С. С. Агафьин, А. А. Краснопевцев

ВЕРИФИКАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТЧУЖДАЕМЫХ НОСИТЕЛЕЙ КЛЮЧЕВОЙ ИНФОРМАЦИИ

В связи с постоянным увеличением спроса на системы, использующие отчуждаемые носители ключевой информации (ОНКИ), задача обеспечения безопасности данных, обрабатываемых в них, становится актуальной. Наибольшее распространение среди ОНКИ приобрела платформа JavaCard, реализующая виртуальную машину для упрощенной версии языка Java. С целью повышения безопасности ее использования предлагается разработать внешнюю по отношению к ОНКИ систему верификации байт-кода, которая позволит удостовериться в отсутствии определенных уязвимостей в программном обеспечении [1].

Отсутствие верификатора байт-кода в платформе JavaCard может приводить к возникновению уязвимостей, рассмотрение которых становится актуальным при появлении нарушителя, имеющего доступ к программному коду разрабатываемого Java-апплета либо к байт-коду до его записи в ОНКИ.

В спецификации JavaCard присутствует обязательный внешний верификатор, однако он используется до преобразования скомпилированного байт-кода в загрузочный модуль апплета, а значит, не может обеспечить защиту от рассматриваемого нарушителя [2].

Предлагается система верификации байт-кода загружаемого апплета, которая позволит исключить заданные уязвимости, специфичные для выбранной модели нарушителя.

СПИСОК ЛИТЕРАТУРЫ:

1. *Mostowski W., Poll E.* Malicious Code on Java Card Smartcards: Attacks and Countermeasures // LNCS. 2008. Vol. 5189. P. 1–16.
2. Java Card Platform Specification 3.0.1. URL: http://www.oracle.com/technetwork/java/ (дата обращения: 30.01.2013).

И. М. Азымшин, В. О.Чуканов

АНАЛИЗ БЕЗОПАСНОСТИ РЕЗЕРВИРОВАННЫХ СИСТЕМ

Оценка безопасности работы больших систем производится методом ветвей и границ. Метод ветвей позволяет получить нижнюю границу безопасности. Методом границ определяется верхняя граница безопасности. Рассмотрим получение нижней границы безопасности на примере. Представим систему в виде графа с элементами системы в вершинах и ребрами, обозначающими связи элементов с точки зрения безопасности. Каждый элемент системы обладает заранее известной вероятностью безотказной работы P_i.

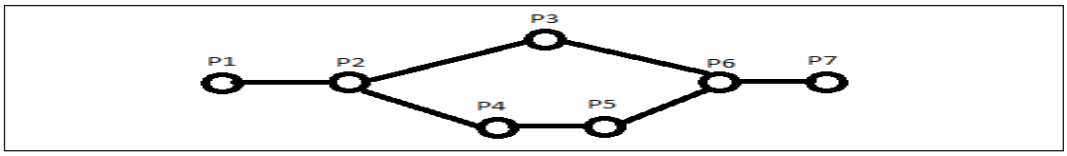

Рис. 1. Произвольная вычислительная система

Предположим, что $P_1<P_2<P_3<P_4<P_5<P_6<P_7$.

Вероятность безотказной работы группы объектов равна произведению вероятностей безотказной работы каждого объекта в этой группе.

Вероятность безотказной работы:

- для ветви $\{P_1,P_2,P_3,P_6,P_7\}$: $P_1 \cdot P_2 \cdot P_3 \cdot P_6 \cdot P_7$,
- для ветви $\{P_1,P_2,P_4,P_5,P_6,P_7\}$: $P_1 \cdot P_2 \cdot P_4 \cdot P_5 \cdot P_6 \cdot P_7$.

Основной задачей для метода ветвей и границ является нахождение ветви с минимальной вероятностью безотказной работы. Все множество ветвей разбивается на подмножества таким образом, чтобы каждое подмножество содержало ветвь, которую не содержат другие. Для каждого подмножества определяется его граница безопасности. Из подмножеств выбирается подмножество с минимальной границей безопасности. Процесс ветвления продолжается до тех пор, пока не отыщется первая ветвь с минимальной границей безопасности. Ее называют «первым рекордом». Затем просматривают остальные ветви. Если их нижние границы больше границы «первого рекорда», то задача решена. Если же есть такие ветви, для которых нижние границы меньше, чем граница «первого рекорда», то подмножество с наименьшей нижней границей подвергается дальнейшему ветвлению, пока не убеждаются, что оно не содержит ветви с меньшей границей безопасности. Если же такая ветвь найдется, то анализ остальных ветвей продолжается относительно нового значения границы безопасности. Эту ветвь называют «вторым рекордом». После анализа всех подмножеств ветвь, являющаяся «вторым рекордом», оказывается ветвью с минимальной вероятностью безотказной работы. В приведенном примере это ветвь $\{P_1,P_2,P_4,P_5,P_6,P_7\}$.

Для систем малой размерности допустимо использование метода усеченного сканирования. В этом методе предполагается выбор критерия, который позволяет не проводить сканирование части ветвей графа. Выберем в качестве такого критерия наличие в ветви элементов с вероятностью безотказной работы ниже значения элемента P_4. Таким образом, в приведенном ранее примере из рассмотрения исключается ветвь $\{P_1,P_2,P_4,P_5,P_6,P_7\}$. Далее для оставшихся ветвей проводится процедура полного сканирования. И выбирается ветвь с минимальным значением вероятности безотказной работы. В приведенном примере это ветвь $\{P_1,P_2,P_3,P_6,P_7\}$.

