УДК 004.056.53

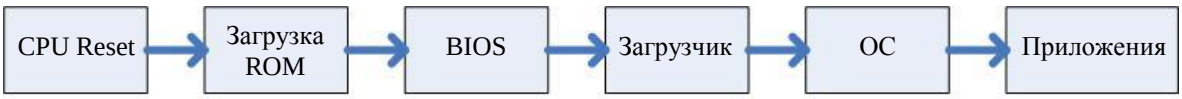
О средствах доверенной загрузки для аппаратных платформ с UEFI BIOS

С. С. Лыдин
Закрытое акционерное общество "ОКБ САПР", Москва, Россия

Рассмотрено системное программное обеспечение нового поколения UEFI BIOS. Помимо функций, призванных повысить удобство эксплуатации компьютерных платформ, UEFI привносит ряд проблем безопасности, обусловленных архитектурными отличиями от "традиционного" BIOS. Проведен краткий анализ возможных угроз информационной безопасности архитектуры UEFI BIOS. Определен круг проблем, которые должны быть разрешены до начала использования этой архитектуры без ограничений.

Ключевые слова: UEFI, BIOS, средства доверенной загрузки, профиль защиты.

Процесс загрузки компьютера и состав компонентов, задействованных в этом процессе, определяются архитектурой системы. На высоком уровне абстракции применительно к большинству компьютеров загрузку можно представить в виде совокупности этапов, показанных на рисунке.



Последовательность загрузки компьютера на высоком уровне абстракции

Из числа представленных на рисунке элементов последовательности основное внимание в данной статье уделяется базовой системе ввода-вывода (basic input/output system, BIOS). Система BIOS представляет собой первую микропрограмму, которая исполняется после включения питания компьютера и хранится в энергонезависимой памяти, как правило микросхеме флеш-памяти на материнской плате компьютера. Основное назначение BIOS состоит в:

- обеспечении инициализации и тестирования на низком уровне аппаратных компонентов компьютера, включая центральный процессор, динамическую оперативную память и т. д.;
- передаче управления загрузчику операционной системы (ОС).

Системы BIOS могут разрабатываться как производителями комплектного оборудования (*original equipment manufacturer*, *OEM*), так и независимыми разработчиками, а поставляются они конечным пользователям производителями материнских плат и компьютеров. Необходимо добавить, что производители часто, в том числе перед поставкой, обновляют системное программное обеспечение для того, чтобы исправить ошибки, поддержать новое аппаратное обеспечение и блокировать уязвимости.

Блокирование уязвимостей BIOS составляет актуальную задачу, поскольку очевидно, что для потенциального нарушителя всегда предпочтительнее скомпрометировать тот компонент, который загружается раньше прочих: получение контроля на более раннем этапе позволяет распространить влияние и на последующие элементы, такие, как код режима управления системой (*System Management Mode*, *SMM*), загрузчик, гипервизор, ОС. Если успешные атаки на программы, исполняемые в пользовательском режиме, при современном положении вещей позволяют нарушителю добиться преимуществ хотя и очень существенных, но все-таки ограниченных областью действия атакованной программы, то вредоносный код, записанный в BIOS, может позволить получить полный контроль над системой. Положение усугубляется тем, что поскольку системный BIOS запускается с высоким уровнем привилегий на ранней стадии загрузки системы, вредоносный код, исполняемый на уровне BIOS, очень трудно обнаружить; кроме того, он может использоваться для повторного "инфицирования" системы даже после того, как была произведена переустановка ОС или даже замена жесткого диска компьютера. В этих условиях, очевидно, *BIOS и загрузчик*

Лыдин Сергей Сергеевич, начальник научно-исследовательского отдела.
E-mail: ssl@okbsapr.ru

Статья поступила в редакцию 26 июня 2016 г.

