключение

В статье рассмотрен метод оценки защищенности пользователей информационной системы от социоинженерной атаки злоумышленника. Рассматривается многоходовая социоинженерная атака, то есть атака, которая затрагивает нескольких пользователей информационной системы, и формируется вероятность поражения информационной системы на каждом шаге атаки. При этом сделано допущение о неограниченных

ресурсах злоумышленника. Дальнейшее развитие исследований может лежать в использовании аналогичного подхода к оценке защищенности пользователей информационной системы, но с ограниченными ресурсами злоумышленника.

Литература

1. Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Модель профиля компетенций злоумышленника в задаче анализа защищённости персонала информационных систем от социоинженерных атак // Информационно-управляющие системы. 2016. №4. С. 77–84.
2. Азаров А.А., Тулупьев А.Л., Соловцов Н.Б., Тулупьева Т.В. SQL-представление реляционно-вероятностных моделей социо-инженерных атак в задачах расчета агрегированных оценок защищенности персонала информационной системы с учетом весов связей между пользователями // Труды СПИИРАН. 2013. Вып. 24. С. 41–53.
3. Азаров А.А., Тулупьев А.Л., Соловцов Н.Б., Тулупьева Т.В. Ускорение расчетов оценки защищенности пользователей информационной системы за счет элиминации маловероятных траекторий социо-инженерных атак // Труды СПИИРАН. 2013. 2(25). С. 171-181.
4. Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социоинженерные атаки. Проблемы анализа. СПб.: Наука, 2016. 352 с.
5. Azarov A.A., Abramov M.V., Tulupyev A.L., Tulupyeva T.V. Models and algorithms for the information system's users' protection level probabilistic estimation // Proceedings of the First International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'16): Volume 2. – 2016. – pp. 39-46.
6. Gupta B.B., Tewari A., Jain A.K., Agrawal D.P. Fighting against phishing attacks: state of the art and future challenges // Neural Computing and Applications. 2017. Vol. 28, No. 12. P. 3629–3654.
7. Huda A.S.N., Živanović R. Accelerated distribution systems reliability evaluation by multilevel Monte Carlo simulation: implementation of two discretisation schemes // IET Generation, Transmission & Distribution. 2017. Vol. 11, No. 13. P. 3397–3405.
8. Kotenko I., Chechulin A., Branitskiy A. Generation of Source Data for Experiments with Network Attack Detection Software. Journal of Physics: Conference Series. — IOP Publishing, 2017. — Vol. 820. — № 1. — P. 012033.
9. Liu J., Lyu Q., Wang Q., Yu X. A digital memories based user authentication scheme with privacy preservation // PloS ONE. 2017. Vol.

12, No. 11. P. 0186925.
10. Schaik P., Jeske D., Onibokun J., Coventry L., Jansen J., Kusev P. Risk perceptions of cyber-security and precautionary behavior // Computers in Human Behavior. 2017. Vol. 62, Issue 11. P. 5678–5693.
11. Struharik R., Vukobratović B. A system for hardware aided decision tree ensemble evolution // Journal of Parallel and Distrib-uted Computing. 2018. Vol. 112. P. 67–83.
12. Terlizzi M.A., Meirelles F.S., Viegas Cortez da Cunha M.A. Behavior of Brazilian Banks Employees on Facebook and the Cybersecurity Governance // Journal of Applied Security Research. 2017. Vol. 12, No. 2. P. 224–252.
13. Willighagen E., Ballings M. genalg: R Based Genetic Algorithm. R package version 0.2.0. 2015. URL: https://CRAN.R-project.org/package=genalg