Поддержка принятия решений по реагированию на нарушения в системах управления с использованием графовых моделей

Е. В. Дойникова
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук;
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
{doynikova, fedorchenko}@comsec.spb.ru

А. В. Федорченко
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
{doynikova, fedorchenko}@comsec.spb.ru

Е. С. Новикова
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
evgenia.novikova123@gmail.com

И. А. Ушаков, А. В. Красов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
ushakovia@gmail.com, krasov@inbox.ru

Аннотация. **Эффективное реагирование на нарушения информационной безопасности в системах управления остается актуальной проблемой в настоящее время, когда их количество, сложность, а также уровень возможных потерь растет. Нарушение может быть вызвано рядом шагов, последовательно осуществляемых нарушителем. В области выбора контрмер для проактивного и реактивного реагирования на нарушения существует большое количество методик. Перспективными представляются методики, основанные на графовых моделях, которые позволяют смоделировать последовательность шагов, вызвавших нарушение. К их преимуществам относится возможность прогнозирования нарушений для своевременного принятия решений по выбору контрмер, а также возможность анализа и учета покрытия контрмер в терминах возможных шагов, приводящих к нарушению. В работе предлагается и описывается методика поддержки принятия решений по реагированию на нарушения информационной безопасности в системах управления на основе графовых моделей, а также разработанные модели предметной области, включая модель контрмер и граф, отображающий шаги, приводящие к нарушениям информационной безопасности.**

Ключевые слова: управление; технические системы; реагирование на нарушения; информационная безопасность; контрмеры; граф; прогнозирование; модель контрмер; принятие решений

I. Введение

В условиях роста количества, сложности и уровня возможных потерь от нарушений информационной безопасности (ИБ), актуальной проблемой управления в технических системах является эффективное реагирование на нарушения за счет своевременного и адекватного выбора и реализации контрмер. В области выбора контрмер существует большое количество методик. Средства защиты информации могут выбираться как на этапе проектирования технической системы, так и на этапе ее эксплуатации. Для управления ИБ на этапе эксплуатации технической системы выделяются реактивный и проактивный подходы к выбору контрмер. Реактивный подход подразумевает реагирование на уже произошедшее нарушение, в то время как проактивный подход подразумевает прогнозирование нарушения и принятие мер до того, как оно нанесет серьезный ущерб. Предотвращение потерь является преимуществом проактивного подхода, однако важно не нанести анализируемой системе серьезный побочный ущерб при реализации контрмер.

Перспективными как для реализации проактивного, так и реактивного подходов показали себя методики, основанные на графовых моделях. К их преимуществам относится возможность прогнозирования нарушений для своевременного принятия решений по выбору контрмер, а также возможность анализа и учета покрытия контрмер в терминах возможных шагов, приводящих к нарушению.

В работе предлагается и описывается методика поддержки принятия решений по реагированию на нарушения ИБ в технических системах на основе графовой модели, а также разработанные модели предметной области, включая модель контрмер и граф, отображающий шаги, приводящие к нарушениям ИБ. Анализируются преимущества и недостатки предложенной методики и рассматриваются направления будущих исследований.

Работа организована следующим образом. Во втором разделе рассматриваются релевантные исследования в области поддержки принятия решений по реагированию на нарушения ИБ. В третьем разделе описывается предложенная методика на основе графовых моделей. В заключении анализируются полученные результаты и предлагаются направления будущих исследований.

II. Релевантные исследования

К настоящему времени исследователями были предложены различные методики выбора контрмер [1–12].

В ряде работ рассматриваются методики на основе теории игр [1, 2]. При этом противодействие нарушениям рассматривается как «игра» нарушителя и администратора по информационной безопасности. Игра представляет собой последовательность состояний и действий. Состояние определяется зависимостями между сервисами и файлами системы и их свойствами, например, уязвимостью или скомпрометированностью [2]. Для изменения состояния необходимо выполнить действие. Действие, в свою очередь, кроме самого действия, определяется предусловием, стоимостью, временем выполнения, выигрышем и исполнителем (игроком). Понятия стоимости и выигрыша вводятся для учета финансового аспекта при анализе информационной безопасности, в том числе для определения стоимости проведения атаки, ущерба от ее проведения и средств, необходимые для ее предотвращения.

