DOI: https://doi.org/10.15688/jvolsu10.2017.3.2

УДК 681.3
ББК 32.973

ТЕНДЕНЦИИ РАЗВИТИЯ ТЕХНОЛОГИЙ СИНТЕЗА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ПОМОЩЬЮ SMT-РЕШАТЕЛЕЙ

Глеб Александрович Попов

Старший преподаватель, кафедра информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Татьяна Александровна Тихомирова

Студент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье рассматривается оригинальный подход к решению задачи синтеза системы защиты информации в автоматизированной системе. Предлагается метод кодирования исходной задачи в виде формализованной проблемы для SMT-решателя. Особенностью метода является выражение характеристик средств защиты в виде функций. Приводится формула на языке теории UFLRA, соответствующая исходной задаче. Описывается процесс интерпретации полученных результатов SMT-решателя. Отмечаются недостатки предложенного подхода.

Ключевые слова: синтез системы защиты, задача на ограничения, информационная безопасность, автоматизированная система, система с полным перекрытием, принятие решений.

Проблема синтеза системы защиты информации для автоматизированной системы в общем случае сводится к оптимальному выбору таких мер защиты, которые бы обеспечивали функционирование системы при минимальных приемлемых рисках в условиях существования определенных угроз. В зависимости от требований к автоматизированной системе (АС) и специфики ее работы задача синтеза может углубляться. Например, понятие оптимальности системы защиты информации (СЗИ) может как означать максимальную эффективность СЗИ при минимальных затратах на ее внедрение и поддержание, так и дополнительно учитывать степень ее влияния на работу АС. Последний вариант трактовки особенно актуален для средств антивирусной защиты, устанавливаемых на автоматизированное рабочее место пользователей АС. Другой причиной усложнения рассматриваемой проблемы является возможность варьирования самих компонентов защищаемой АС. Наконец, главная сложность заключается в формализации списка угроз и зна-

чений рисков, которые могут представлять собой зависимые от различных факторов и друг от друга величины.

Наиболее известным подходом к решению задачи синтеза СЗИ является использование модели с полным перекрытием. Однако, ввиду описанных выше сложностей, неизбежно возникающих при работе с реальными АС, непосредственное применение данной модели затруднено, как на этапе формализации, так и на этапе поиска решения. Для преодоления этих трудностей предлагается подход, заключающийся в следующем:

1. Исходная задача кодируется в терминах теории UFLRA (линейная арифметика с неинтерпретируемыми типами и функциями).

2. Полученная задача решается с помощью одного из существующих программных SMT-решателей.

3. Производится интерпретация результата.

В языке UFLRA разрешается составлять выражения, состоящие из действительных чисел и арифметических действий над ними, использовать кванторы $\exists$ и $\forall$, объединять переменные в упорядоченные множества произвольной длины (пары, тройки, и т. д.), а также вводить собственные неинтерпретируемые типы данных.

Первый этап кодирования задачи синтеза СЗИ на языке SMT-решателя заключается в определении домена дискурса D. В большинстве случаев D представляет собой упорядоченное множество, имеющее в качестве своих элементов значения, каждое из которых описывает определенное свойство или характеристику защищаемой АС. Благодаря возможности использования неинтерпретируемых типов характеристики АС не обязательно должны иметь численные значения. Таким образом, отдельно взятое значение $d \in D$ описывает текущее состояние защищаемой АС.

Угрозы АС также могут быть описаны значением из домена дискурса, так как для каждой угрозы можно определить, подвержена ли ей защищаемая АС в текущем состоянии d или нет. Для выражения зависимостей между отдельными угрозами на элементы d можно накладывать дополнительные ограничения, учитывающие значения нескольких свойств одновременно.

Наконец, механизмы защиты кодируются в виде функций с сигнатурой $M:D \to D$, так как это отвечает мысли о том, что применение каждого механизма изменяет состояние системы. Благодаря тому, что механизм защиты в предлагаемой модели является функцией, а не значением, возможности определения свойств механизмов защиты значительно расширяются. Так, например, использование каких-либо двух механизмов может давать кумулятивный эффект или, наоборот, снижать эффективность третьего механизма.

