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.