Результатом работы методик на основе теории игр является оптимальная стратегия, то есть наилучшая последовательность действий, которую администратор или нарушитель может применить для достижения своих целей. Например, целью администратора может быть поиск наиболее эффективной по стоимости и времени стратегии установления патчей. Для выбора стратегии, минимальной по стоимости и времени, авторы в [2] предлагают минимизировать сумму затрат и времени, необходимых для выполнения всех действий в стратегии. Таким образом, преимуществом методов на основе теории игр являются возможность учета временного и стоимостного аспектов.

Другим широко используемым в рамках методик принятия решений методом является логический вывод на графовых моделях [3, 4]. Идея таких методик состоит в формировании графа возможных действий, вызвавших нарушение и последующего определения того, каким образом можно предотвратить наибольшее количество самых критичных путей. Так, в [3] для формирования рекомендаций по реализации защитных мер авторы предлагают методику, в основе которой лежит граф с множеством предусловий, позволяющий выявить наиболее критичные уязвимости системы. Под наиболее критичными авторы понимают уязвимости, дающие нарушителю наибольший доступ в системе. Узлы графа представляют собой атакующие действия, связанные между собой в случае совпадения пред и постусловий их выполнения. Предусловиями атакующего действия является достижимость соответствующего хоста и наличие на нем уязвимостей или ошибок конфигурации. Достижимость хоста для нарушителя определяется наличием связи с ним и администраторского или гостевого доступа. Постусловиями является получение одного из четырех видов доступа на хосте – администраторского, гостевого, отказа в обслуживании или другого (потеря конфиденциальности и/или целостности). Авторы формируют рекомендации по реализации защитных мер на основе показателей, определяющих, как много путей, ведущих к нарушениям ИБ, будет заблокировано в случае реализации защитной меры.

Методика реализована в рамках программного средства NetSPA (NETwork Security and Planning Architecture). К ее основным преимуществам можно отнести применимость для оперативного построения графов для сетей большого масштаба.

Подробно процесс выбора контрмер с использованием инструмента NetSPA описывается в [4]. Для оценивания защищенности сети и выбора контрмер авторы используют показатель *процент компрометации сети* (Network Compromise Percentage, NCP). NCP определяет процент хостов сети, на которых нарушитель может получить права пользователя или администратора. Для выбора защитных мер предлагается алгоритм, включающий следующие шаги:

- обход графа в ширину и создание списка входящих дуг для каждого хоста (соответствующих уязвимостям, которые могут быть использованы для компрометации хоста);
- подбор защитных мер для этих дуг, т.е. таких мер, которые устраняют дуги графа;
- формирование групп хостов, для которых могут использоваться одни и те же защитные меры, с учетом пересечений между потомками узлов графа;
- расчёт NCP для каждой защитной меры после ее реализации;
- вычисление разницы между предыдущим и новым значением NCP.
- сортировка защитных мер в соответствии с максимальной разницей.

Для выбора защитных мер в режиме эксплуатации анализируемой системы рядом исследователей предлагаются методики на основе байесовских графов [5–7].

В ряде работ описываются методики определения общего уровня защищенности системы [8]. Данный показатель может использоваться для сравнения уровня защищенности до и после внедрения защитных мер и последующего выбора защитных мер.

В [9, 10] рассматривается показатель выбора контрмер, основанный на определении ожидаемых потерь и эффективности контрмер. В [9] вводится показатель выбора контрмер для реагирования на нарушения ИБ *показатель возврата инвестиций в реагирование* (Return-On-Response-Investment, RORI). При расчете RORI учитываются эффективность реагирования, ожидаемые негативные последствия нарушения ИБ в случае отсутствия контрмер, ожидаемые негативные последствия нарушения в случае реализации контрмер, побочные потери при реагировании, затраты на контрмеры. Для определения эффективности реагирования, ожидаемых негативных последствий и побочных потерь используется граф зависимостей сервисов, который позволяет учесть распространение ущерба в анализируемой системе.