Задав принципы кодирования составляющих задачи синтеза, определим и что является ее решением. Результатом синтеза системы защиты информации является множество функций M, такое, что при применении всех функций из этого множества к начальному состоянию АС d_0 будет достигнуто состояние оптимальной защиты. Это определение исходит из посылки, что композиция любых двух функций из M коммутативна. В большинстве случаев это условие соблюдается, однако при наличии в модели особенно сложных средств защиты может начать играть роль порядок их применения для достижения искомого состояния. В этом случае решением задачи синтеза будет являться не множество средств защиты, а однонаправленный граф, узлам которого соответствуют средства защиты из множества M, а ребра определяют порядок применения средств защиты к защищаемой АС. Легко заметить, что последний случай является обобщением первого – элементы множества можно связать в граф таким образом, что каждый узел будет иметь не более чем два ребра, а свойство направленности ребер графа здесь не играет роли.

Формально задача синтеза системы защиты АС с помощью SMT-решателя требует следующие входные данные:

1. Функция защиты $\phi_{защ}$, устанавливающая соотношение между исходным состоянием защищаемой АС и состоянием, которое необходимо достичь.

2. Множество функций $\phi_i(d_i, d_i+1)$, описывающих применяемые механизмы защиты. Как и в случае с $\phi_{защ}$, эффект от механизма защиты выражается в виде соотношения между предыдущим и следующим состояниями АС.

Обозначим $\phi_{сз} = \phi_1 \wedge ... \wedge \phi_n$. Тогда конечное выражение, подающееся на вход SMT-решателя, будет иметь вид

$$\exists \phi_{соед}(d_1, ..., d_n) \forall d_{вх}, d_{вых}, d_1, ..., d_n : (\phi_{сз}(d_1, ..., d_n) \wedge \wedge \phi_{соед}(d_1, ..., d_n)) \rightarrow \phi_{защ}(d_{вх}, d_{вых}), \quad (1)$$

где $\phi_{соед}$ – вспомогательная функция-ограничение, играющая роль композиции для функций ϕ_i.

Язык теории UFLRA, однако, не позволяет использовать функции в подкванторных выражениях. Чтобы решить эту проблему, вводятся дополнительные целочисленные переменные l_i в количестве, равном мощности множества M средств защиты. Эти переменные кодируют позиции узлов в графе и их связи с другими узлами. Эта мысль выражается ограничением $0 \le l_{d_i} \le N$. Таким образом, квантифицированное выражение $\exists \phi_{соед}: ...$ может быть заменено на $\exists l_{d_1}, ..., l_{d_n}: ...$, что удовлетворяет требованиям SMT-решателя.

К выражению (1) необходимо также добавить еще одно ограничение – требование отсутствия циклов в графе. Это ограничение имеет вид $l_{d_i} < l_{d_2} < ... < l_{d_n}$ и добавляется к выражению (1) с помощью конъюнкции.

Выражение синтеза передается на вход SMT-решателя, который подбирает значения переменных l_i, удовлетворяющие всем заданным ограничениям. Эти значения представляют собой решение задачи синтеза СЗИ в АС – последовательность действий, которые необходимо осуществить, чтобы достичь желаемого состояния системы, причем это решение будет использовать минимально необходимое число средств защиты. Если добавить полученное решение в выражение (1) в виде дополнительных ограничений, можно получить новое решение, отличающееся от предыдущего. Повторение этого процесса позволит найти все возможные решения задачи синтеза для данной АС.

Расширив домен дискурса D свойством, характеризующим оптимальность СЗИ с нужной нам точки зрения (например, соотношения цена/качество или производительность/качество), и задав отношение порядка между элементами D, можно трансформировать задачу синтеза в задачу поиска локального минимума или максимума. Современные SMT-решатели обладают функционалом для автоматического решения задач такого типа, то есть от пользователя даже не требуется дополнительного кодирования ограничений, выражающих искомые экстремумы.

В заключение необходимо отметить, что несмотря на свою эффективность описанный подход обладает и недостатками:

1. Формальное описание механизмов защиты является нетривиальной задачей и требует от пользователя определенных навыков.

2. Данный метод нельзя применять для автоматического синтеза СЗИ, так как задача удовлетворения ограничений, к которой сводится задача синтеза, является неразрешимой в общем случае. На практике имеет место тонкая подстройка параметров SMT-решателя, что требует участия человека.

