Инженерный вестник Дона, №2 (2023)
ivdon.ru/ru/magazine/archive/n2y2023/8186

Имитационное моделирование реализации компьютерной атаки с повышением привилегий пользователя системы электронного документооборота

Н.В. Шишов[1], В.А. Ломазов[2,3], В.И. Ломазова [2,3]

[1]Белгородский университет кооперации, экономики и права,
[2]Белгородский государственный аграрный университет им. В.Я. Горина,
[3]Белгородский государственный национальный исследовательский университет,

Аннотация: Работа посвящена проблематике защиты системы документооборота органов государственного управления. Целью работы является построение имитационной модели реализации целевой компьютерной атаки с учетом одновременного (протекающего с незначительным запаздыванием) реагирования средств защиты системы документооборота. Для моделирования предложено использовать аппарат сетей Петри-Маркова, сочетающий в себе представление смены состояний атакуемой системы в виде марковских (полумарковских) процессов и выразительные возможности сетей Петри для описания взаимодействия процессов. Построенная модель отражает как специфику атак с повышением привилегий пользователя, так и особенности процессов обработки документов, а также используемые механизмы противодействия в получении неправомерного доступа. Вычислительные эксперименты, проводимые с использованием построенной имитационной модели, позволяют оценить возможные риски и принять решение по выбору наиболее эффективной системы защиты от рассмотренного типа атак.
Ключевые слова: система электронного документооборота, компьютерная атака, имитационное моделирование, сеть Петри-Маркова.

Введение. Развитие современных цифровых технологий, наряду с несомненными положительными аспектами, обусловленными многократным сокращением трудозатрат и времени реализации информационных процессов, имеет также негативные стороны, связанные с уязвимостью систем корпоративного и государственного управления по отношению к различного рода угрозам информационной безопасности [1].

Повсеместное внедрение и широкомасштабное использование автоматизированных систем, эксплуатируемых на объектах/органах государственного управления, привело к формированию нового профиля компьютерной преступности, при котором злоумышленник, используя аппаратные и программные средства, получает несанкционированный доступ к данным и совершает над ними операции с целью нарушения

функционирования процессов безопасности и формирования подходов для получения неправомерного доступа к данным системам [2, 3].

Изучение стандартов и нормативно-правовых актов в области защиты информации в системах электронного документооборота (СЭД) [4-6], а также научных работ, посвященных этой тематике (например, [7-9]), позволило сделать вывод о недостаточном использовании методов имитационного моделирования для решения задач оценки рисков и выработки проектных решений по созданию систем эффективной защиты СЭД. При этом не исследован вопрос о возможности одновременного осуществления угрозы и реагирования применяемых средств защиты информации.

Это определило цель настоящей работы, состоящую в построении имитационной модели реализации целевой компьютерной атаки на СЭД, предполагающей несанкционированное повышение привилегий пользователя (как один из типовых видов атак) с учетом одновременного (протекающего с незначительным запаздыванием) реагирования средств защиты.

Материалы и методы. Моделирование реализации целевой компьютерной атаки на автоматизированные системы государственного управления является трудозатратной и сложной задачей, в рамках которой рассматривается ряд взаимосвязанных параллельных процессов [10]. Для имитационного моделирования предлагается использовать аппарат сетей Петри-Маркова, сочетающий в себе представление смены состояний атакуемой СЭД в виде марковских (полумарковских) процессов и выразительные возможности сетей Петри для описания взаимодействия процессов.

Сеть Петри-Маркова может быть формально представлена в виде [11]:

$$\theta = <П, M>,$$

где $П$ – сеть Петри, определяющая структуру сети Петри-Маркова, а M – случайный процесс, накладываемый на структуру $П$.

Граф сети Петри-Маркова представлен на рис. 1.

