КОМПЛЕКСНАЯ ЗАЩИТА ВСТРАИВАЕМЫХ ЗАПОМИНАЮЩИХ УСТРОЙСТВ ОТ НЕСАНКЦИОНИРОВАННЫХ ИЗМЕНЕНИЙ

С.Б. Мусин, А.А. Иванюк
ООО Softeq Flash Solutions
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: sergei.musin@softeq.com, ivaniuk@bsuir.by

Предлагается комплексный подход к защите запоминающих устройств (ЗУ), при котором ЗУ рассматривается как самоподдерживающаяся система, в которой возможны санкционированные и несанкционированные изменения. В рамках такого подхода совместно с методом адаптивного сигнатурного анализа (АСА) применим алгоритм отрицательного отбора искусственной иммунной системы для контроля ЗУ.

Введение

Высокая конкуренция на быстро растущем рынке современных мобильных устройств приводит к все большей степени интеграции компонентов на одном кристалле. А она, в свою очередь, к выдвижению все более жестких требований к надежности «Систем-на-Кристалле» (СнК), ввиду высокой вероятности появления случайных сбоев и неисправностей. Хранение персональной и конфиденциальной информации, а также перспективы использования мобильных устройств для осуществления бесконтактных платежей вносят особые требования к защищенности информации от злоумышленников.

В СнК интегрированы различные функциональные блоки, но наиболее важными с точки зрения надежности и защиты информации являются запоминающие устройства (ЗУ). Во-первых, ЗУ занимают большую площадь кристалла по сравнению с другими функциональными блоками. Во-вторых, ЗУ хранят пользовательские данные, которые являются объектом атаки злоумышленника.

Несмотря на то, что комплексные подходы к проектированию СнК существуют уже достаточно давно, подходов к совместному рассмотрению надежности и защищенности немного [1]. В настоящем докладе рассматривается защищита ЗУ от несанкционированных изменений, которые являются результатом как случайных сбоев и неисправностей элементов ЗУ, так и результатом воздействия злоумышленника с целью неавторизованного использования.

I. Существующие подходы

Как правило, на СнК располагается дополнительная аппаратура оперативного контроля и встроенного самотестирования ЗУ. Оперативный контроль используются во время работы ЗУ по назначению. При записи информации в ЗУ устройство контроля добавляет избыточность, которая позволяет обнаруживать ошибки при считывании. При самотестировании функционирование ЗУ по назначению останавливается, затем на вход подаются тестовые наборы, по реакции на которые определяется наличие неисправностей. В современных ЗУ применяется контроль с использованием помехоустойчивых кодов, а также тестирование на базе разрушающих и неразрушающих маршевых тестов. В последних, для определения реакции схемы на тестовые воздействия, применяется сигнатурный анализ (СА). Для повышения надежности хранения информации в ЗУ применяется математический аппарат теории помехоустойчивого кодирования. При этом хранимое в ЗУ слово считается сообщением, которое передается по каналу связи, не в пространстве, а во времени. Однако, существует ряд отличительных особенностей функционирования ЗУ [2-3]. Так, в работе [2] предлагается рассматривать ЗУ как специфический канал связи, так как: 1) ЗУ работают по схеме «кодирование – передача по каналу связи – перекодирование – декодирование» (перекодирование осуществляется в случае необходимости изменения информации без предварительного считывания), 2) приемник и источник сообщения в ЗУ физически располагаются в одном месте, что позволяет использовать одно устройство для выполнения кодирования и декодирования, 3) возможен саморемонт ЗУ с учетом местоположения дефектных запоминающих элементов. В обзоре [3] выделяются следующие отличительные признаки обращения с содержимым ЗУ от сообщения, передаваемого по каналу связи: 1) сообщение поступает в приемник последовательно, а хранимое слово записывается целиком; 2) цикл обращения к ЗУ ограничивает время кодирования и декодирования, 3) кодер и декодер должны быть комбинационными схемами ограниченной глубины. Здесь же приведены цели и перспективы дальнейших исследований, среди которых необходимость кодирования, наряду с хранящимися в памяти данными их адресов, а также проводить совместное изучение кодовой защиты памяти и

ее диагностики методами СА. Указанные цели были достигнуты с разработкой метода адаптивного сигнатурного анализа (АСА) [4].

СА позволяет избежать сравнения с эталоном большого количества тестовых реакций путем их сжатия с определенной степенью достоверности в компактную оценку – сигнатуру. При этом содержимое ЗУ кодируется с использованием циклического кода [5]. Применение СА в процессе функционирования ЗУ по назначению существенно замедляет работу, так как необходимо повторное вычисление сигнатуры при каждом изменении хранимых данных. Метод адаптивного сигнатурного анализа (АСА) решает эту проблему путем суммирования по модулю два предыдущего значения сигнатуры и адреса ячейки, хранимое значение в которой изменилось.