должны восприниматься нарушителем как более привлекательные объекты атаки. Действительно, в прошлые годы было опубликовано довольно большое количество сообщений о моделях возможных атак именно на эти цели. Нецелесообразно останавливаться на них подробно, достаточно упомянуть только о двух типовых примерах [1]:

- атаки на BIOS, заключающиеся в подмене исходного кода BIOS вредоносным кодом BIOS, внедренным нарушителем;
- атаки на загрузчик, заключающиеся в установке подконтрольного нарушителю так называемого буткита (*bootkit* — разновидность "руткита" (*rootkit*), который исполняется в режиме ядра), "инфицирующего" загрузчик. При этом "буткит" может использоваться для организации утечки чувствительной информации, обрабатываемой в процессе загрузки, такой, как пароли шифрования информации на жестком диске.

Подводя краткий промежуточный итог, можно констатировать, что *подмена микропрограммы BIOS вредоносным программным обеспечением в общем случае представляет опасную угрозу*, которая может быть частью сложной атаки на информационную систему организации, направленной на достижение длительного отказа в обслуживании (если BIOS в результате атаки подвергается разрушению) или обеспечение долгосрочного функционирования вредоносного кода в составе системы (если в результате атаки производится "инфицирование" BIOS) [2].

Однако относительно практической стороны вопроса следует отметить, что атаки на так называемый традиционный BIOS (*Legacy BIOS*), который до сих пор выступал в качестве предмета рассмотрения, как правило, связаны с низким уровнем мотивации нарушителя к их реализации в силу слабого уровня стандартизации "традиционного" BIOS. Попытка разработать и внедрить вредоносный код, который мог бы использовать одновременно уязвимости, например, систем HP, Dell и IBM, обычно рассматривается нарушителем как неэффективная, потому что эти системы работают по-разному и реализовать универсальный механизм атаки весьма затруднительно. Иными словами, "эксплойты" для "традиционных" BIOS отличаются высоким уровнем зависимости от системы (как от версии BIOS, так и от частного случая реализации аппаратных компонентов, таких, как чипсет материнской платы). Подавляющая часть существующего вредоносного кода исполняется на уровне ядра ОС и более высоких уровнях, чтобы существовала возможность использовать его на максимально широком подмножестве систем. В силу указанного обстоятельства *известны лишь немногие практические реализации атак на уровне "традиционного" BIOS*. В качестве характерного примера можно привести лишь вирус "Чернобыль", обнаруженный в 1998 г. Для современных компьютеров этот вирус неактуален, поскольку они не содержат уязвимостей, которые им использовались [2].

Между тем интенсивно осуществляемый переход от реализации "традиционного" BIOS к реализации, основанной на едином расширяемом микропрограммном интерфейсе (*Unified Extensible Firmware Interface* (UEFI)), наряду с получением ряда функциональных преимуществ, в контексте обеспечения информационной безопасности характеризуется снижением для нарушителя сложности задачи внедрения вредоносного кода на уровне BIOS. Прежде чем привести подтверждения этому тезису, необходимо кратко ознакомиться с назначением и основными особенностями UEFI.

Интерфейс UEFI — это современный интерфейс между ОС и микропрограммами, управляющими низкоуровневыми функциями оборудования. Если последовательно придерживаться прежнего достаточно высокого уровня абстракции, процесс загрузки компьютера, использующего UEFI, формально представляется таким же, как и в случае с "традиционным" BIOS. Разница заключается в том, что код UEFI запускается, как правило, в современном 64-битном защищенном режиме работы процессора, тогда как код микропрограммы BIOS исполняется в 16-битном реальном режиме работы процессора. Однако в отличие от фактически неизменной по своему функциональному содержимому микропрограммы BIOS, система UEFI представляет собой программируемый интерфейс с довольно широким набором возможностей, совокупность которых придает ему черты самостоятельной операционной системы, пусть и облегченной. Основанием для подобной характеристики является то, что спецификация UEFI определяет, в частности, следующие элементы:

