Семинар Лыдина С. С. на InfoSecurity-2016

Проблемы доверенной загрузки систем с UEFI BIOS

Процесс загрузки компьютера и состав компонентов, задействованных в этом процессе, определяется архитектурой системы.

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 др.;
- передаче управления загрузчику ОС.

BIOS могут разрабатываться как производителями комплектного оборудования (original equipment manufacturer, OEM), так и независимыми разработчиками, а поставляются конечным пользователям – производителями материнских плат и компьютеров. Нужно 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, 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: 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 всё-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 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.

Однако что касается практической стороны вопроса, следует отметить, что атаки на так называемый «традиционный» BIOS (Legacy BIOS), 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.

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 году. Для современных компьютеров этот вирус неактуален, поскольку они не содержат уязвимостей, которые им использовались.

Интенсивно осуществляемый в настоящее время 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.

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:

- 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. 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

- 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)

Кроме того, спецификация UEFI определяет возможность загрузки компьютера по сети с помощью протокола удаленной загрузки и доступа к загрузочным образам, хранящимся в сетях хранения данных.

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

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, которые реализует функции по предотвращению несанкционированного доступа к программным и (или) техническим ресурсам компьютера на этапе его загрузки.

На протяжении многих лет и до настоящего времени 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 том 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 ограничен, 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:

- все интерфейсы UEFI BIOS стандартизированы. Из этого следует то, 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

- UEFI BIOS имеет несоизмеримо более богатый набор функциональных возможностей. Это означает, во-первых, что проверить UEFI BIOS теми же методами, что использовались при проверке «традиционного» BIOS, не удастся, а во-вторых, усложнение и расширение его функциональности неизбежно влечет за собою увеличение «площади поверхности» для проведения разнообразных атак

- наличие широкого набора функций прикладного значения и наличие 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, 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

Таким образом, 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 нового подхода как 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.

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 сейчас 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 отличаться), 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 при этом обеспечиваться не будет. При этом внешне ситуация может выглядеть абсолютно естественно, существующие недостатки окажутся только отретушированы, а не искоренены.

Попытки решения описанной технической проблемы в частном случае, которые предпринимаются в настоящее время, выглядят несколько более оправданными, но, разумеется, в самом лучшем случае могут привести к достижению лишь локальных успехов. К числу таких попыток, по-видимому, следует отнести создание собственного 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 микросхемы UEFI BIOS микросхемой стороннего производителя, и др.

Очевидно, 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, по меньшей мере, в государственных информационных системах, в которых обрабатывается информация ограниченного доступа, и, возможно, переход на использование новых защищенных архитектур.