Р. Г. Коркикян

ПРИМЕНЕНИЕ ЛАЗЕРА ДЛЯ СОЗДАНИЯ СБОЕВ В РАБОТЕ МИКРОКОНТРОЛЛЕРА

Одним из способов создания вычислительных ошибок, необходимых для атак методом индуцированных сбоев [1], является лазер с инфракрасным спектром излучения [2]. Текущие технологические процессы позволяют создавать ячейки памяти типа SRAM, ширина и высота которых меньше 1 мкм [3], поэтому изменение нескольких байт памяти возможно только при воздействии лазером на очень небольшую поверхность, не сравнимую с площадью поверхности всего чипа. Облучение большого числа ячеек памяти приведет к хаотической ошибке, бесполезной с точки зрения практического анализа. Помимо ограничений на размер пучка лазера, использование защитных технологий и увеличение объема памяти также уменьшают зону, воздействие на которую ведет к ошибке, не распознаваемой защитным механизмом системы. Данная статья описывает алгоритм работы лазерной установки, позволяющий автоматизировать локализацию уязвимой зоны микроконтроллера. Все опыты проводились в лаборатории CMP Charpak французского университета Ecole des Mines.

Эта исследовательская лаборатория имеет следующее оборудование: лазер, передвижная платформа, на которой устанавливается исследуемый образец, синхронизирующая плата, позволяющая контролировать время выстрела лазера, две камеры, система охлаждения и персональный компьютер (см. рисунок 1). Платформа может перемещаться по двум осям X и Y. Минимальный шаг составляет 1 мкм. Время, в течение которого лазер воздействует на поверхность чипа, составляет 5 нс. Ширина лазерного пучка задается с помощью микроскопа, а его энергия и другие параметры контролируются с помощью специального терминала.

Передвижная платформа с зафиксированным на ней чипом, сам микроконтроллер и синхронизирующая плата подсоединены к компьютеру. Программный интерфейс позволяет выбрать начальное и конечное положение платформы и задать шаг перемещения по двум осям, также он позволяет установить начальное и конечное время запаздывания, с которым создается сигнал от синхронизирующей платы после получения сигнала от микроконтроллера. Алгоритм, который использовался во время эксперимента, представлен ниже:

1. Лазер заряжен, микроконтроллер ожидает команды для начала вычислений.
2. Компьютер посылает сигнал на микроконтроллер.
3. Микроконтроллер начинает выполнение алгоритма, и в определенный момент на одном из его выходов генерируется сигнал, передаваемый на синхронизирующую плату.
4. Синхронизирующая плата распознает сигнал от микроконтроллера и с заданным временем запаздывания создает сигнал для лазера.
5. Лазер получает сигнал от синхронизирующей платы и генерирует луч, после чего начинается процесс перезарядки.
6. Чип заканчивает вычисления и отправляет результат по COM-порту на компьютер.
7. Компьютер записывает текущее положение платформы, параметры лазера, время запаздывания и результат вычислений микроконтроллера. Затем он изменяет время запаздывания синхронизирующей платы или перемещает платформу.
8. Если платформа не достигла конечной точки, то алгоритм возвращается на шаг 1.

В начале эксперимента был использован расфокусированный лазерный луч с большой энергией, для того чтобы определить возможность нарушения работы микроконтроллера. Вся поверхность чипа была последовательно протестирована, при этом в каждой точке было сделано небольшое число выстрелов. Часть ошибок была распознана защитными механизмами, которые

перезагружали микроконтроллер, но некоторые ошибки приводили к неправильным вычислениям. Далее лазер фокусировался на поверхности, положение платформы фиксировалось в точке, где была получена хоть одна ошибка, а шаг времени запаздывания выбирался как можно меньшим. Если в этой точке удавалось получить несколько ошибок, то она полагалась уязвимой и уже в дальнейшем использовалась для атак на криптографические алгоритмы. Данный метод позволил обнаружить уязвимую зону, которая составляет всего 0,125 % от площади поверхности чипа.

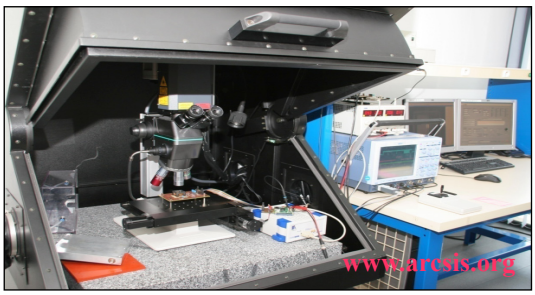

Рис. 1. Оборудование для эксперимента

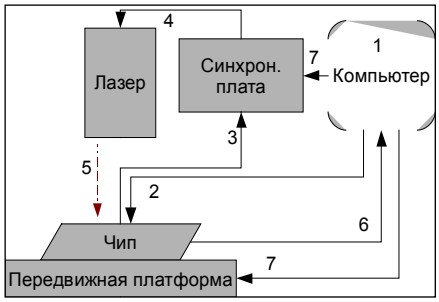

Рис. 2. Схема работы алгоритма

СПИСОК ЛИТЕРАТУРЫ:

1. *Киви Б.* Что показало вскрытие // Хакер. 2003. № 36. Р. 56–62.
2. *Skorobogatov S. P.* Semi-invansive attacks // Technical report. 2005.
3. *Agoyan M., Dutertre J.-M., Mirbaha A.-P., Naccache D., Ribotta A.-L., Tria A.* How to flip a bit? // IEEE 16th International On-Line Testing Symposium. 2010. P. 235–239.

И. Ю. Коркин

МЕТОД ВЫЯВЛЕНИЯ АППАРАТНОЙ ВИРТУАЛИЗАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ НА ОСНОВЕ МЕХАНИЗМА КЭШИРОВАНИЯ

Несанкционированное присутствие монитора виртуальных машин в системах представляет особую угрозу для безопасности в ситуациях, когда виртуализация сочетается с мерами по искажению показаний процессорного счетчика тактов. Поэтому разработка средств обнаружения монитора для таких ситуаций представляет актуальную задачу.