Для повышения безопасности системы возможно использование резервирования ее элементов. При резервировании элемента повышается его значение вероятности безотказной работы. Рассмотрим резервирование на основе мажоритарной логики, которое используется при резервировании элементов или целых блоков. При мажоритарном резервировании сигнал подается на нечетное число идентичных элементов. С выходов этих элементов сигналы поступают на вход так называемого решающего (мажоритарного) элемента, назначением которого является выделение из группы сигналов (среди которых могут быть и ошибочные) безошибочного сигнала. Мажоритарный элемент выдает сигнал на своем выходе только в том случае, если на его вход поступили аналогичные сигналы от большинства идентичных элементов, т. е. его выходной сигнал всегда принимает значение, равное значению большинства входных сигналов (2 из 3, 3 из 5 и т. д.). Рассмотрим мажоритарный элемент, реализующий операцию «два из трех». Будем считать, что вероятности безотказной работы резервированных элементов равны. И вероятность безотказной работы одного резервированного

элемента равна P_0. Тогда в случае, если мажоритарный элемент обладает идеальной надежностью, т. е. $P_р = 1$, вероятность безотказной работы блока равна $P = 3 \cdot P_0^2 - 2 \cdot P_0^3$. Если же решающий элемент неидеален, т. е. $P_р \neq 1$, то вероятность безотказной работы блока равна $P = P_р \cdot (3 \cdot P_0^2 - 2 \cdot P_0^3)$. В рассматриваемой вычислительной системе проведем резервирование элементов P_3 и P_6 с помощью мажоритарного элемента, реализующего операцию «два из трех». Используя метод ветвей и границ, рассчитаем вероятность безотказной работы всей системы.

Вероятность безотказной работы:

- для ветви $\{P_1,P_2,P_3,P_6,P_7\}$: $P_1 \cdot P_2 \cdot [P_р \cdot (3P_3^2 - 2P_3^3)] \cdot [P_р \cdot (3P_6^2 - 2P_6^3)] \cdot P_7$,
- для ветви $\{P_1,P_2,P_4,P_5,P_6,P_7\}$: $P_1 \cdot P_2 \cdot P_4 \cdot P_5 \cdot [P_р \cdot (3P_6^2 - 2P_6^3)] \cdot P_7$.

Вероятность безотказной работы рассматриваемой вычислительной системы будет равна минимальной вероятности безотказной работы двух ветвей.

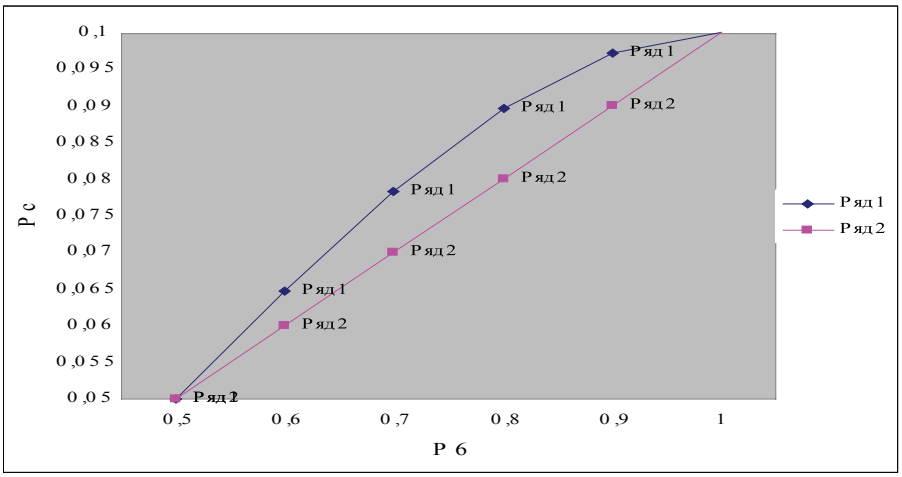

Рис. 2. Графики безотказной работы для ветви $\{P_1,P_2,P_4,P_5,P_6,P_7\}$ в зависимости от изменения вероятности безотказной работы элемента P_6 ($P_{яд1}$ — с резервированием элемента P_6, $P_{яд2}$ — без резервирования элемента P_6)

В работе рассмотрены методы оценки безопасности вычислительных систем. Описан метод повышения безопасности вычислительных систем. Приведены формулы расчета вероятности безотказной работы для произвольной вычислительной системы.

СПИСОК ЛИТЕРАТУРЫ:

1. *Чуканов В. О.* Надежность программного обеспечения и аппаратных средств систем передачи данных атомных электростанций: Учебное пособие. М.: МИФИ, 2008.
2. *Гуров В. В., Чуканов В. О.* Основы теории и организации ЭВМ. М.: БИНОМ. Лаборатория знаний, 2012.
3. *Александрович А. Е., Бородакий Ю. В., Чуканов В. О.* Проектирование высоконадежных информационно-вычислительных систем. М.: Радио и связь, 2004.
4. *Коваленко И. Н., Кузнецов Н. Ю.* Методы расчета высоконадежных систем. М.: Радио и связь, 1988.