3. Для получения окончательного решения необходима дополнительная обработка результатов, полученных от решателя.

4. Метод имеет экспоненциальную сложность по времени в зависимости от мощности в худшем случае.

СПИСОК ЛИТЕРАТУРЫ

1. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М. : Горячая линия – Телеком, 2006.

2. Apt, K. Principles of constraint programming / K. Apt. – Cambridge University Press, 2003.

3. Fischer, B. Autobayes: A system for generating data analysis programs from statistical models / B. Fischer and J. Schumann // J. Funct. Program. – 2003. – № 13(3). – P. 483–508.

4. Lauriere, J.-L. A Language and a Program for Stating and Solving Combinatorial Problems / J.-L. Lauriere // Artificial Intelligence. – 1978. – 10 (1). – P. 29–127.

5. Taly, A. Synthesizing switching logic using constraint solving / A. Taly, S. Gulwani and A. Tiwari // Proc. 10th Intl. Conf. on Verification, Model Checking and Abstract Interpretation, VMCAI. – Springer-Verlag, 2009. – P. 305–319.

6. The analysis of methods and approaches for modeling components of the complex organizational and technical systems “smart city” / Yu. S. Bakhracheva, A. A. Kadyrov, A. A. Kadyrova, E. A. Maksimova // Вестник Волгоградского государственного университета. Серия 10, Инновационная деятельность. – 2017. – Т. 11, № 2. – С. 6–10. – DOI: https://doi.org/10.15688/jvolsu10.2017.2.1.

REFERENCES

1. Belov E.B., Los V.P., Meshcheryakov R.V., Shelupanov A.A. *Osnovy informatsionnoy bezopasnosti. Uchebnoe posobie dlya vuzov* [Fundamentals of Information Security. Textbook for High Schools]. Moscow, Goryachaya liniya – Telekom Publ., 2006.

2. Apt K. *Principles of constraint programming*. Cambridge, Cambridge University Press, 2003.

3. Fischer B., Schumann J. Autobayes: A system for generating data analysis programs from statistical models. *J. Funct. Program*., 2003, no. 13 (3), pp. 483-508.

4. Lauriere J.-L. A Language and a Program for Stating and Solving Combinatorial Problems. *Artificial Intelligence*, 1978, vol. 10 (1), pp. 29-127.

5. Taly A., Gulwani S., Tiwari A.. Synthesizing switching logic using constraint solving. *Proc. 10th Intl. Conf. on Verification, Model Checking and Abstract Interpretation, VMCAI*. Springer-Verlag, 2009, pp. 305-319.

6. Bakhracheva Yu.S., Kadyrov A.A., Kadyrova A.A., Maksimova E.A. The analysis of methods and approaches for modeling components of the complex organizational and technical systems "smart city". *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 10, Innovatsionnaya deyatelnost* [Science Journal of Volgograd State University. Technology and Innovations], 2017, vol. 11, no. 2, pp. 6-10. DOI: https://doi.org/10.15688/jvolsu10.2017.2.1.

SYNTHESIS OF INFORMATION SECURITY SYSTEM BY MEANS OF SMT-SOLVERS

Gleb Aleksandrovich Popov

Senior Lecturer, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Tatyana Aleksandrovna Tikhomirova

Student, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The problem of synthesis of information security system for automated systems in general, is reduced to the optimal choice of such measures of protection that would ensure the functioning of the system at the minimum acceptable risks in terms of the existence of certain threats. Depending on the requirements for the automated system and the nature of its work, the tasks of synthesis would increase. For example, the concept of optimality of information security system can mean maximum efficiency of such system with minimal operation and maintenance, and the extent of its impact on the operation of the automated system. Another reason for the complexity of the problem is the possibility of varying the components which protect automated system. Finally, the main difficulty lies in the formalization of the list of threats and risk values, which can be dependent on various factors.

The article examines an original approach to solving the task of information security system's synthesis in the automated system. The authors propose the method for encoding the initial problem into a formalized one for a SMT solver. The method represents the characteristics of the security measures in the form of functions. The formula corresponding to the original problem is given in UFLRA theory language. The interpretation process of SMT solver's results is given. Shortcomings of the proposed method are outlined.

Key words: security system synthesis, constraint solving, informational security, automated system, overlapping system, decision-making.