Автор:
01.03.18 20:19 -

Группа исследователей из университета штата Огайо разработала новый вариант атаки Spectre , позволяющий обойти средства изоляции кода и данных, предоставляемые технологией Intel SGX (Software Guard Extensions). Новый вид атаки получил название SgxPectre . Предложенный в обновлении микрокода Intel метод защиты на основе инструкции IBRS блокирует SgxPectre, но программная защита Reptoline, по мнению исследователей, не эффективна против атаки на SGX.

Технология SGX появилась в процессорах Intel Core шестого поколения (Skylake) и предлагает серию инструкций, позволяющих выделять приложениям пользовательского уровня закрытые области памяти - анклавы, содержимое которых не может быть прочитано и изменено даже ядром и кодом, выполняемым в режимах ring0, SMM и VMM. Передать управление коду в анклаве невозможно традиционными функциями перехода и манипуляциями с регистрами и стеком - для передачи управления в анклав применяется специально созданная новая инструкция, выполняющая проверку полномочий. При этом помещённый в анклав код может применять классические методы вызова для обращения к функциям внутри анклава и специальную инструкцию для вызова внешних функций. Для защиты от аппаратных атак, таких как подключение к модулю DRAM, применяется шифрование памяти анклава.

Концептуальная возможность применения уязвимости в механизме спекулятивного выполнения косвенных переходов для получения содержимого анклавов SGX была показана ещё в середине января. Разработчикам SgxPectre удалось довести метод до практической реализации, пригодной для проведения реальных атак. Метод может применяться для атаки на произвольные приложения для анклавов, написанные с использованием Intel SGX SDK, Rust-SGX или Graphene-SGX, и позволяет не только извлечь секретное содержимое памяти анклава, но и определить содержимое регистров, используемых только в режиме анклава.

Метод базируется на том, что на выполнение предсказания переходов для кода, выполняемого внутри анклава, могут влиять программы, выполняемые вне анклава - состояние блока предсказания переходов не сбрасывается перед входом в режим анклава и код вне анклава может манипулировать целями предсказания переходов внутри анклава. Соответственно порядок выполнения (control flow) программы в анклаве

может быть временно изменён для спекулятивного выполнения инструкций, выполнение которых не будет учтено, но повлияет на состояние кэша.

Манипулируя состоянием гонки (race condition) между спекулятивно выполненными обращениями к памяти и задержкой в процессе определения актуальной ветви исполнения, можно добиться оседания в кэше содержимого памяти анклава и внутренних регистров. Для оценки изменений в кэше далее могут применяться обычные механизмы восстановления через атаку по сторонним каналам вида "flush-reload".

Read more http://www.opennet.ru/opennews/art.shtml?num=48173