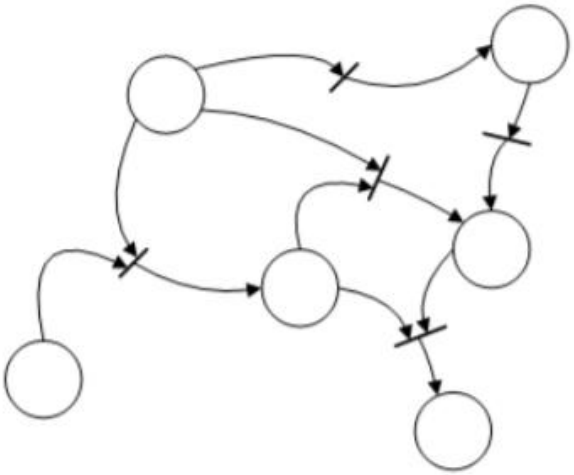

Рис. 1. – Граф сети Петри-Маркова

Сеть Петри-Маркова можно представить в виде ориентированого двудольного графа, где имеется два типа вершин: позиции и переходы.

Позиция (кружок) устанавливает некоторые условия для последовательности изменения состояния одного или нескольких объектов. В свою очередь, переход (вертикальная черта) имитирует процесс изменения состояния одного или нескольких объектов.

Способность приведения в действие определенного математического объекта описывается ориентированной дугой, ведущей из заданных позиций в соответствующие переходы (из переходов в позиции). Возможность осуществления перехода определяется наличием входящих дуг, а также наличием дуг, соответствующих заданным ограничениям «И», «ИЛИ», «НЕ».

При описании имитационного моделирования процесса реализации угрозы информационной безопасности в СЭД в ходе воздействия на систему защиты информации вводятся следующие обозначения математических объектов: S_i – описание возможных позиций исследуемого процесса, t_i – описание возможных переходов, где индекс i соответствует номеру позиции (перехода).

Результаты. Атака с повышением привилегий определяется как сетевая атака с целью получения неправомерного доступа к правам (элементам информационного ресурса) сверх тех, которые предусмотрены настройками учетной записи пользователя [12]. При реализации данного вида атаки может быть задействован субъект внешней угрозы или инсайдер. Несанкционированное повышение привилегий является ключевым этапом цепочки сетевых атак и обычно включает в себя использование уязвимости, такой как системная ошибка или неправильная конфигурация контроля доступа.

Вид сети Петри-Маркова, описывающей процесс реализации целевой компьютерной атаки путем несанкционированного повышения привилегий для учетных записей СЭД, представлен на рис. 2.

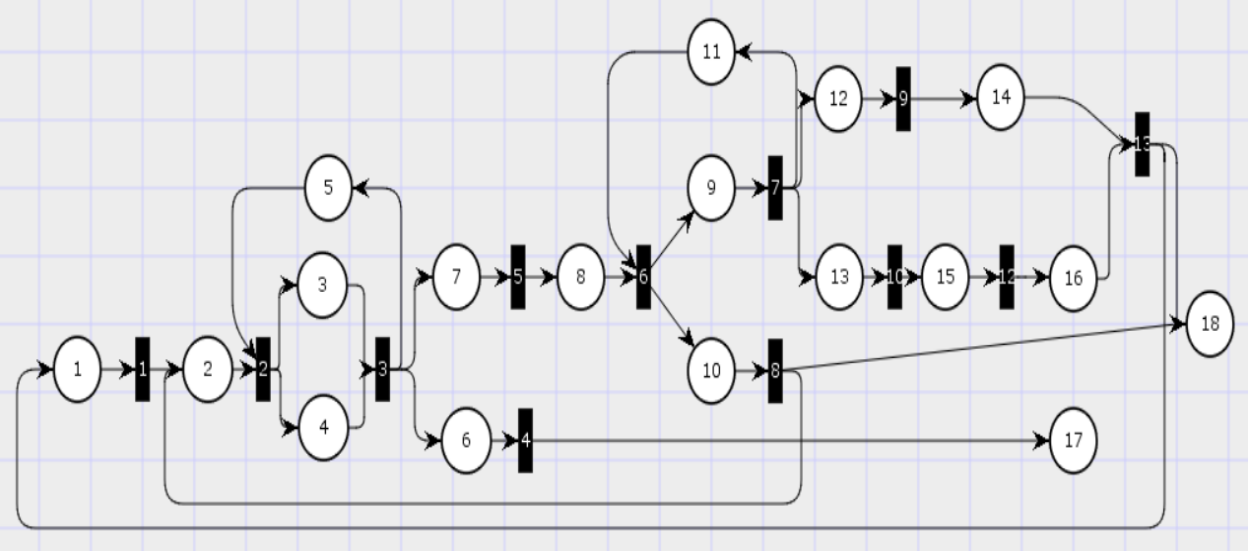

Рис. 2. – Вид сети Петри-Маркова, моделирующей процесс повышения привилегий для учетных записей СЭД

Описание математических объектов сети Петри-Маркова, моделирующей процесс реализации целевой компьютерной атаки путем повышения привилегий для учетных записей СЭД приведено в таблице № 1.