– *сервисы*. В UEFI допускается два типа сервисов: загрузочные (*boot services*) и среды выполнения (*runtime services*). Первые функционируют только до загрузки ОС компьютера и обеспечивают взаимодействие с графическими и текстовыми терминалами, шинами и т. д., а сервисы среды выполнения доступны даже из ОС компьютера;

– *драйверы устройств*. В UEFI реализуется платформонезависимая среда драйверов *EFI Byte Code* (*EBC*). Взаимодействие ОС с драйверами устройств, как правило, осуществляется через EBC, что позволяет ОС компьютера использовать

UEFI для базовой поддержки графических и коммуникационных функций до загрузки драйверов, установленных в ОС. Некоторые архитектурно-зависимые (*non-EBC*) драйверы имеют интерфейсы для использования ОС напрямую;

– *приложения*. Независимо от загружаемой ОС программа UEFI поддерживает возможность запуска отдельных приложений, которые могут разрабатываться и устанавливаться по усмотрению производителей компьютеров. К числу таких приложений относится, например, оболочка UEFI (*UEFI shell*). Оболочка может быть загружена еще до запуска ОС компьютера и использоваться для выполнения различных приложений: утилит по установке и настройке операционных систем, файловых менеджеров, утилит для просмотра файлов и т. д. Команды оболочки также позволяют копировать или перемещать файлы и каталоги в поддерживаемых файловых системах, загружать и выгружать драйверы. Оболочка поддерживает командную строку и командные файлы, аналогичные командам и пакетным файлам DOS.

Кроме того, спецификация UEFI определяет возможность *загрузки компьютера по сети* с помощью протокола удаленной загрузки (*preboot execution Environment, PXE*) и доступа к загрузочным образам, хранящимся в сетях хранения данных (s*torage area network, SAN*).

Даже приведенного (далеко не полного) перечня функциональных возможностей UEFI BIOS достаточно для того, чтобы с очевидностью показать, что *до загрузки ОС в компьютере, фактически, производится загрузка отдельной многофункциональной системы*.

Ранее было показано насколько важным для обеспечения информационной безопасности системы является сохранение целостности BIOS и компонентов, загружаемых после BIOS. Если рассматривать проблему безопасности информации несколько шире, следует постулировать, что важно обеспечить доверенную загрузку ОС, в рамках которой, помимо сохранения целостности ОС, выполняются, как правило, процедуры контроля устройств, с которых загружается ОС, а также процедуры идентификации и аутентификации пользователя.

В сложившейся практике перечисленные функции реализуются средствами доверенной загрузки (СДЗ), под которыми понимаются программно-технические средства, реализующие функции по предотвращению несанкционированного доступа к программным и (или) техническим ресурсам компьютера на этапе его загрузки. СДЗ являются элементами подсистемы защиты информации от несанкционированного доступа и применяются на компьютерах совместно с другими средствами защиты информации.

На протяжении многих лет СДЗ разрабатывались и совершенствовались в условиях использования совместно с "традиционными" BIOS. Это обстоятельство определяло их архитектуру и принципы функционирования. В частности, при использовании "традиционного" BIOS обоснованной является реализация принципа, согласно которому СДЗ начинает свою работу после выполнения системного BIOS и далее обеспечивает выполнение заданного набора требований доверия безопасности; при этом принимается, что код самого BIOS механизмами СДЗ проверять не нужно, поскольку, как было показано выше, атаки, связанные с подменой "традиционного" BIOS, на практике, по сути, не реализуются. Но в случае, если угроза подмены системного BIOS при использовании в информационной системе некоей организации все же признается актуальной, следует в установленном порядке проверить микропрограмму на наличие уязвимостей, позволяющих осуществить такую подмену. Данная проверка практически реализуема, поскольку общая архитектура и принципы функционирования "традиционного" BIOS хорошо известны, объем микропрограммного кода и набор функций весьма ограничены, а на выработку подходов к проведению различных исследований в распоряжении сообщества специалистов имелся не один десяток лет.

Ситуация выглядит совершенно иначе в случае использования UEFI BIOS.