В [10] рассматриваются недостатки показателя RORI, который не позволяет учесть вариант отсутствия контрмер и размер инфраструктуры системы. Авторы предлагают улучшенный показатель RORI, который вычисляется на основе ожидаемых годовых потерь (соответствует последствиям негативного события в случае отсутствия контрмер), которые зависят от критичности и правдоподобности нарушения; уровня снижения риска в случае реализации контрмеры; ожидаемых годовых затрат на новую контрмеру; годовых затрат на инфраструктуру (оборудование, поддержка), в случае реализации защитной меры.

В [11, 12] используются экономические индексы для оценивания возможных потерь и эффективности контрмер. Отличие этих походов от вышеупомянутых состоит в том, что в данном случае годовые потери вычисляются на основе исторических данных о частоте инцидента, предотвращаемого контрмерой, в год. Преимущество таких методов состоит в установлении прямой зависимости между финансовыми затратами организации и потерями от нарушений ИБ.

Не смотря на большое количество работ, проблема реагирования на нарушения ИБ остается открытой. Методики, основанные на графах, являются перспективным решением для проактивного и реактивного реагирования. Одной из основных сложностей при выборе контрмер с использованием графов является ресурсоемкость алгоритмов. В работе предлагается методика выбора контрмер с использованием графов и рассматриваются возможные варианты преодоления данной проблемы.

III. Поддержка принятия решений по реагированию на нарушения информационной безопасности

Разработанная методика поддержки принятия решений по реагированию на нарушения ИБ предназначена для выбора средств защиты на этапе проектирования технической системы, а также для проактивного выбора контрмер в режиме эксплуатации. В основе разработанной методики лежит граф, который отображает пути, которые могут привести к нарушениям ИБ в системе с учетом ее слабых мест, и определяется следующим образом:

$$CYG=(AA, L, Pc),$$

где AA – множество узлов графа, соответствующих возможным атакующим действиям, использующим слабые места системы; L – множество связей между узлами графа ($L \subseteq AA \times AA$); Pc – дискретные локальные распределения условных вероятностей [13, 14].

Наличие связи между узлами графа и вероятность перехода от одного узла графа к другому зависит от пост и предусловий выполнения соответствующих атакующих действий.

Контрмера описывается следующим кортежем:

$$CM=(W, P, M, Cov, AGI, SDI),$$

где W – слабое место или уязвимость, против которой направлена контрмера; P – платформа или конфигурация, в которой применима контрмера; M – режим работы системы (проектирование или эксплуатация); Cov – область действия контрмеры (элемент графа, хост, подсеть, сеть); AGI – влияние на граф (удаление, добавление, изменение); SDI – влияние на граф зависимостей сервисов (удаление, добавление, изменение); граф зависимостей сервисов определяет зависимости между бизнес сервисами и техническими ресурсами системы и предназначен для определения побочного ущерба в случае реализации контрмеры.

Модель контрмеры вводится для того, чтобы определить, как реализация контрмеры влияет на граф, который отображает пути, которые могут привести к нарушениям ИБ в системе, и граф зависимостей сервисов, и рассчитать показатели эффективности контрмеры и побочного ущерба от ее реализации, которые являются составляющими показателя выбора контрмер, используемого при выборе контрмер.

Методика выбора контрмер в режиме проектирования включает следующие этапы [15]:

1. добавление в набор точек для применения контрмер *CMN* всех входных узлов графа, т.е. узлов, изначально доступных нарушителю;
2. определение узлов графа, не входящих в *CMN*, и представляющих наибольший риск [4], добавление их в *CMN*;
3. определение списка контрмер *CMs*, доступных для *CMN*;
4. сортировка контрмер в *CMs* по покрытию *Cov*, т.е. количеству узлов графа из *CMN*, на которые они повлияют; в случае контрмер, влияющих на равное количество узлов, создается несколько списков контрмер CMs_i;
5. выбор контрмер для каждого узла из *CMN* на основе полученных списков *CMs*: сначала выбираются контрмеры, действующие на наибольшее количество узлов графа, оставшиеся контрмеры выбираются с учетом максимального несовпадения покрытий, и так пока не будут охвачены все узлы;
6. вычисление показателя выбора контрмер для полученных на шаге 5 списков *CMs*: на этом шаге перестраиваются граф шагов, которые могут привести к нарушениям ИБ в системе, и граф зависимостей сервисов с учетом того, что контрмеры из рассматриваемого списка внедрены, пересчитываются риски для каждого узла, если остаются высокие риски, то список контрмер отбрасывается;
7. если на шаге 6 все списки контрмер были отброшены, возврат алгоритма на шаг 5 (при этом новые списки формируются начиная со второй контрмеры в списках *CMs*), в противном случае выбирается список *CMs* с максимальным суммарным значением показателя выбора контрмер.

Отметим, что для переопределения уровня риска необходимо перестроить граф.

Показатель выбора контрмер определяется следующим образом:

$$CSI = ExpectedLossesTot_a – ExpectedLossesTot_b = Risk_a \cdot 1000 – (Risk_b \cdot 1000 + CD \cdot AssetCriticality + CC),$$

где $ExpectedLossesTot_a$ – ожидаемые потери в случае успешной реализации нарушения до реализации контрмеры; $ExpectedLossesTot_b$ – ожидаемые потери в случае успешной реализации нарушения после реализации контрмеры; $Risk_a$ – риск до реализации контрмеры; $Risk_b$ – риск после реализации контрмеры; *AssetCriticality* – критичность затрагиваемого актива в денежных единицах; *CC* – стоимость контрмеры; *CD* – уровень побочного ущерба в результате реализации контрмеры, который определяется на основе графа зависимостей сервисов.

Методика выбора контрмер в режиме эксплуатации отличается тем, что основной целью является предотвращение нарушения, а не повышение общего уровня защищенности анализируемой системы. Контрмеры реализуются в зависимости от текущих и спрогнозированных шагов нарушителя. При этом учитывается расстояние до критичного ресурса, которое определяется как количество узлов графа до ресурса с высоким уровнем критичности. Если оно превышает заданное значение, то система ждет нового события для уточнения своих оценок, если нет – система предлагает контрмеру на основе имеющихся данных со степенью точности, соответствующей количеству уже выявленных релевантных событий. Методика включает следующие основные этапы [13]: (1) добавление в набор точек для применения контрмер *CMN* узлов графа с высоким уровнем риска; (2) определение расстояния до критичного ресурса; (3) если расстояния до критичного ресурса меньше заданного значения – переход к этапу (4), иначе – ожидание новых событий; (4) определение списка контрмер *CMs*, доступных для *CMN*; (5) сортировка контрмер в *CMs* по покрытию *Cov*, т. е. количеству узлов графа из *CMN*, на которые они повлияют; в случае контрмер, влияющих на равное количество узлов, создается несколько списков контрмер CMs_i; (6) определение контрмер для каждого узла графа на основе полученных списков: сначала выбираются контрмеры, действующие на наибольшее количество узлов графа, оставшиеся контрмеры выбираются с учетом максимального несовпадения покрытий, и так пока не будут охвачены все узлы; (7) вычисление показателя выбора контрмер для полученных на шаге 6 списков *CMs*, при этом пересчитываются риски для каждого узла, если остаются высокие риски, то список контрмер отбрасывается; (8) если на шаге 7 все списки контрмер были отброшены, возврат алгоритма на шаг 5 (при этом новые списки формируются, начиная со второй контрмеры в списках *CMs*), в противном случае выбирается список *CMs* с максимальным суммарным значением показателя выбора контрмер.

