электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 519.686

Современные типы атак на BIOS

Иванников П.В., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Алтухов Н.О., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Алёшин В.А., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
v.aleshin@bmstu.net

Список используемых терминов и сокращений:
—BIOS – basic input/output system – базовая система ввода/вывода;
—EFI – extensible firmware interface – расширяемый интерфейс прошивки;
—ПО – программное обеспечение;
—FLASH – энергонезависимая электрически стираемая память;
—SPI – Serial Peripheral Interface – последовательный периферийный интерфейс;
—MBR – master boot record – главный загрузочный сектор;
—SMM – System Management Mode – режим системного управления;
—SMI – system management interrupt handlers – обработчик системных прерываний;
—API – application programming interface – интерфейс прикладного программирования;
—ЭВМ – электронно-вычислительная машина;
—ISA – Industry Standard Architecture
—LPC – Low Pin Count.

Введение

В настоящее время в мире ПК в основном используются две системы API-интерфейсов для взаимодействия ОС с аппаратным обеспечением ЭВМ – Legacy BIOS и EFI. Каждый из них имеет характерные особенности, и, как следствие, уязвимости, позволяющие злоумышленникам подменять содержащиеся в энергонезависимой памяти образы ПО [1].

С момента появления BIOS для взаимодействия между устройствами, микросхемами и микропроцессорами использовались различные интерфейсы: ISA, LPC, SPI. В настоящее время в основном используется интерфейс SPI [2].

В данной статье рассмотрены основные векторы атаки на базовую подсистему. Статья основана на презентации Юрия Булыгина [и др.] и других материалах с конференций по компьютерной безопасности и статьях в журналах по КБ.

Принцип работы Legacy BIOS

Основные этапы загрузки ПК с момента включения (перезагрузки) до передачи управления ОС можно выделить следующим образом [1]:

—Обращение к так называемому начальному адресу в ROM памяти BIOS, который хранит начальные инструкции;

—Инициализация ЦП и чипсета;

—Инициализация кэша процессора в качестве RAM, загрузка и исполнение команд в кэше;

—Инициализация основной памяти, её адресация;

—Составление списка устройств, подсоединенных по шине PCI;

—При необходимости чтение «драйверов» с внешних устройств (например, видеокарты), для их корректного взаимодействия с BIOS системы;

—Чтение MBR записи и её исполнение;

—Загрузка ядра ОС.

UEFI

Теперь взглянем как работает система EFI (в дальнейшем будем ее называть UEFI, в связи с тем, что Intel отказалась от собственной реализации EFI и перешла к стандартизированной подсистеме) (рис. 1).

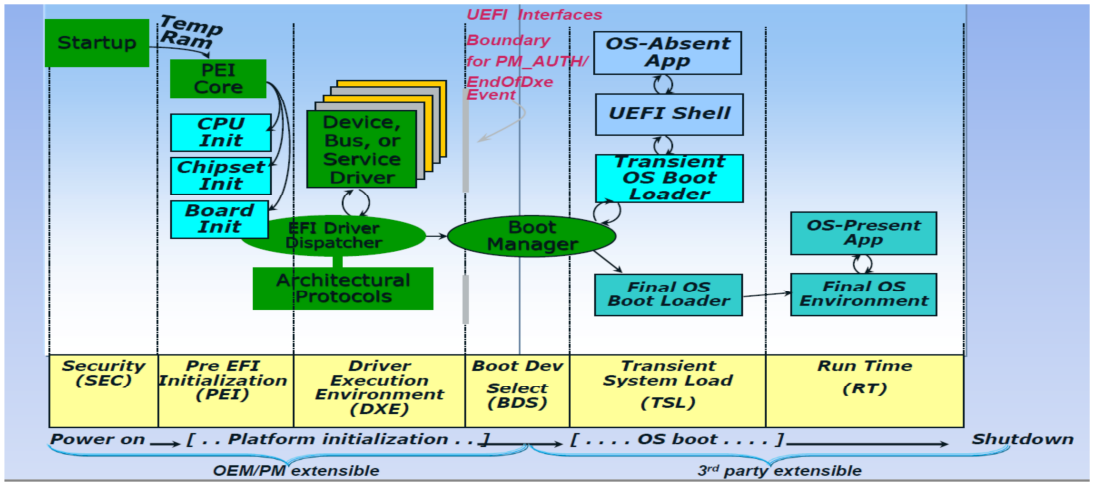

Рис 1. Временная шкала загрузки ПК под управлением UEFI. Схема взята из презентации Винсента Циммера

