Шаповалов Е.В. Применение методов QA-инженерии при анализе функциональной безопасности драйверов. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей VIII Всерос. научно-техн. конф. – Пенза: ПДЗ, 2008. – С. 118-120.

ПРИМЕНЕНИЕ МЕТОДОВ QA-ИНЖЕНЕРИИ ПРИ АНАЛИЗЕ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ДРАЙВЕРОВ

Е.В. Шаповалов

Астраханский государственный технический университет,
г. Астрахань

При аттестации объектов автоматизации на соответствие категории защищенности немаловажную роль играют спецпроверки и специсследования аппаратного обеспечения АС, входящих в объект автоматизации. Спецпроверки проводятся для выявления вредоносных элементов среди электронных компонентов АС. Специсследования ориентированы на оборудование, входящее в комплекс исследования, и не связывают работу оборудования с программным обеспечением АС. Тем не менее работа оборудования целиком и полностью зависит от программной конфигурации устройства в ОС. Анализ канала утечки информации через ПЭМИ при заданной конфигурации возлагается на человека, так же, как и контроль за неизменностью конфигурации при дальнейшей работе АС. Основные программные модули операционных систем, осуществляющие взаимодействие с аппаратурой, в большинстве ОС работают на уровне ядра, и практически все их действия скрыты от пользователя. Это уровень вседозволенности в системе. Поменяв несколько параметров работы оборудования, можно изменить его излучающие характеристики, а значит, и расширить зону разведдоступности. За работой драйверов следят программы, работающие на том же уровне, что и сам драйвер, и скрыть изменения в конфигурации от них не составит труда. Таким образом, убедившись с помощью спецпроверок, что оборудование само по себе не содержит вредоносных элементов, ответственность за его излучающие характеристики ложится исключительно на драйвер (или несколько драйверов в зависимости от сложности оборудования и принципов его взаимодействия с системой). Чтобы быть уверенным, что драйвер как программное обеспечение не содержит в себе закладок и прочих вредоносных элементов, необходимо провести его тестирование и анализ. Тестирование должно проходить с полнейшим покрытием кода драйвера. Каждая ветка программы должна получить управление как минимум раз за время тестового прогона. При этом необходимо осуществить совместную работу как автоматического теста, так и оборудования, фиксирующего данные по излучению. Такая методика могла бы для каждого устройства задавать предел возможных максимальных и минимальных уровней излучения. Используя программы тестирования и выработав ряд параметров, по которым можно было бы фиксировать отклонения от целевого назначения драйвера, можно находить критичные участки кода и заранее спланированные закладки внутри драйвера. К сожалению, точно определить назначение того или иного модуля драйвера никто, кроме его разработчика, не сможет.

В этой связи можно обратиться к современным наработкам специалистов в области разработки качественного программного обеспечения и их методам и

правилам ведения тестирования программных продуктов. И, исходя из них, выработать необходимый метод для драйверов при тестировании именно с точки зрения информационной безопасности.

Что же «предлагают» нам QA-инженеры (quality assurance) для решения поставленной задачи? Во-первых, специалисты тестирования программного обеспечения делят методы тестирования на «black box» (далее bb) тестирование (т.е. тестирование «черного ящика») и «white box» (далее wb) тестирование (т.е. тестирование «белого ящика»). Где-то между ними существует среднее «gray box» тестирование (т.е тестирование «серого ящика»). Bb-тестирование имеет сугубо функциональную направленность. То есть тестировщик не владеет исходным кодом программы, и все манипуляции с ней производятся исходя из логики работы программы и на основе документации к ней. Этот метод тестирования вполне автоматизируется. При Wb-тестировании у тестировщика под рукой есть исходный код программы, и вся работа проходит именно с ними. При gb-тестировании тестировщик работает как с исходным кодом программы, так и с уже готовым приложением. Это наиболее всеобъемлющий процесс тестирования, а значит, и наиболее эффективный.

Наиболее сложным и наиболее актуальным является способ bb-тестирования. Это обусловлено тем, что в большинстве случаев специалисту, заинтересованному в безопасности используемого программного обеспечения, приходится работать с продуктами, функциональная безопасность которых не может быть гарантированна производителем. Огромное количество драйверов так и остаются «черными ящиками» для пользователей. Именно поэтому стопроцентно предсказать технические и в том числе и частотные характеристики аппаратуры невозможно. Bb-тестирование может решит эту проблему. Самая подходящая стратегия тестирования при этом – так называемое «дымящееся тестирование» (smoke tests). Суть данного способа заключается в передаче функциям программы предельно возможных объемов данных или задании предельно допустимых режимов ее работы и фиксировании ее поведения при этом. Эта стратегия дает возможность специалисту, тестирующему драйвер, задать рамки, в которых может работать заданное устройство. Введя в данную систему анализатор спектра, фиксировать можно будет не поведение самого драйвера, а изменение излучающих характеристик оборудования.

На сегодняшний день на рынке очень мало программных продуктов, позволяющих реализовать это на практике. Наиболее развито тестирование драйверов именно по методикам wb-тестов. Это, конечно, оправданно именно с точки зрения QA-инженеров. Однако стоит взглянуть на сегодняшнее положение вещей и с точки зрения безопасности. Возможно, именно сейчас методика тестирования драйверов и аппаратуры на безопасность внутренней функциональности может стать как никогда востребованной.