Как было показано в работе [6] применение математического аппарата теории кодирования к методу АСА отличается от других подходов. В методе АСА все данные хранимые ЗУ рассматриваются в качестве кодового слова, например, кода Хэмминга (адреса ЗУ соответствуют столбцам проверочной матрицы кода), а сигнатура как синдром этого кодового слова. Запись информации в ЗУ рассматривается как санкционированное изменение первоначального кодового слова и сопровождается соответствующим изменением синдрома (сигнатуры). При возникновении несанкционированных изменений (сбой, неисправность) синдром не изменяется. Для проведения контроля целостности хранимых данных синдром рассчитывается повторно, а наличие ошибок определяется по разности с эталонным синдромом.

II. Предлагаемый подход

Представление ЗУ как специфического канала связи, предполагает пассивное удержание информации во времени, причем надежность хранения информации зависит только от физической надежности ЗУ и используемого кода коррекции ошибок. С другой стороны, на примере метода АСА видно, что наличие динамического процесса (периодического контроля ЗУ), не вписывается в такую парадигму. Судя по всему, эффективнее рассматривать ЗУ как активную самоподдерживающуюся систему (self-sustaining system) [7]. В такой системе сохранение устойчивого состояния с течением времени поддерживается отрицательной обратной связью. Иными словами, целостность хранимой информации контроллируется периодически, а в случае необходимости производится самокоррекция и самовосстановление информации.

Эффективность такого представления иллюстрирует концепция искусственной иммунной системы (ИИС), основная роль которой заключается в распознавании контроллируемых объектов и классификации их как «своих» или «чужих». Наиболее распространенной моделью ИИС, является алгоритм отрицательного отбора (АОО). В работе [8] показана применимость АОО к анализу тестовых реакций при самотестировании цифровых схем. Причем точное обнаружение ошибок возможно с помощью сравнительно небольшого количества детекторов и использованием различных правил сравнения.

Рассмотрим АОО применительно к ЗУ:

Шаг 1. Генерируется набор детекторов, который состоит из заданного количества случайных двоичных векторов, размерности равной размерности сигнатуры АСА. Шаг 2. В процессе функционирования ЗУ по назначению происходит сравнение значений принимаемых эталонной сигнатурой с элементами множества детекторов и, если какой-то из элементов множества совпадает со значением сигнатуры («свой»), то он заменяется в этом множестве новым. Шаг 3. Периодически выполняется процедура самоконтроля, в которой рассчитывается рабочая сигнатура и сравнивается помимо текущей эталонной с элементами набора детекторов. Если сигнатуры из набора детекторов сравнимы с рабочей сигнатурой («чужой»), считается возможным несанционтрованный доступ к содержимому ЗУ.

Заключение

Перспективным направлением дальнейших исследований является оценка роста количества детекторов необходимых для поддержания требуемой достоверности системы контроля, исследование методов повышения достоверности, а также эффективной аппаратной реализации.

1. Zhen Wang, Karpovsky, M. Reliable and secure memories based on algebraic manipulation correction codes // in On-Line Testing Symposium (IOLTS), 2012 IEEE 18th International, june 2012, pp. 146–149.
2. Guillaume Duc and Ronan Keryell, CryptoPage: An Efficient Secure Architecture with Memory Encryption // Integrity and Information Leakage Protection, ACSAC 2006. LNCS, 2006, pp. 483–492, Springer
3. Конопелько В.К., Лосев В.В. Надежное хранение информации в полупроводниковых запоминающих устройствах. М.: Радио и связь, 1987
4. Сагалович Ю.Л., Кодовая защита оперативной памяти // Автоматика и телемеханика, №5, 1991. – С. 3-45
5. Ярмолик В.Н., Иванюк А.А. Встроенное самотестирование памяти с использованием сигнатурного анализа // Логическое проектирование, 1997. – С.170-180
6. Горшков В.Н. Надежность оперативных запоминающих устройств ЭВМ. Л.: Энегроатомиздат, 1987
7. Иванюк А.А., Мусин С.Б., Ярмолик В.Н. Использование адаптивного сигнатурного анализа для обнаружения многократных ошибок ОЗУ // Микроэлектроника, №3, 2007. – С.246-253
8. Cleonilson P. Souza, Francisco M. Assis, Raimundo C. S. Freire, Embedded Integrated Circuit Testing Based On Artificial Immune Systemи // Revista INNOVER, Vol. 1, No 1, March 2014 - P.1-8