Давайте рассмотрим немного подробнее временную «ленту» работы UEFI:

—Запуск системы;

—Предварительная инициализация UEFI:

—Загрузка временной памяти «в ядро» инициализации;

—инициализация ЦП, чипсета;

—Работа среды выполнения драйверов – получение драйверов от оборудования, шин и т.д., их распаковка и загрузка в ядро UEFI; стоит помнить, что драйвер распаковщика хранится в развёрнутом виде, и представляет из себя бинарный файл, непосредственно исполняемый UEFI;

—Загрузчик – выбирает загрузочное устройство;

—Промежуточная загрузка системы:

—выполнение ОС-независимых приложений в оболочке UEFI (если таковая имеется), начало загрузки ОС;

—Вызов загрузчика ОС;

—Передача управления ОС.

Теперь мы практически полностью готовы приступить к атаке на BIOS, осталось рассмотреть, как выполняется обновление прошивки BIOS и безопасная загрузка ОС, так активно внедряемая консорциумом во главе с Майкрософт и которой так противятся разработчики (рис. 2).

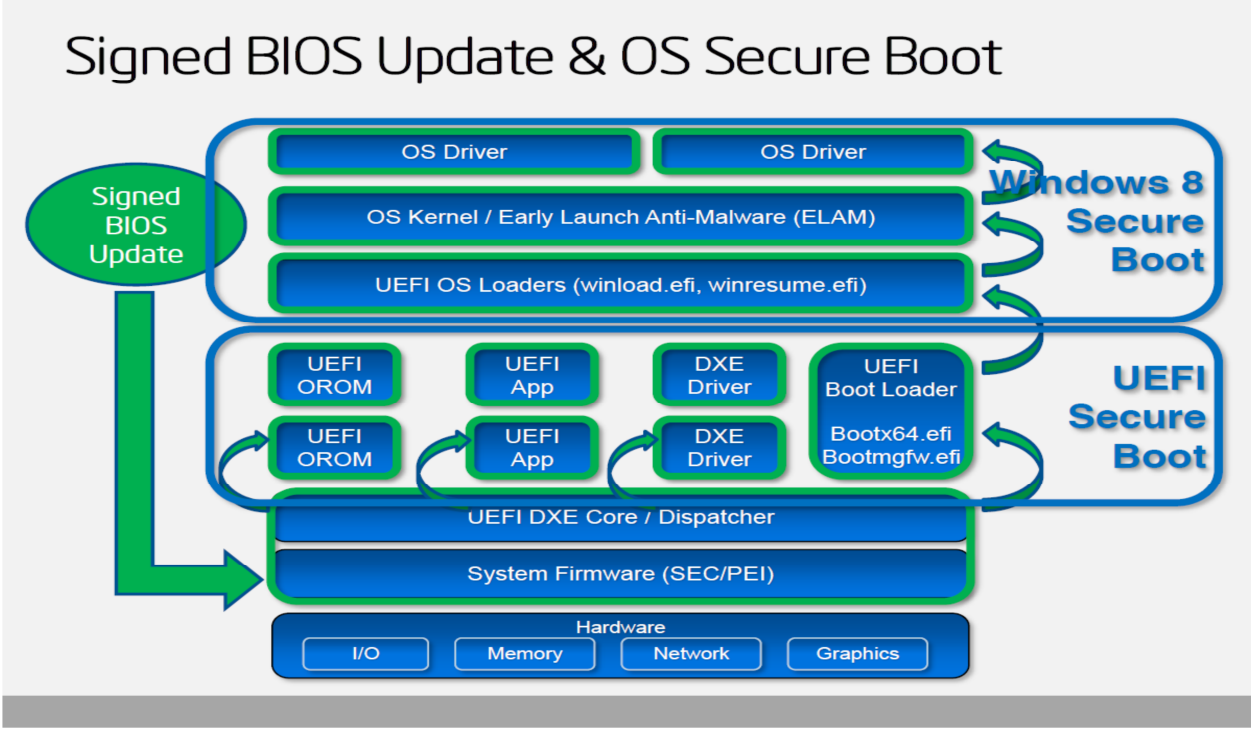

Рис 2. Принципиальная схема механизма Secure Boot

Приступим непосредственно к обзору существующих уязвимостей в обеих системах защиты [1].

