Подходы к моделированию сценариев развития многоходовых социоинженерных атак

А. О. Хлобыстова
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
aok@dscs.pro

А. Л. Тулупьев
Санкт-Петербургский государственный университет
alt@dscs.pro

***Аннотация*. Цифровизация современного общества влечёт за собой повышение качества и рост количества кибератак. При этом наиболее эффективным способом нарушения конфиденциальности организации являются социоинженерные атаки, реализация которых основывается на использовании нетехнических уязвимостей системы. Частным видом таких атак являются многоходовые социоинженерные атаки, когда при совершении атаки задействуется сразу цепочка пользователей. Настоящая работа направлена на улучшение подходов к моделированию сценариев развития многоходовой социоинженерной атаки за счёт учёта прямых действий злоумышленника, перехода атаки между двумя пользователями и опосредованной атаки на пользователя.**

Ключевые слова: социоинженерные атаки, социальный граф, сценарий развития многоходовой социоинженерной атаки, критичные узлы, информационная система

I. Введение

В наше время наиболее распространённым методом нарушения информационной безопасности остаются социоинженерные атаки [1−3]. Под социоинженерной атакой понимается набор прикладных психологических и аналитических приемов, которые злоумышленники применяют для скрытой мотивации пользователей публичной или корпоративной сети к нарушениям устоявшихся правил и политик в области информационной безопасности [4].

В настоящий момент российские и зарубежные исследователи активно работают над проблемой повышения уровня защищённости организации от социоинженерных атак. Так существует ряд работ, исследующих различные способы по увеличению осведомлённости пользователей о социоинженерных атаках [5−7]; работы, в которых разрабатываются обучающие компьютерные игры [8−9]; веб-приложение-сканер, позволяющий определять уровень уязвимостей сотрудников при приёме на работу и в дальнейшем на основе собранной информации производить выборочное обучение сотрудников [10]. Однако такие меры по большей части направлены на защиту от прямого социоинженерного воздействия. В то время как для организаций наибольшую опасность представляют многоходовые социоинженерные атаки, при которых с целью заполучения наибольшей выгоды злоумышленниками задействуется сразу цепочка пользователей [11].

Данная статья направлена на улучшение подходов к моделированию многоходовых социоинженерных атак на пользователя. Значимость исследования заключается в создании основы для разработки автоматизированного комплекса по выявлению наиболее критичных узлов информационной системы в контексте социоинженерных атак.

II. Постановка задачи

В качестве основы для моделирования многоходовых социоинженерных атак удобно использовать социальный граф сотрудников организации, вершины которого ассоциированы с пользователями информационной системы, а дуги — это связи между ними [4][4]. С математической точки зрения социальный граф – это взвешенный орграф $G = (U, E)$, где $U = \{U_i\}_{i=1}^{n}$ – множество вершин (пользователей), $E = \{(U_i, \mathrm{U}_j, p_{ij})\}_{1 \le i, j \le n, i \ne j}$ – множество упорядоченных троек с заданной оценкой вероятности распространения атаки от пользователя U_i к пользователю U_j.

Оценка вероятности успеха распространения многоходовой опосредованной атаки злоумышленника на пользователя U_j, при которой точкой входа является пользователь U_i, может быть найдена согласно следующей формуле [4]:

$$p_{\mathrm{Tr}} = p_i \prod_{l=i}^{j-1} \left(1 - p_{l(l+1)}\right) = \exp\left\{ \ln \frac{1}{p_i} + \sum_{l=i}^{j-1} \ln \frac{1}{p_{l(l+1)}} \right\}, \quad (1)$$

где $\mathrm{Tr} = (U_i, E_i, ..., E_{j-1}, U_j)$ – сценарий развития многоходовой социоинженерной атаки, p_i – оценка вероятности успеха социоинженерной атаки на пользователя U_i, а $p_{l(l+1)}$ – вероятность распространения атаки от пользователя U_l к пользователю U_{l+1}. При этом стоит отметить, что нахождение p_i и $p_{l(l+1)}$ является сложным процессом, базирующемся на получении

Работа выполнена по ГЗ СПб ФИЦ РАН № 0073-2019-0003; поддержана Санкт-Петербургским государственным университетом, проект № 73555239; при финансовой поддержке РФФИ, проект №20-07-00839.

нечеткой, неполной, нечисловой информации от самих сотрудников организации и/или при извлечении их из цифровых следов, подробнее в [4, 12, 13].