Таблица № 1

Описание математических объектов сети Петри-Маркова, моделирующей процесс реализации целевой компьютерной атаки путем повышения привилегий для учетных записей СЭД

№	Описание позиции	№	Описание перехода
S_1	Злоумышленник готов к проведению атаки. Запуск штатной программы для изменения привилегий	t_1	Штатная программа запущена
S_2	Запуск клиентского приложения СЭД	t_2	Клиентское приложение СЭД запущено
S_3	Попытка аутентификации	t_3	Аутентификационные данные введены верно, штатная программа изменения привилегий запущена и система защиты информации не обнаружила нарушений
S_4	Направление запроса на изменение привилегий	t_4	Учетная запись заблокирована
S_5	Попытка повторной аутентификации	t_5	Получен доступ в СЭД
S_6	Блокировка учетной записи	t_6	Сопоставление полномочий доступа пользователя и запрашиваемого документа
S_7	Вход в СЭД	t_7	Допуск к документу получен
S_8	Обращение к документу	t_8	Доступ к документу заблокирован
S_9	Допуск к документу	t_9	Запрос на изменение сформирован
S_{10}	Блокировка доступа к документу	t_{10}	Запрос на удаление сформирован
S_{11}	Повторная попытка получить доступ к документу	t_{11}	Работа с документом завершена
S_{12}	Запрос на изменение документа	t_{12}	Документ удален
S_{13}	Запрос на удаление документа	t_{13}	Работа с документом завершена
S_{14}	Документ изменен		
S_{15}	Документ удален		
S_{16}	Удаление документа		
S_{17}	Регистрация события СЗИ		
S_{18}	Завершение работы		

Злоумышленники обычно идут по пути наименьшего сопротивления. В случае если у злоумышленников имеется достаточно времени для реализации данного вида атаки они приложат усилия для того, чтобы остаться незамеченными. Независимо от того, включает ли это маскировку их исходного IP-адреса или удаление журналов на основе используемых ими учетных данных, любые доказательства их присутствия отражают показатель компрометации [13]. Как только организация идентифицирует вторжение, она может отслеживать намерения злоумышленника и/или потенциально приостановить или завершить сеанс доступа.

Заключение. Разработанная с использованием аппарата сетей Петри-Маркова имитационная модель реализации целевой компьютерной атаки, состоящей в несанкционированном повышении привилегий пользователя, и реакции системы защиты СЭД на эту атаку, позволяет провести вычислительные эксперименты, дающие возможность оценить риски при различных технологиях ведения электронного документооборота и различных проектных решениях системы его защиты, а, следовательно, выбрать наилучшее решение.

Литература

1. Targowski A. Information Technology and Societal Development. 1st Edition. 2008. 462 p.

2. Прокушев Я.Е., Пономаренко С.В., Пономаренко С.А. Моделирование процессов проектирования систем защиты информации в государственных информационных системах // Computational nanotechnology. 2021. № 1. URL: elibrary.ru/item.asp?id=45590599.

3. Киселев А.Ю. Социальная инженерия: человеческий фактор как проблема информационной безопасности // Дыльновские чтения. 2017. С. 169-173.

4. Филиппова Н.В. Правовое регулирование защиты информации в государственных информационных системах // Охрана, безопасность, связь. 2021. № 6-2. С. 73-78.

5. Миронова А.О., Гончаренко Ю.Ю., Гоголь А.С., Фролова А.Н. Применение методики оценки угроз безопасности информации // Энергетические установки и технологии. 2021. № 4. С. 71-75.