Атаки на BIOS

SPI Flash

Защита флэш-памяти BIOS от записи является важной и необходимой мерой обеспечения безопасности настольных систем [1, 5]. К сожалению, многие производители не уделяют этому должного внимания, из-за чего открывают злоумышленникам пути к изменению образов управляющих подсистем. Основных моментов несколько:

—Как ни банально, но зачастую системы защиты, предусмотренные производителями микросхем, просто не включены;

—Не используется защита, основанная на SMM;

—При использовании безопасных диапазонов SPI не обеспечивается полная защита Flash BIOS;

—Часть платформ запускают защиту предрайверов только при их загрузке, что также открывает дополнительные уязвимости.

Возможные варианты атак (так называемые атаки «подавлением»):

—Некоторые системы защищаются от перезаписи путем выставления в 0 регистра записи-чтения (BIOSWE) и установкой блокировки на этот регистр, однако не используют SMM защиту (то есть мы при генерации прерывания SPI мы можем перейти в привилегированный режим);

—Это самое событие генерируется при изменении ключа BIOSWE в 1. Таким образом, одной из возможных атак является блокирование этих сигналов. Например, мы можем отключить SMI, если это разрешено конфигурацией оборудования.

Для предотвращения атак подобного рода необходимо заблокировать конфигурацию SPI Flash выставлением особого бита.

SMI Handlers

Один из возможных векторов атаки лежит прямиком через уязвимость повышения привилегий в SMM (SMM privilege escalation) [5]. Эти язвимости позволяют злоумышленнику получить доступ к физической памяти и портам ввода-вывода для выполнения произвольного кода, например, руткита в SMM-памяти с использованием SMM-привелегий [1].

Как это достигается: прошивка BIOS содержит специальный код в многочисленных хэндлерах SMI (handlers), которые работают в SMM режиме и загружаются при запуске системы (boot time) в защищенной части RAM (SMRAM) [1]. Однако некоторые хэндлеры «транслируются» в незащищенные участки. Поэтому любой процесс с правами, достаточными для доступа к физ. памяти, может заменить содержимое данной области памяти собственным кодом (см. повышение привилегий).

Обновление BIOS

К сожалению, проверка подписи при обновлении BIOS всё еще редкость, в связи с чем возникает следующий вектор атаки (успешно реализованный в MEBROMI):

—Изменение бинарного образа BIOS ROM инжектированием в него вредоносного ISA Option ROM при помощи официальной утилиты прошивки (создания) BIOS образа;

—Стирание SPI Flash для прошивки нового образа BIOS (при помощи выставления триггеров SPI);

Существующие проблемы в обновлении UEFI BIOS [1, 3]:

—В образе BIOS существуют неподписанные секции (такие как лого); отображение лого происходит до включения защиты SPI Flash; Intel BIOS разрешает менять стартовое лого при помощи своих утилит; если задать размер изображения достаточно большим, то произойдет переполнение в область PF handler, в результате чего мы можем установить точку входа внутри BMP файла, хранящего изображение, тем самым открывается возможность перезаписи BIOS Flash.

Проблемы в настройке и защите аппаратного обеспечения

SMRAM

SMM режим имеет выделенную память, называемую SMRAM. Доступ к ней определяется двумя битами, D_LCK и D_OPEN. D_OPEN отвечает за возможность доступа к этой памяти, и если он выставлен в 0, то все обращения переадресуются в видео-память. Бит D_LCK отвечает за возможность выставления бита D_OPEN, и в большинстве систем этот доступ заблокирован, и сменить его можно только при загрузке. Однако, имея возможности администратора можно выставить этот бит через видео-память, что открывает возможность атаки в не SMM режиме.

Атака «внедрением в кэш»

На платформах Intel существует уязвимость, позволяющая сделать SMRAM кэшируемой (что недопустимо с точки зрения безопасности и все попытки записать что-

либо в эту область должны быть отменены контроллером памяти). Атакующий вызывает SMI прерывание, которое переключает ЦП в режим SMM. SMM пытается обратиться к SMRAM, но так как мы пометили её кэшируемой, то перед тем, как обратиться к DRAM, происходит обращение к кэшу, в котором лежит вредонос, исполняемый в SMM режиме.

«Переадресация»

В некоторых чипсетах Intel существует уязвимость, позволяющая переадресовать память в защищенное пространство, тем самым позволяя злоумышленникам получить доступ к SMRAM без SMM режима и свободно работать с ней, будто с оперативной памятью.