Во-первых, все интерфейсы UEFI BIOS стандартизированы. Из этого следует, что в отличие от случая, когда используется "традиционный" BIOS, реализация атак на UEFI BIOS не состоит в сильной зависимости от архитектуры системы и один и тот же "эксплойт" может использовать уязвимости на множестве компьютеров. В свою очередь, это означает, что сообщество больше не имеет права считать, что атаки на BIOS не реализуются на практике, что у нарушителя отсутствует для этого мотивация. Теоретические выводы подкрепляются и действительностью. Например, в [3] сообщается, что вследствие использования многими BIOS одного и того же кода обнаружены уязвимости, актуальные для 80 % исследованных компьютеров, включая модели Dell, Lenovo и HP; при этом уязвимости было настолько легко обнаружить, что удалось даже написать скрипт для автоматизации этого процесса, с помощью которого было выявлено множество уязвимостей. Далее, на конференции CanSecWest Vancouver 2015 исследователи из Legbacore продемонстрировали способ внед-

рения низкоуровневого троянского компонента LightEater [4]. Действуя на уровне UEFI, этот "буткит" остается невидимым для антивирусов. В проведенной демонстрации использовались материнские платы производства Acer, Asus, Gigabyte, Foxconn и MSI. В некоторых материнских платах удалось записать во флеш-память BIOS недопустимую инструкцию через модифицированный драйвер ядра, в результате чего успешную загрузку удалось выполнить только после физической замены чипа. В целом это напоминает новый виток развития вирусов типа "Чернобыль", но с гораздо более серьезными последствиями. Эти выводы подтверждаются и многими другими свидетельствами (см., например, [5—7]).

Во-вторых, UEFI BIOS имеет несоизмеримо более богатый набор функциональных возможностей (в качестве иллюстрации, дополнительной к тем многим, что уже были приведены ранее, можно отметить, например, что объем спецификации UEFI BIOS последней версии 2.6, составляет более 2500 страниц), состав которого может существенно отличаться в различных системах в зависимости от предпочтений производителя. Это означает, во-первых, что проверить UEFI BIOS теми же методами, что использовались при проверке "традиционного" BIOS, не удастся, а во-вторых, что усложнение и расширение его функциональности неизбежно влечет за собой увеличение "площади поверхности" для проведения разнообразных атак.

И наконец, наличие широкого набора функций прикладного значения и принципиальной возможности осуществления таких атак на UEFI BIOS, которые актуальны сразу для множества компьютеров, заставляет пересмотреть подход к процедурам обновления системного BIOS. Следует признать, что на практике в информационных системах организаций процедура обновления "традиционного" BIOS представляла собой весьма редкое явление или же вообще не производилась. Очевидно, что в случае с UEFI BIOS ее придется производить (локально и (или) через сеть) значительно чаще, что, в свою очередь, открывает новый класс уязвимостей для системного BIOS. В пользу значимости данной проблемы свидетельствует хотя бы то, что NIST выпустил специальные рекомендации по снижению вероятности угроз UEFI BIOS, бóльшая часть содержания которых посвящена обеспечению защиты именно процедур обновления [2].

Таким образом, можно констатировать, что принципы обеспечения доверенной загрузки систем с UEFI BIOS должны принципиально отличаться от тех, что на протяжении многих лет применялись для систем на основе "традиционного" BIOS. Эти различия, по-видимому, обусловливают необходимость выработки как нового подхода для установления требований безопасности, которым должно удовлетворять соответствующее СДЗ, так и нового подхода к формированию со стороны регуляторов заключения о соответствии продукта предъявленным к нему требованиям безопасности информации.

В качестве реакции на данный тезис может последовать возражение. В соответствии с информационным письмом ФСТЭК России от 06.02.2014 № 240/24/405 "Об утверждении Требований к средствам доверенной загрузки" с 1 января 2014 г. сертификация средств защиты информации, реализующих функции доверенной загрузки, в системе сертификации ФСТЭК России проводится на соответствие утвержденным Требованиям к средствам доверенной загрузки. И поскольку данные требования разрабатывались и утверждались в условиях, когда UEFI BIOS уже получил достаточно широкое распространение, от разработчика, возможно, не требуется ничего иного, как выполнить указанные требования, а от оценщика — в ходе сертификационных испытаний проверить соответствие СДЗ требованиям, изложенным в профилях защиты СДЗ.

