В. Э. Вольфенгаген, А. А. Борзяк, А. С. Доронин, Л. Ю. Исмаилова, С. В. Косиков, В. В. Навроцкий

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ В УСЛОВИЯХ ВОЗНИКНОВЕНИЯ СЕМАНТИЧЕСКОЙ НЕСТАБИЛЬНОСТИ[1]

Обсудим вопрос развития эффекта возникновения семантической нестабильности и возможного нарушения безопасного режима функционирования информационной системы.

В настоящее время для представления предметной области наибольшую популярность имеют языки фреймов, а сам фрейм понимается как иерархически упорядоченное представление стандартной ситуации действительности [1–2]. Вместе с тем представление ситуаций, когда индивид меняет свои прежние свойства и начинает проявлять себя с новыми свойствами, становясь не отличимым от уже имевшихся индивидов с этими последними свойствами, в рамках известных формализмов не получает должного решения [3].

В приложениях при построении специализированных информационных систем, например, для блогосферы и иных динамичных интернет-сообществ подобный эффект возникает часто, а пути его преодоления все еще остаются до конца не изученными. В более общей постановке задача отыскания индивида по оставленной им «информационной траектории» в настоящее время выходит на передний план, требуя своего решения. Один из основных результатов данной работы связан с разработкой и применением специальной коммутативной диаграммы, позволяющей отслеживать «информационную траекторию» индивида. Это особенно важно и актуально для динамичных сетей, подвергающихся частой модификации и/или реорганизации [4–6].

Эффекты и диаграммы. Рассмотрим эффект, дающий представление о динамике предметной области, причем довольно общего вида. Более конкретно обсудим возможные пути изменения некоторых областей, составляющими элементами которых являются индивиды. В частности, можно обсуждать их «переселение», «клонирование», «копирование» и т. п. Содержательную интерпретацию g-переселения f-клонированных индивидов представим следующей диаграммой (рис. 1).

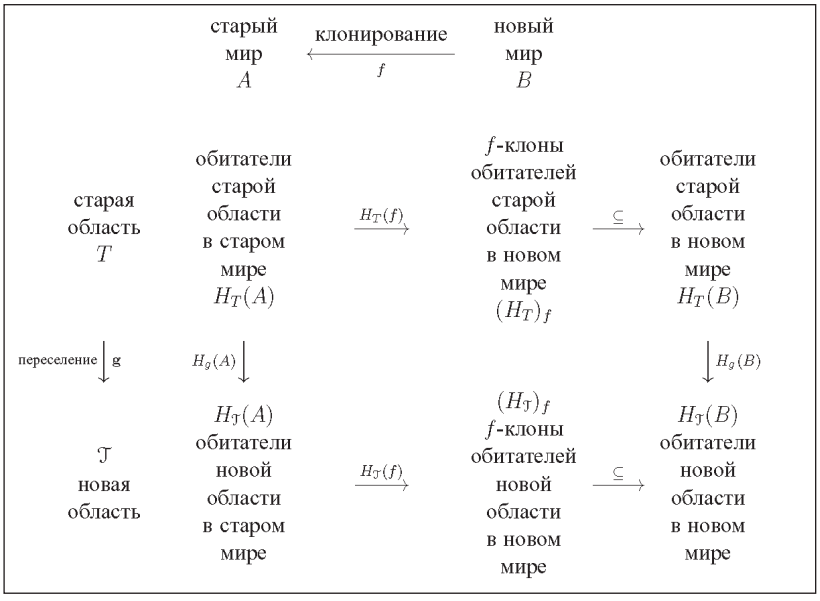

Рис. 1. Семантическая нестабильность под действием транзакций

[1] Работа является обобщением результатов, которые связаны с построением обобщенной вычислительной модели и получены в разное время при выполнении проектов, частично поддержанных грантами РФФИ 13-07-00679-а, 13-07-00705-а, 13-07-00716-а, 11-07-00305-а, 11-07-00096-а, 12-07-00554-а, 12-07-31091-мол-а, 11-07-00106-а, 11-07-00080-а.

Эта диаграмма базируется на определенных допущениях, касающихся поведения индивидов. Пусть сами по себе, под воздействием внутренних причин, индивиды не меняются, но могут стать или нет обитателями какой-либо области. Обитатели некоторой области могут порождаться, населяя данную область, а также могут перестать обитать в этой области, прекращая свое существование. Об этом можно говорить и в терминах переселения обитателей из одной области в другую. Таким образом, области могут меняться под воздействием каких-либо внешних причин, что будем связывать с транзакциями. Можно также считать, что индивиды меняются под воздействием каких-либо внутренних причин вне зависимости от того, меняются области или нет. Это будем связывать с клонированием.

