Основная идея защиты проектов от неавторизованного пользователя основана на кодировании комбинационных схем цифровых устройств. Защита базируется на введении дополнительных логических элементов в структуру схемы, формировании ключевого кода, применение которого вводит схему в область правильного функционирования [3]. Основная задача, которая должна быть решена для эффективной практической реализации данной общей идеи, заключается в том, чтобы определить оптимальное множество внутренних линий схемы и количество ключевых элементов для создания максимальных трудностей для злоумышленника по поиску правильного ключа.

В докладе задача кодирования сводится к поиску неисправностей константного типа кодируемой структуры, обнаруживаемых на большем количестве выходных линий и на максимальном количестве входных векторов. Для решения задачи применяются методы и средства тестового диагностирования [4, 5].

Список литературы

1. Security analysis of integrated circuit camouflaging / J. Rajendran [et al.] // ACM SIGSAC conference on Computer & communications security. Berlin. 4–8 November 2013. P. 709–720.

2. Hardware Trojans: Lessons learned after one decade of research / K. Xiao [et al.] // ACM transactions on design automation of electronic system. 2016. Vol. 22. No. 1.

3. Weighted Logic Locking: A New Approach for IC Piracy Protection / N. Karousos [et al.] // IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS). 2017. P. 221–226.

4. Золоторевич Л.А. Функциональный контроль СБИС типа СнК // Сб. науч. статей «Технологии автоматизации и управления». 2017. Вып. 3. В 2 кн. Книга 2. С. 216–225.

5. Золоторевич Л.А. Модели неисправностей при верификации проектов и контроле цифровых систем // Матер. Междунар. науч. конф. «Компьютерные науки и информационные технологии». Саратов, 2018. С. 160–163.

МЕТОДЫ ПОВЕДЕНЧЕСКОЙ АНАЛИТИКИ В ПОСТРОЕНИИ МОДЕЛИ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.М. Кадан

Модель вероятного нарушителя информационной безопасности важна для систематизации данных о возможностях и типах нарушителей, целях их несанкционированных воздействий и выработки адекватных организационных и технических методов противодействия. Правильно разработанная модель вероятного нарушителя является гарантией построения адекватной системы обеспечения информационной безопасности: опираясь на построенную модель, можно строить адекватную систему информационной защиты. При разработке модели нарушителя обычно учитывают: категории лиц, к которым можно отнести нарушителя; цели, градации по степени опасности и важности; анализ его технических возможностей; предположения и ограничения о характере действий.

В докладе предлагается и демонстрируется построение модели вероятного нарушителя на основе анализа лог-файлов информационной системы. Анализ ведется с использованием методов поведенческой аналитики, среди которых выделяется метод когортного анализа [1]. Когортный анализ рассматривает данные из некоторого набора данных (например, платформы электронной коммерции, веб-приложения или онлайн-игры), и вместо того, чтобы рассматривать всех пользователей как единое целое, разбивает их на связанные группы. Идея когортного анализа состоит в том, чтобы выполнить такое разбиение по определенным признакам или похожему поведению, и отслеживать развитие этих групп во времени в течение определенных временных интервалов. Построение модели нарушителя было продемонстрировано на примере информационной системы, являющейся компьютерной игрой для социальных сетей. Использование лог-файлов такой системы позволило получить для исследования набор данных объемом более 600 ГБ, содержащий около 10^{10} записей о поведении более 35 млн. пользователей. В качестве основных характеристик рассматривалась минимизация финансовых потерь разработчика от применения целенаправленной рекламы.

Список литературы

1. Aukeman, Mark. Cohort Analysis – understanding your customers / edwblog.com | EDW+ Delivering on the Big Data promise [Электронный ресурс]. URL: http://edwblog.com/adhoc/cohort-analysis-%E2%80%94-understanding-customer-behavior/32 (дата доступа: 09.05.2019).

БЕЗОПАСНОСТЬ СИСТЕМЫ И СИСТЕМА ОТКАЗОУСТОЙЧИВОСТИ

Камил Ихаб Абдулджаббар Камил, М.Б. Абросимов

Отказоустойчивость компьютерной системы – это способность системы продолжать сохранять свою работоспособность после отказа одного или нескольких составных компонентов. Начиная с середины 90-х годов быстрое развитие вычислительных программных приложений, работающих в режиме реального времени, особенно спроса на интеллектуальные устройства, встроенные в программное обеспечение, породило насущную проблему, связанную с отказоустойчивостью программного обеспечения. Неизбежность появления проблемы заключается в том, что синтез системы выполняется лицом, не являющимся специалистом этой системы. Большинство людей, регулярно пользующиеся компьютерами, сталкиваются с проблемой сбоя системы либо сбоев программного обеспечения, работы диска, потери питания, либо в результате ошибки шины. В некоторых случаях эти сбои не более чем мелкая неприятность; в других же случаях они приводят к значительным потерям. Второй вывод, вероятно, станет более распространенным, нежели предыдущий, поскольку зависимость общества от автоматизированных систем возрастает. Отказоустойчивая система должна быть в состоянии устранять неисправности отдельных аппаратных или программных компонентов, устранять сбои питания или другие виды неожиданных аварий и по-прежнему соответствовать своей спецификации. Отказоустойчивость необходима еще и потому, что без нее практически невозможно создать идеальную систему.Надежность системы – это вероятность того, что она будет оставаться работоспособной (потенциально, несмотря на сбои) в течение всего периода работы. Наличие у системы очень высокого уровня надежности наиболее значимо в критически важных приложениях, связанных с управлением космическими кораблями многоразового использования или промышленными объектами, в работе которых любой сбой может повлечь гибель людей [1]. Безопасность и надежность системы – это те вопросы, которые становятся все более важными в сегодняшнем развивающемся мире. Безопасность, гарантирующая выполнение системой требуемой работы, идет рука об руку с надежностью, гарантирующей правильность работы системы. Взаимодействие безопасности и надежности является краеугольным камнем бесперебойной работы функциональной системы на долгие годы. Безотказность работы системы является одним из аспектов ее надежности; однако она по своей природе более сложна, чем безопасность системы, поскольку она содержит атрибуты триады информационной безопасности (CIA) («конфиденциальность, целостность и доступность»). При этом к трем указанным атрибутам необходимо добавить три других: защищенность (безопасность), эксплуатационная технологичность и надежность. Защищенность (безопасность) системы характеризуется «отсутствием аварийных последствий для пользователей и окружающей среды». Эксплуатационная технологичность означает способность системы производить текущий ремонт, техническое обслуживание и вносить другие изменения, такие как исправления и обновления системы. Поскольку безопасность и надежность системы направлены на решение одной и той же цели, способствующей ее доступности, надежность системы тесно взаимосвязана с ее безопасностью. В большинстве случаев мы можем утверждать, что более надежная система должна быть безопасной. Меры безопасности применяются к системе с целью обеспечения ее надежности; но, если вследствие атаки будет нанесен ущерб безопасности системы, то тогда доступ к ней будет прекращен в тех случаях, когда надежность системы гарантирует ее доступность[2].

Список литературы

1. Basic Concepts and Taxonomy of Dependable Secure Computing / Avizienis Algirdas [et al.] // Process for developing common vocabulary in the information security area. 2007. № 1. P. 10–51.