Требования существуют, однако следует признать, что их недостаточно для решения описанной проблемы безопасности. Одно из основополагающих свойств любого профиля защиты заключается в том, что он предоставляет независящее от реализации описание требований безопасности, но не регламентирует, каким образом будут выполняться изложенные в нем требования. На самом высоком уровне абстракции процессы загрузки при использовании двух типов BIOS сходны, и, значит, попытка формирования независящих от реализации требований безопасности имеет право на существование. Однако дальше было показано, что при ближайшем рассмотрении имеющиеся между двумя типами BIOS различия носят настолько принципиальный характер, что принципы обеспечения доверенной загрузки систем с "традиционным" BIOS оказываются недействительными для систем с UEFI BIOS. Таким образом, именно разница в реализации становится очень значимым препятствием на пути выполнения требований, обнажая их недостаточность.

Можно привести множество примеров для подтверждения справедливости этого утверждения. Так, в профилях защиты СДЗ устанавливается, что СДЗ должно реализовывать функцию управления доступом к ресурсам компьютера в части обеспечения недоступности штатными средствами его

ресурсов в случае загрузки нештатной ОС. Данное условие представляется в целом совершенно справедливым, но с учетом того, что UEFI BIOS, как было показано, как раз является штатным средством и реализует многие функции, свойственные операционной системе, включая функции доступа к ресурсам компьютера *еще прежде, чем производится загрузка* как штатной, так и нештатной ОС, нужно признать, что выполнения указанного в профилях защиты условия недостаточно для достижения соответствующих целей безопасности.

Кроме того, профили защиты СДЗ основываются на предположении о том, что среда функционирования СДЗ должна обеспечивать невозможность отключения (обхода) компонентов СДЗ. Фактически это означает, что та или иная организация должна каким-то образом сделать так, чтобы с помощью механизмов UEFI BIOS используемых в ней компьютеров нельзя было отключить компоненты СДЗ. Ответ на вопрос о том, каким образом это можно обеспечить в условиях, когда UEFI BIOS, в сущности, представляет собой обновляемую операционную систему с переменным составом элементов и большим числом функциональных возможностей, не очевиден, хотя попытки его отыскать предпринимаются [8]. Открытыми остаются и другие вопросы, в частности о том, должно ли СДЗ каким-то образом обеспечивать безопасное обновление BIOS, и если нет, то какой компонент подсистемы информационной безопасности должен контролировать процедуру обновления; каким образом СДЗ должно расценивать попытку загрузки компьютера по сети и т. д.

Разумеется, все изложенное не означает, что проблема безопасности, связанная с использованием UEFI BIOS, не решаема в принципе. На все вопросы, конечно, существуют ответы, и могут быть разработаны как соответствующие технические решения, так и методы проверки соответствия этих решений требованиям безопасности информации. Но для этого требуется еще приложить существенные усилия со стороны сообщества специалистов по информационной безопасности, направленные в том числе, если не на разработку отдельных профилей защиты для систем с UEFI BIOS (хотя этот шаг выглядит логически обоснованным, поскольку среда функционирования СДЗ, содержащая в своем составе "традиционный" BIOS, принципиально отличается от среды функционирования СДЗ, содержащей UEFI BIOS, и, следовательно, состав даже высокоуровневых требований безопасности как к СДЗ, так и к его среде функционирования может быть различным), то, по крайней мере, на разработку методических материалов по реализации и оценке требований к таким системам на основе результатов накопления научно-технического опыта. В противном случае выполнение требований может превратиться в пустую формальность и привести к ситуации, когда будут разрабатываться СДЗ, которые полностью удовлетворяют положениям нормативных документов и используются при оснащении компьютеров в коммерческих и государственных организациях, а нейтрализация актуальных угроз и реализация целей информационной безопасности обеспечиваться не будут. При этом внешне ситуация может выглядеть абсолютно естественно, но существующие недостатки окажутся только отретушированными, а не искорененными.