Также в [4] в качестве модели расчёта оценок защищённости пользователей от многоходовых социоинженерных атак предлагалось агрегировать оценки всех возможных траекторий реализации социоинженерной атаки. Оценку вероятности успеха социоинженерной атаки злоумышленника на пользователя U_k по всем возможным траекториям предлагалось рассчитывать следующим образом:

$$P_{U_k} = 1 - \prod_{\mathrm{Tr}} (1 - p_{\mathrm{Tr}}), \qquad (2)$$

где $\mathrm{Tr} = (U_i, E_i, ..., E_{k-1}, U_k)$ – сценарий развития многоходовой социоинженерной атаки, конечной точкой, которого является пользователь U_k, p_{Tr} – оценка вероятности успеха распространения многоходовой атаки злоумышленника по данной траектории.

Однако модели (1) и (2) не учитывают то, как будут реагировать на социоинженерную атаку пользователи, через которых она распространяется, кроме того, в данные модели не входит реакция на атаку конечного пользователя (U_k). Таким образом, целью настоящей работы стало улучшение подходов к моделированию сценариев развития многоходовой социоинженерной атаки за счёт учёта прямых действий злоумышленника, перехода атаки между двумя пользователями и действию опосредованной атаки на пользователя.

III. Релевантные работы

Обзор и категоризация методов прогнозирования популярности и распространения информации были представлены в работе [14], в том числе авторы описывают различные графовые модели. Метрика для моделирования каскадных графов, включающая себя силу связи между двумя учетными записями на основе их взаимного взаимодействия (цитаты, ответы и ретвиты) была предложена в [15]. Данная статья может быть полезна для дополнения оценок распространения атаки между двумя пользователями.

Математический анализ моделей распространения информации рассматривался в [16], а именно была описана модель отложенного распространения слухов, основывающаяся на теории графов и дифференциальных уравнений в частных производных.

Задача моделирования распространения информации часто встречается при рассмотрении и разработке моделей максимизации влияния [17−19]. Так в [17] была описана общая концепция распространения информации по некоторой сети, а также представлены две популярные модели распространения информации, в частности, линейная пороговая модель. В исследовании [20] при разработке новой меры централизации для ранжирования пользователей сети в качестве основы используются линейная пороговая и независимая каскадная модели.

IV. Предлагаемые подходы

Перечислим все события, которые могут происходить при атаке злоумышленника на пользователей информационной системы:

- $A_i^{(1)}$: прямая атака злоумышленника на пользователя U_i;
- S_{ij}: распространение атаки между двумя пользователями U_i к U_j;
- $A_j^{(k)}$: опосредованная атака на пользователя U_j, при которой была задействована цепочка из k пользователей.

Для оценки вероятности успеха наступления события $A_i^{(1)}$ (прямой социоинженерной атаки на пользователя) могут быть использованы модели, предлагаемые в [4, 21]. А именно авторы предлагают строить оценки вероятности успеха на основе профиля уязвимостей пользователя, который в свою очередь может быть построен на основе оценки его личностных особенностей. В рамках текущего исследования будем предполагать, что каждому событию $A_i^{(1)}$ уже сопоставлена оценка вероятности наступления данного события $\mathrm{P}(A_i^{(1)}) = p_i^{(1)}$.

Согласно [4, 12] могут быть получены оценки вероятности распространения атаки между всевозможными парами пользователей $\mathrm{P}(S_{ij}) = p_{ij}$.

Наконец, рассмотрим подробнее $A_j^{(k)}$ – опосредованную атаку на пользователя. Вероятность успеха наступления данного события должна зависеть от успеха наступления всех предыдущих, а также учитывать профиль уязвимостей пользователя U_j и его личностные особенности, то есть вероятность наступления $A_j^{(1)}$. В то же время успех такой атаки должен быть выше успеха наступления $A_j^{(1)}$ за счёт того, что сама атака в данном случае будет носить неявный характер, так как к пользователю U_j запрос поступит не от самого злоумышленника, а от какого-то знакомого пользователя из окружения.

Рассмотрим простейший случай социального графа $G = (U, E), \quad U = \{U_1, U_2\}, \quad E = \{(U_1, U_2, p_{12})\}$, что соответствует Рис. 1. Событие $A_2^{(2)}$ могло произойти тогда и только тогда, когда уже произошли события $A_1^{(1)}$ и S_{12}, поэтому для описания модели наступления события $A_2^{(2)}$ воспользуемся формулой условной вероятности:

$$P(A_2^{(2)}) = P(A_2^{(2)} \mid A_1^{(1)} S_{12}) = \frac{P(A_1^{(1)} S_{12} A_2^{(2)})}{P(A_1^{(1)}) P(S_{12} \mid A_1^{(1)})}.$$