6. Якубов Р.Ж. Обзор методического документа «Меры защиты информации в государственных информационных системах», утвержденного ФСТЭК России 11 февраля 2014 г. // Молодежный научно-технический вестник. 2014. № 10. URL: elibrary.ru/item.asp?id=22621764.

7. Перепелкина О.А. Математическое моделирование системы электронного документооборота и делопроизводства в исполнительных органах государственной власти на примере Пензенской области // Науковедение. 2017. №6. URL: elibrary.ru/item.asp?id=32598229.

8. Гостищева Т.В., Ломазов В.А., Малий Ю.В. Модели и методы проектирования систем защиты информации. Белгород: Издательство Белгородского университета кооперации, экономики и права, 2021. 175 с.

9. Прокушев Я.Е., Пономаренко С.В. Сравнительный анализ средств программно-аппаратной защиты информации, применяемых в информационных системах персональных данных // Информация и безопасность. 2012. № 1. С. 31–36.

10. Андреев Д.А., Панфилов А.Н., Скоба А.Н. Управление операционными процессами операторов сложных систем // Инженерный вестник Дона. 2017. №3. URL: ivdon.ru/ru/magazine/archive/n3y2017/4322.

11. Ivutin A.N., Larkin E.V., Lutskov Y.I., Novikov A.S. Simulation of concurrent process with Petri-Markov nets // Life Science Journal. 2014. №11, URL: lifesciencesite.com/lsj/life1111/086_25899life111114_506_511.pdf.

12. Менциев А.У., Чебиева Х.С. Современные угрозы безопасности в сети Интернет и контрмеры (обзор) // Инженерный вестник Дона. 2019. №4. URL: ivdon.ru/ru/magazine/archive/n4y2019/5859.

13. Alkhalil Z., Hewage C., Nawaf L., Khan I. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy // Frontiers of Computer Science. 2021. URL: frontiersin.org/articles/10.3389/fcomp.2021.563060/full.

References

1. Targowski A. Information Technology and Societal Development. 1st Edition. 2008. 462 p.

2. Prokushev Ya.E., Ponomarenko S.V., Ponomarenko S.A. Computational nanotechnology. 2021. № 1. URL: elibrary.ru/item.asp?id=45590599.

3. Kiselev A.Yu. Dylnovskie chteniya. 2017. pp. 169-173

4. Filippova N.V., Ohrana, bezopasnost, svyaz. 2021. № 6-2. pp. 73-78.

5. Mironova A.O., Goncharenko Yu.Yu., Gogol A.S., Frolova A.N. Energeticheskie ustanovki i tekhnologii. 2021. № 4. pp. 71-75

6. Yakubov R.Zh. Molodezhnyj nauchno-tekhnicheskij vestnik. 2014. № 10. URL: elibrary.ru/item.asp?id=22621764.

7. Perepelkina O.A. Naukovedenie. 2017, №6. URL: elibrary.ru/item.asp?id=32598229.

8. Gostishcheva T.V., Lomazov V.A., Malij YU.V. Modeli i metody proektirovaniya sistem zashchity informacii. Belgorod: Izdatel'stvo Belgorodskogo universiteta kooperacii, ekonomiki i prava, 2021. 175 p.

9. Prokushev Ya.E., Ponomarenko S.V. Informaciya i bezopasnost. 2012. № 1. pp. 31–36.

10. Andreev D.A., Panfilov A.N., Skoba A.N. Inzhenernyj vestnik Dona. 2017, №3. URL: ivdon.ru/ru/magazine/archive/n3y2017/4322.

11. Ivutin A.N., Larkin E.V., Lutskov Y.I., Novikov A.S. Life Science Journal. 2014. №11. URL: lifesciencesite.com/lsj/life1111/086_25899life111114_506_511.pdf.

12. Menciev A.U., CHebieva H.S. Inzhenernyj vestnik Dona. 2019, №4. URL: ivdon.ru/ru/magazine/archive/n4y2019/5859.

13. Alkhalil Z., Hewage C., Nawaf L., Khan I. Frontiers of Computer Science. 2021. URL: https: frontiersin.org/articles/10.3389/fcomp.2021.563060/full.