IV. Заключение

В работе рассмотрена предлагаемая методика поддержки принятия решений для реагирования на нарушения ИБ в технических системах путем выбора контрмер на этапах проектирования и эксплуатации с использованием графа. В основе методик выбора контрмер лежит алгоритм полного перебора с ограничениями, что определяет существенную ресурсоемкость предложенных методик. Тем не менее, при реализации методик процессы перестроения графа и определения эффективности предлагаемой контрмеры могут быть распараллелены, что позволит существенно снизить временные затраты и удовлетворить требования к оперативности в режиме эксплуатации системы для своевременного реагирования на нарушения. В дальнейшей работе планируется провести серию экспериментов, подтверждающих данное утверждение, а также провести исследования в области оптимизации предложенной методики и алгоритмов.

Список литературы

[1] He W., Xia C., Zhang C., Ji Y., Ma X. A network security risk assessment framework based on game theory // Proceedings of the Second International Conference on Future Generation Communication and Networking, FGCN '08 (Hainan Island, 13-15 Dec. 2008). Volume 2. IEEE, 2009. P. 249–253.

[2] Bursztein E., Mitchell J.C. Using strategy objectives for network security analysis // Information Security and Cryptology ; series: Lecture Notes in Computer Science. Volume 6151. Springer Berlin Heidelberg, 2010. P. 337–349.

[3] Ingols K., Lippmann R.P., Piwowarski K. Practical attack graph generation for network defense // Proceedings of 22nd Annual Conference on the Computer Security Applications (Miami Beach, FL, 2006). IEEE, 2006. P. 121–130.

[4] Lippmann R.P. Validating and restoring defense in depth using attack graphs // Proceedings of MILCOM 2006 (Washington, DC).

[5] Khosravi-Farmad M., Bafghi A. Bayesian Decision Network-Based Security Risk Management Framework. Journal of Network and Systems Management. 28. 10.1007/s10922-020-09558-5. 2020.

[6] Li F., Li Y., Leng S., Guo Y., Geng K., Wang Z., Fang L. Dynamic Countermeasures Selection for Multi-Path Attacks. Computers & Security. 97. 101927. 10.1016/j.cose.2020.101927. 2020.

[7] Poolsappasit N., Dewri R., Ray I. Dynamic security risk management using Bayesian attack graphs // IEEE Transactions on Dependable and Security Computing. 2012. Vol.9, No.1. P. 61–74.

[8] Kotenko I., Stepashkin M. Attack graph based evaluation of network security // Proceedings of the 10th IFIP Conference on Communications and Multimedia Security (Heraklion, Greece, 2006). 2006. P. 216–227.

[9] Kheir N., Cuppens-Boulahia N., Cuppens F., Debar H. A service dependency model for cost-sensitive intrusion response // Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS'10). Vol. 6345. 2010. P. 626–642.

[10] Granadillo G.G., Debar H., Jacob G., Achemlal M. Individual countermeasure selection based on the return on response investment index // LNCS, Computer Network Security, proceedings of the 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2012 (St. Petersburg, Russia, October 17-19, 2012). Vol.7531. Springer, 2012. P. 156–170. DOI: 10.1007/978-3-642-33704-8_14.

[11] Hoo K.J.S. How Much is Enough? A Risk-Management Approach to Computer Security: PhD thesis / Stanford University, 2000.

[12] Cremonini M., Martini P. Evaluating information security investments from attackers perspective: the Return-On-Attack (ROA) // Proceedings of the Fourth Workshop on the Economics of Information Security (2-3 June 2005), 2005.

[13] Kotenko I., Doynikova E. Selection of countermeasures against network attacks based on dynamical calculation of security metrics // Journal of Defense Modeling and Simulation. Vol.15, Issue 2. 2018. P. 181–204. DOI: 10.1177/1548512917690278.

[14] Дойникова Е.В., Котенко И.В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер // Труды СПИИРАН, 2018. Вып. 2(57). С. 211–240. DOI: 10.15622/sp.57.9.

[15] Doynikova E., Kotenko I. The multi-layer graph based technique for proactive automatic response against cyber attacks // Proceedings of the 26th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2018). Cambridge, UK, March 21-23, 2018. Los Alamitos, California. IEEE Computer Society. 2018. P.470-477. DOI: 10.1109/PDP2018.2018.00081.