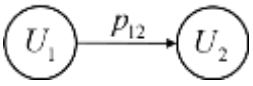

Рис. 1. Распространение атаки между двумя пользователями

Если социальный граф задан следующим образом: $G=(U,E)$, $U=\{U_1,U_2,U_3\}$, $E=\{(U_1,U_3,p_{13}),(U_2,U_3,p_{23})\}$, что соответствует Рис. 2, а $A_1^{(1)}$ и $A_2^{(1)}$ — независимые. Модель наступления события $A_3^{(2)}$ должна учитывать вероятность распространения атаки и от U_1, и от U_2. То есть событие $A_3^{(2)}$ может наступить только после того, как наступило событие $A_1^{(1)}$ или $A_2^{(1)}$, и атака успела распространиться от них к третьему пользователю, то есть произошли события S_{13} или S_{23} соответственно. Учитывая это, модель параллельного распространения атаки на пользователя U_3 может быть задана следующим образом:

$$P(A_3^{(2)})=P(A_3^{(2)}\,|\,A_1^{(1)}S_{13})\cup P(A_3^{(2)}\,|\,A_2^{(1)}S_{23})=$$

$$=\frac{P(A_1^{(1)}S_{12}A_3^{(2)})}{P(A_1^{(1)})P(S_{13}|A_1^{(1)})}+\frac{P(A_2^{(1)}S_{23}A_3^{(2)})}{P(A_2^{(1)})P(S_{22}|A_2^{(1)})}.$$

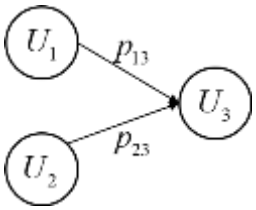

Рис. 2. Параллельное распространение атаки

Если социальный граф задан как: $G=(U,E)$, $U=\{U_1,U_2,U_3\}$, $E=\{(U_1,U_2,p_{12}),(U_2,U_3,p_{23})\}$, что соответствует Рис. 3, и наступили события $A_1^{(1)}$, S_{12}, $A_2^{(2)}$, S_{23}. Тогда модель наступления события $A_3^{(3)}$:

$$P(A_3^{(3)})=P(A_3^{(3)}\,|\,A_1^{(1)}S_{12}A_2^{(2)}S_{23})=$$

$$\frac{P(A_1^{(1)}S_{12}A_2^{(2)}S_{23}A_3^{(3)})}{P(A_1^{(1)})P(S_{12}\,|\,A_1^{(1)})P(A_2^{(2)}\,|\,A_1^{(1)}S_{12})P(S_{23}\,|\,A_1^{(1)}S_{12}A_2^{(2)})}.$$

Рис. 3. Последовательное распространение атаки

Наконец, рассмотрим общий случай задания социального графа $G=(U,E)$, $U=\{U_i\}_{i=1}^{n}$, $E=\{(U_i,U_j,p_{ij})\}_{1\le i,j\le n,i\ne j}$. Пусть известно, что уже произошли события $\{A_{i_1}^{(1)}\}_{1<i_1\le n}$, …, $\{A_{i_k}^{(1)}\}_{1<i_k\le n}$, $\{S_{i_j i_l}\}_{1\le i_j,i_l\le k+1,\,j\ne l}$, тогда вероятность наступления события $A_{k+1}^{(k+1)}$ будет задаваться следующим образом:

$$P(A_{k+1}^{(k+1)})=\bigcup_{i_1,\dots,i_k} P(A_{i_{k+1}}^{(k+1)}\,|\,A_{i_1}^{(1)}S_{i_1i_2}\dots S_{i_{k-1}i_k}A_{i_k}^{(k)}S_{i_ki_{k+1}}),$$

где $A_{i_1}^{(1)}$ – прямая атака злоумышленника на пользователя U_{i_1}; $A_{i_k}^{(k)}, k>1$ – опосредованная атака злоумышленника на пользователя U_{i_k}, при которой была задействована цепочка из k пользователей; $S_{i_ji_l}$ – распространение атаки от U_{i_j} к U_{i_l}.

V. Заключение

Таким образом, в работе были предложены подходы к моделированию сценариев развития многоходовой социоинженерной атаки, учитывающие три типа событий: прямые действия злоумышленника, переход атаки между двумя пользователями и опосредованную атаку на пользователя. Настоящее исследование находит своё применение при дальнейшем проектировании сложных систем управления информационной безопасностью организации, а именно при создании автоматизированного комплекса для выявления наиболее критичных узлов информационной системы в контексте социоинженерных атак. В дальнейшем предполагается доработать модель, добавив учёт изменения успеха реализации атаки при повторных действиях злоумышленника.