UEFI Secure Boot

На рассмотрении уязвимостей, основанных на недостатках технологии Secure Boot, стоит остановиться подробнее, так как эта технология наиболее современна и, следовательно, вектор атак в ближайшем будущем будет направлен именно на нее (рис. 3).

Иерархия ключей в Secure Boot

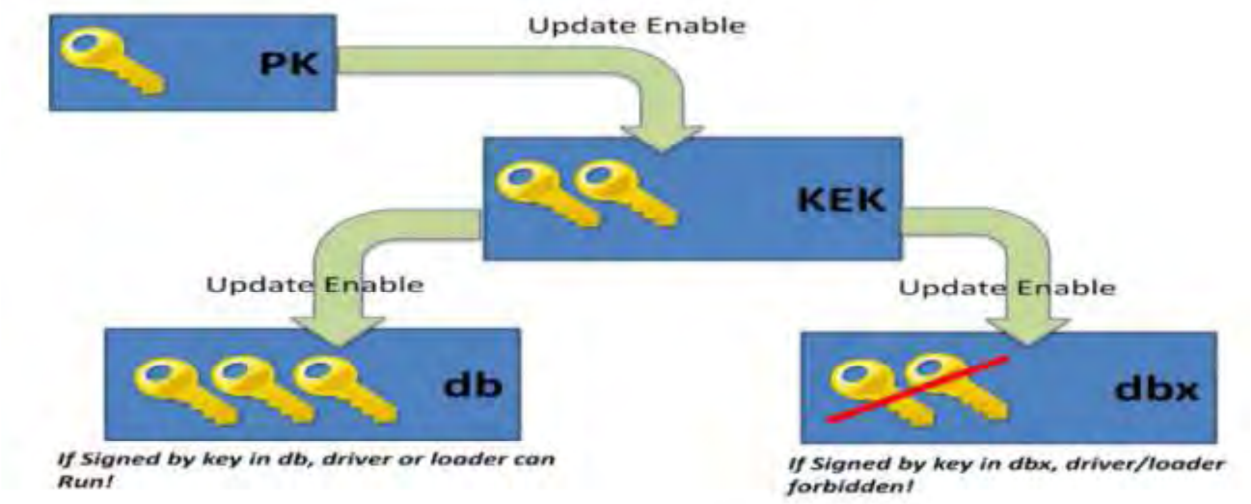

Рис. 3. Иерархия ключей Secure Boot

—Platform Key (PK): верифицирует ключи KEK; подтверждает изготовителя платформы;

—Key Exchange Keys (KEKs): подтверждает ключи DB и DBX; подтверждает подписи образов (в разработке).

Возможные атаки против Secure Boot (и активно использующиеся «энтузиастами»):

—Изменение PK ключа (платформо-зависимая операция);

—Отключение Secure Boot изменением системной переменной (SPI Flash);

—Отключение политик безопасности драйверов.

Выводы

1) Несмотря на постоянный прогресс в области защиты BIOS и появлении новых технологий, существует достаточное количество уязвимостей, способных нанести вред компьютерам [1, 3, 4, 5];

2) Для реализации 90% атак нападающему необходимо либо иметь физический доступ к компьютеру, либо уязвимость в операционной системе, управляющей им [2].

Список литературы

1. Bulygin Y., Loucaides J., Furtak A., Bazhaniuk O., Matrosov A. Summary of Attacks Against BIOS and Secure Boot. Available at: https://vk.com/doc18561130_367121401?hash=29c151c24a2cb3932e&dl=3614ed2e37cc8b05ba, accesed 14.03.2015.
2. Хакер. Режим доступа: https://xakep.ru/2009/01/15/46783/ (дата обращения: 15.03.2015).
3. Zimmer V. Secure boot, network boot, verified boot, oh my. Available at: https://docs.google.com/file/d/0BxgB4JDywk3MdnRsbnh6NW9rYU0/edit?pli=1, accessed 15.03.2015.
4. Wojtczuk R., Tereshkin A. Attacking Intel BIOS. Available at https://www.blackhat.com/presentations/bh-usa-09/WOJTCZUK/BHUSA09-Wojtczuk-AtkIntelBios-SLIDES.pdf, accesed 15.03.2015.
5. System Management Mode Hack SMM for «Other Purposes». Available at: http://phrack.org/issues/65/7.html, accessed 15.03.2015.