Небезопасное взаимодействие объектов. На приведенной схеме показан фундаментальный вариант взаимодействий объектов, примером и частным случаем которых служит семантическая сеть. Один объект-участник взаимодействия заставляет другие объекты действовать в интересах его схемы разворачивания событий и так, что это не противоречит структуре организации объектов атакованной системы, не распознается ее механизмами и не вызывает с их стороны отвергания взаимодействия. Возникает случай манипулирования сетью, осуществленный путем подмены той существенной части сети, например одного из ее концептов, в котором записана принципиально важная для функционирования и развития сети «программа».

Можно предложить некоторые решения по локализации подобных семантических вирусов, когда одним из концептов вместе с сопутствующим ему фрагментом семантической сети приходится пожертвовать ради сохранения работоспособности и целостности всей сети.

Вирусование. Вирусование можно признать состоявшимся лишь в том случае, когда индивид начинает выступать в прежде несвойственном ему качестве, причем не запланированным им способом. Действительный смысл вирусования оказывается скрытым, причем требуются специальные действия по его выявлению. Возникающие случаи и ситуации приходится подвергать исследованию. Если исследование окажется успешным, то это означает, что получено направление действий, способных различать вирусованные и невирусованные индивиды. Для этого понадобится, как минимум, механизм логической фильтрации, который позволяет ответить на вопрос, есть ли у индивидов признаки вирусования.

Кроме того, можно воспользоваться интерпретацией индивидов, позволяющей отличить трансформированного индивида от «здорового». В собственном смысле этого слова интерпретация, или толкование, понимается как восстановление неявных или специально скрытых связей с контекстом, со средой. В данном случае приходится виртуально воссоздавать как можно более полный контекст обитания индивида и различными способами погрузить в него имеющиеся факты об этом индивиде. При этом выполняется отбор наиболее существенных сторон, сопровождающийся их классификацией. Выразительные возможности интерпретации определяются способностью устанавливать переходы индивида от одного контекста к другому, а получающиеся при этом «моментальные фотографии» действительности — сводить единые смысловые блоки.

Варианты интерпретации. Можно предложить два подхода к выполнению интерпретации. В первом из них просто дается логический анализ поведения индивида. Если устанавливаются нарушения семантической целостности, противоречивости, то интерпретируемый индивид рассматривается как кандидат на то, что он трансформирован. При ином подходе его поведение рассматривается как одно из целого спектра возможностей. Далее каждая из возможностей погружается в сгенерированный для фиксации возможной трансформации контекст.

Состояния сети. В рассуждениях с объектами состояние рассматривается как значение функции, взятой из функциональной схемы, в заданной точке — одной из многих «точек

наблюдения». Это находится в полном соответствии с общей моделью и средой вычислений, основанной на представлении о переменном домене, или объекте $H_T(I)$:

$H_T(I) = \{h \mid h : I \to T\}$.

Переходы состояний описываются следующим образом. С вычислительной точки зрения множество индивидов порождается, например, из T посредством:

$H_T(\{i\}) \subseteq T$ для $i \in I$.

Это состояние является состоянием переменного объекта $H_T(I)$, где T представляет собой локальный универсум возможных индивидов. Указатель i маркирует семейство индивидов, которое «наблюдаемо» из i. Состояния $s1$, $s2$... функциональной схемы получают представление посредством стадий переменного объекта:

$s1 : H_T(\{i\}) = \{h(i)\} \subseteq T$

$s2 : H_T(\{i\}) = \{h(i)\} \subseteq T$

... : ... ...

Переходы, или преобразования, $g : s1 \to s2$ являются компонентами событий (они представляются тройками):

$<s1, s2; g>$.

Идея переменного объекта дает естественное представление эффектов перехода в случае динамики вычислений с объектами. Более того, оно обеспечивает удобный метатеоретический контекст. Всевозможные эффекты выражаются добавлением естественных преобразований H_g : $H_T \to H_T$ для отображения

$g : T \to T$.

Поэлементный анализ для $i \in I$ дает:

$H_g(I)$: $H_T(I)$ э $h \to g \circ h \in H_T(I)$,

$H_g(\{i\})$: $T \supseteq \{h(i)\} \to \{(g \circ h)(i)\} \subseteq T$.

А это означает, что множество преобразований вводит законы предметов, т. е. те законы, которым предметы обязаны удовлетворять в случае рассуждений с объектами.

Как немедленный и непосредственный результат, получается ясное понимание взаимодействия предметов — посредством переменной состояния, являющейся общей для взаимодействующих предметов. Таким образом, множество естественных преобразований является представлением законов. А приводимая далее короткая диаграмма определяет, о каких именно законах идет речь:

$\{h(i)\} \subseteq T$,

$x1 \in \{h(i)\}$; $x2 \in \{h(i)\}$; $z \in T$,

... $\Phi(x1)$ & $\Psi(x2)$ & $x1 = z$ & $x2 = z$ ... ,

где z — общая переменная (объединенная переменная состояния).

Сходными приемами можно дать анализ практически значимых частных случаев общей диаграммы на рис. 1.