Список литературы

[1] Klimburg-Witjes N., Wentland A. Hacking humans? Social Engineering and the construction of the "deficient user" in cybersecurity discourses // Science, Technology & Human Values. 2021. № 0162243921992844. doi: 10.1177/0162243921992844

[2] Wang Z., Zhu H., Sun L. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods // IEEE Access. 2021. Vol. 9. Pp. 11895−11910. doi: 10.1109/ACCESS.2021.3051633

[3] Hijji M., Alam G. A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions // IEEE Access. 2021. Vol. 9. Pp. 7152−7169. doi: 10.1109/ACCESS.2020.3048839

[4] Абрамов М.В., Тулупьева Т.В., Тулупьев А.Л. Социоинженерные атаки: социальные сети и оценки защищенности пользователей. СПб.: ГУАП, 2018. 266 с.

[5] Shahbaznezhad H., Kolini F., Rashidirad M. Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter? // Journal of Computer Information Systems. 2020. Pp. 1−12. doi: 10.1080/08874417.2020.1812134

[6] Aldawood H., Skinner G. Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions // IEEE Access. 2020. Vol. 8. Pp. 67321−67329. doi: 10.1109/ACCESS.2020.2983280

[7] Campbell C.C. Solutions for counteracting human deception in social engineering attacks // Information Technology & People. 2019. Vol. 32, №5. Pp. 1130−1152. doi: 10.1108/ITP-12-2017-0422

[8] Loffler E., Schneider B., Zanwar T., Asprion P.M. CySecEscape 2.0-A Virtual Escape Room To Raise Cybersecurity Awareness // International Journal of Serious Games. 2021. Vol. 8, №1. Pp. 59−70. doi: 10.17083/ijsg.v8i1.413

[9] Krylov B., Abramov M. Automatic hierarchical task network planning system for the Unity game engine // Conference on Artificial Intelligence 2020. CEUR Workshop Proceedings, 2020. Pp. 122─133.

[10] Astakhova L.V., Medvedev I.A. An Information Tool for Increasing the Resistance of Employees of an Organization to Social Engineering Attacks // Scientific and Technical Information Processing. 2021. Vol. 48, №1. Pp. 15−20. doi: 10.3103/S0147688221010020

[11] Как социальная инженерия открывает хакеру двери в вашу организацию [Электронный ресурс] // Positive technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/social-engineering (дата обращения: 26.05.2021).

[12] Khlobystova A.O., Tulupyeva T.V., Maksimov A.G., Korepanova A.A. An approach to quantification of relationship types between users based on the frequency of combinations of non-numeric evaluations // International Conference on Intelligent Information Technologies for Industry. Springer, Cham, 2019. Pp. 206−213. doi: 10.1007/978-3-030-50097-9_21

[13] Korepanova A.A., Oliseenko V.D., Abramov M.V. Applicability of Similarity Coefficients in Social Circle Matching // 2020 XXIII International Conference on Soft Computing and Measurements (SCM). IEEE, 2020. Pp. 41−43. doi: 10.1109/SCM50615.2020.9198782

[14] Zhou F., Xu X., Trajcevski G., Zhang K. A survey of information cascade analysis: Models, predictions, and recent advances. ACM Computing Surveys (CSUR), 2021. Vol. 54. №. 2. Pp. 1−36. doi: 10.1145/3433000

[15] Zola P., Cola G., Mazza M., Tesconi, M. Interaction strength analysis to model retweet cascade graphs. Applied Sciences, 2020. Vol. 10. №. 23. P. 8394. doi: 10.3390/app10238394

[16] Zhu L., Guan G., Zhang Z. Mathematical analysis of information propagation model in complex networks // International Journal of Modern Physics B, 2020. Vol. 34. №. 26. P. 2050240. DOI: 10.1142/S0217979220502409

[17] Jing D., Liu T. Context-based influence maximization with privacy protection in social networks // EURASIP Journal on Wireless Communications and Networking, 2019. Vol. 142, №1. Pp. 1−21. doi: 10.1186/s13638-019-1405-5

[18] Bagheri E., Dastghaibyfard G., Hamzeh A. FAIMCS: A fast and accurate influence maximization algorithm in social networks based on community structures // Computational Intelligence, 2021. P. e12466. doi: 10.1111/coin.12466

[19] Shahrouz S., Salehkaleybar S., Hashemi M. gIM: GPU Accelerated RIS-Based Influence Maximization Algorithm // IEEE Transactions on Parallel and Distributed Systems, 2021. Vol. 32. №. 10. Pp. 2386−2399. doi: 10.1109/TPDS.2021.3066215

[20] Riquelme F., Gonzalez-Cantergiani P., Molinero X., Serna M. Centrality measure in social networks based on linear threshold model. Knowledge-Based Systems, 2018. Vol. 140, Pp. 92−102. doi: 10.1016/j.knosys.2017.10.029

[21] 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.