Попытки решения описанной технической проблемы в частном случае, которые предпринимаются, выглядят оправданными, но при самом лучшем раскладе могут привести к достижению лишь локальных успехов. К числу таких попыток, по-видимому, следует отнести создание собственной UEFI BIOS с интегрированным сертифицированным СДЗ, которое предназначено для выполнения требований безопасности. В рамках подобных решений остаются нерешенными все те же вопросы обновления UEFI BIOS, нейтрализации угроз, реализуемых с помощью штатных средств UEFI BIOS, обеспечения защиты обширного уже эксплуатирующегося в организациях парка компьютеров, условия гарантийного обслуживания которых не предусматривают возможность замены одной из микросхем UEFI BIOS микросхемой стороннего производителя, и т. д.

Очевидно, что для разработки универсальных СДЗ, адекватных существующим проблемам безопасности, требуется время. При этом компьютеры на основе UEFI BIOS со всеми известными и еще не до конца осознанными уязвимостями используются уже сейчас. В существующих условиях представляется целесообразным временный отказ от использования компьютеров с UEFI BIOS, как минимум, в государственных информационных системах, в которых обрабатывается информация ограниченного доступа.

Литература

1 *Ruan X.* Platform Embedded Security Technology Revealed // Apress, 2014.

2 *Cooper D., Polk W., Regenscheid A., Souppaya M.* BIOS Protection Guidelines // NIST Special Publication. 2011. No. 800. P. 147.

3 *Zetter K.* Hacking BIOS Chips Isn't Just the NSA's Domain Anymore. URL: http://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems (дата обращения 19.04.2016).

4 *Kallenberg C., Kovah X.* LegbaCore. How many million BIOSes would you like to infect? URL: https://reverse.put.as/wp-content/uploads/2016/01/HowManyMillionBIOSesWouldYou LikeToInfect_Whitepaper_v1.pdf (дата обращения 19.04.2016).

5 *Mimoso M.* NEW BIOS IMPLANT, VULNERABILITY DISCOVERY TOOL TO DEBUT AT CANSECWEST. URL: https://threatpost.com/new-bios-implant-vulnerability-discovery-tool-to-debut-at-cansecwest/111710/ (дата обращения 19.04.2016).

6 *Pauli D.* Noobs can pwn world's most popular BIOSes in two minutes. URL: http://www.theregister.co.uk/2015/03/19/cansecwest_talk_bioses_hack/ (дата обращения 19.04.2016).

7 *Fox-Brewster T.* "Voodoo" Hackers: Stealing Secrets From Snowden's Favorite OS Is Easier Than You'd Think. URL: http://www.forbes.com/sites/thomasbrewster/2015/03/18/hacking-tails-with-rootkits/#6537d0596143 (дата обращения 19.04.2016).

8 *Алтухов А. А.* Неатомарный взгляд на РКБ как на композицию перехвата управления и контроля целостности. В: Комплексная защита информации. Мат. XX науч.-практ. конф. Минск, 19–21 мая 2015 г. — Минск: РИВШ, 2015. С. 53—55.

Modules of trusted boot for hardware platforms with UEFI BIOS

S. S. Lydin
Closed Joint Stock Company "OKB SAPR", Moscow, Russia

UEFI BIOS is the new generation firmware. Besides the convenient this new platform brings to us, it has completely different architecture with legacy BIOS, which leads some security concerns. This paper analyzes the possible security threats on UEFI BIOS architecture and defines the range of issues that must be resolved before the proper use of this architecture.

Keywords: UEFI, BIOS, modules of trusted boot, protection profile.

Bibliography — 8 references. *Received June 26, 2016*