Заключение. Представлен подход к обеспечению безопасности информационной системы в условиях возникновения семантической нестабильности.

1. Сформулировано представление о семантической нестабильности в работе информационной системы.

2. При анализе случаев семантической нестабильности учтено воздействие транзакций.

3. Проанализированы условия, при которых из-за семантической нестабильности возможно нарушения безопасного режима функционирования информационной системы.

4. Построена базовая вычислительная модель индивидов и концептов, фиксирующая семантическую нестабильность и потенциально способная ее предотвратить.

СПИСОК ЛИТЕРАТУРЫ:

1. *Wolfengagen V. E.* Applicative computing. Its quarks, atoms and molecules / Edited by Dr. L. Yu. Ismailova. Moscow: «Center JurInfoR», 2010. — 62 p.
2. *Вольфенгаген В. Э., Исмаилова Л. Ю., Косиков С. В.* Структура компьютинга и конструирование вычисления // Наука и образование. МГТУ им. Н. Э. Баумана. Электрон. журн. 2010. № 08. URL: http://technomag.edu.ru/doc/153062.html (дата обращения: 15.12.2012).
3. *Вольфенгаген В. Э., Исмаилова Л. Ю., Косиков С. В.* Модель вычислений, чувствительная к семантической нестабильности // Наука и образование. МГТУ им. Н. Э. Баумана. Электрон. журн. 2010. № 12. URL: http://technomag.edu.ru/doc/163548.html (дата обращения: 15.12.2012).
4. *Исмаилова Л. Ю., Косиков С. В., Вольфенгаген В. Э., Зинченко К. Е.* Средства инструментальной поддержки композиции и специализации предметно-ориентированных механизмов наследования для правовых деловых игр // В мире научных открытий. 2010. № 1—4. С. 32—36. URL: http://nkras.ru/vmno/issues/articles/2010/1-4.pdf (дата обращения: 15.12.2012).
5. *Вольфенгаген В. Э., Исмаилова Л. Ю., Косиков С. В., Лаптев А. Д., Назаров В. Н., Рословцев В. В., Сафаров И. С., Степанов А. Л.* Аппликативный компьютинг: попытки установить природу вычислений // Вестник Удмуртского университета. Сер. 1: Математика. Механика. Компьютерные науки. Электрон. журн. 2009. Вып. 2. С. 110—117. URL: http://vst.ics.org.ru/uploads/vestnik/2_2009/vu09213.pdf (дата обращения: 15.12.2012).
6. *Вольфенгаген В. Э., Исмаилова Л. Ю., Косиков С. В., Лаптев А. Д., Назаров В. Н., Рословцев В. В., Сафаров И. С., Степанов А. Л.* Комбинаторы: объекты, помогающие понять строение компьютинга // Вестник Удмуртского университета. Сер. 1: Математика. Механика. Компьютерные науки. Электрон. журн. 2009. Вып. 2. С. 118—131. URL: http://vst.ics.org.ru/uploads/vestnik/2_2009/vu09214.pdf (дата обращения: 15.12.2012).

Е. И. Гончаров

АВТОМАТИЧЕСКАЯ ДЕОБФУСКАЦИЯ ИСПОЛНЯЕМОГО КОДА, ЗАЩИЩЕННОГО С ПРИМЕНЕНИЕМ ВИРТУАЛЬНЫХ МАШИН

Обфускация, или запутывание кода, — это модификация кода программы таким образом, что она полностью сохраняет свою функциональность, но анализ и понимание алгоритмов ее работы значительно усложняются. Обфускация может применяться как для защиты законных интересов (например, для сокрытия авторских алгоритмов), так и для маскировки недекларированных возможностей ПО. Причем использование запутывания кода во вредоносном ПО в настоящий момент крайне широко распространено. Таким образом, для анализа подобных программ автоматизирование деобфускации, или «распутывания кода», является актуальной проблемой.

Для деобфускации бинарного кода, запутанного с использованием непрозрачных предикатов, свойства полиморфизма и добавления «мертвого» кода, достаточно успешно применяются методы символьного исполнения и абстрактной интерпретации [1]. В то же время код, защищенный с помощью виртуальных машин, все еще представляет серьезную проблему, так как успешность анализа сильно зависит от опыта аналитика. В этой работе описывается разрабатываемый автоматический метод деобфускации виртуальных машин класса «decode-dispatch», в основе которого лежат указанные методы символьного исполнения и абстрактной интерпретации, учитывающие характерные особенности данного класса. В случае успеха в разработке данного метода решение этой актуальной задачи перейдет из разряда трудоемких в разряд примитивных.

СПИСОК ЛИТЕРАТУРЫ:

1. *Udupa S. K., Debray S. K., Madou M.* Deobfuscation: Reverse Engineering Obfuscated Code // 12th Working Conference on Reverse Engineering, 2005. С. 45-54.