УДК 004.056.52

УПРАВЛЕНИЕ ДОСТУПОМ ПУТЕМ БЛОКИРОВКИ ЗАГРУЗКИ MBR

Сироткин Е.А. [1], студент гр.153503 Плиска В.С. [2], магистрант гр.255741.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Рогов М.Г. – ассистент кафедры информатики

Аннотация. Данная статья рассматривает значимость защиты загрузочного сектора компьютера в контексте информационных технологий и компьютерной безопасности. Значительное внимание уделяется описанию применения современных методов управления доступом через блокировку загрузки, таких как UEFI Secure Boot и TPM, с целью обеспечения безопасности загрузочного процесса компьютерных систем. Упоминаются актуальные угрозы, которые присутствуют в контексте обеспечения безопасности MBR.

Ключевые слова. MBR, UEFI Secure Boot, TPM, компьютерная безопасность, загрузочный сектор, атаки на загрузку, защита от вредоносного ПО, UEFI, буткит, руткит, безопасная загрузка, цифровая подпись, аппаратное обеспечение, безопасный запуск.

В контексте информационных технологий и компьютерной безопасности, защита загрузочного сектора компьютера, включая мастер загрузочной записи (MBR), становится ключевым аспектом обеспечения целостности и безопасности системы. Загрузочный сектор является первым участком, который загружается при включении компьютера, и поэтому его целостность и безопасность критически важны. Ведь именно здесь начинается процесс загрузки операционной системы, и любые изменения или атаки на этот участок могут иметь серьезные последствия для функционирования всей системы.

MBR представляет собой критически важный компонент, отвечающий за инициализацию загрузки операционной системы на компьютере. Он содержит информацию о структуре диска и процессе загрузки операционной системы. Однако его уязвимость к модификациям представляет серьезную угрозу для безопасности системы. Несанкционированное изменение MBR может привести к блокировке загрузки операционной системы, внедрению вредоносного кода или даже полному отказу в доступе к данным.

Для злоумышленников модификация загрузочной записи представляет интерес, так как она обеспечивает незаметное внедрение в систему и сохранение доступа к ней на длительное время. Они могут использовать такие методы для выполнения кражи данных, шпионажа, установки вредоносного ПО или даже для проведения вымогательства.

В процессе загрузки компьютера вначале всегда отрабатывается BIOS. На этой стадии кроме тестирования и активации компонентов, происходит также и выбор устройства, с которого будет происходить дальнейшая загрузка. Это может быть дискета, жёсткий диск, сетевой ресурс, встроенное ПЗУ или любое иное устройство (алгоритм выбора загрузочного устройства может быть различным и зависит от реализации BIOS). После выбора загрузочного устройства, управление всей дальнейшей загрузкой BIOS полностью передаёт этому устройству. В случае, если устройство имеет только один раздел (как, например, дискета или сетевая загрузка), то выбор однозначен, и загрузка продолжается сразу с этого устройства. Однако, если устройство содержит несколько разделов, каждый из которых потенциально может быть загрузочным (как, например, в случае жестких дисков), то возникает неопределённость: с какого именно раздела производить загрузку. Для разрешения неоднозначности по выбору раздела было предложено вынести этот вопрос из ведения BIOS и передать этот выбор самому устройству. Возникла идея использовать для этого небольшую программу, записанную на самом носителе, которая и осуществляла бы данный выбор. Так появилась концепция MBR [1].

Главная загрузочная запись (MBR) – код и данные, необходимые для последующей загрузки операционной системы и расположенные в первых физических секторах (чаще всего в самом первом) на жёстком диске или другом устройстве хранения информации. MBR содержит небольшой фрагмент исполняемого кода, таблицу разделов диска (partition table) и специальную сигнатуру.

Последние два байта MBR называются сигнатурой. Значение этих байтов должно быть равно определенному значению. В случае, если это не так, запись считается некорректной [2].

Код, который находится в разделе MBR (Master Boot Record), является ключевой частью загрузочного процесса компьютера. Этот код, известный как загрузочный код (boot code), представляет собой небольшую программу, которая выполняется при включении компьютера и инициирует процесс загрузки операционной системы. Загрузочный код в MBR может быть реализован как на ассемблере, так и на языке высокого уровня, в зависимости от предпочтений разработчика и требований конкретной системы. Этот код выполняет несколько важных задач, начиная с поиска активного раздела на жестком диске. После определения активного раздела, он осуществляет чтение дополнительного загрузочного кода из его начального сектора, называемого загрузочным заголовком (Boot Record, BR). Этот дополнительный загрузочный код может содержать дополнительную логику или информацию, необходимую для успешной загрузки операционной системы. Далее, загрузочный код в MBR загружает

операционную систему в оперативную память компьютера, часто путем чтения необходимых секторов с диска и их загрузки в память. После того как операционная система загружена, загрузочный код передает управление ей, что запускает процесс загрузки операционной системы и начало работы компьютера. Этот код имеет критическое значение для корректной работы компьютера и определяет, как операционная система будет загружаться при каждом включении. Из-за своей важности, изменение или повреждение загрузочного кода в MBR может привести к неполадкам или недоступности системы.

Таблица разделов диска в MBR является ключевой частью хранения информации о разделах на жестком диске компьютера. Эта небольшая структура данных, размером в 64 байта, представляет собой неотъемлемый элемент загрузочного процесса и файловой системы операционной системы. Она содержит информацию о разделах, которые фрагментируют жесткий диск, делая его доступным для хранения и управления файлами и данными. Каждая запись в таблице разделов MBR содержит информацию о конкретном разделе, включая его начальный и конечный секторы, тип файловой системы (например, FAT32, NTFS и другие), а также флаги, определяющие активный раздел и другие характеристики. Эта информация необходима для операционной системы, чтобы правильно читать и записывать данные на диск, а также для загрузчика, чтобы определить, с какого раздела нужно загрузить операционную систему.

Пример структуры MBR, включающий в себя фрагмент исполняемого кода, таблицу разделов диска и сигнатуру показан на рисунке 1.

Рисунок 1 – Схематическое изображение структуры MBR

Загрузочная область MBR и загрузочный сектор являются ключевыми элементами не только для начала загрузки операционной системы, но и для обеспечения целостности и стабильности работы компьютера в целом. Эти небольшие, но критически важные компоненты содержат не только код, необходимый для запуска загрузочного процесса, но и информацию о структуре диска, включая таблицу разделов. Однако, именно из-за их ключевой роли MBR становится объектом пристального внимания злоумышленников. Атаки на него могут привести к серьезным последствиям, таким как блокировка работы операционной системы, уничтожение или утрата данных, а также предоставление злоумышленнику долгосрочного контроля над системой. Наиболее распространенными атаками, направленные на MBR, являются rootkit-атаки и bootkit-атаки.

Руткит – это набор компьютерных программ, как правило, вредоносных, предназначенных для обеспечения доступа к компьютеру или его программной части, который не разрешен иным способом (например, неавторизованному пользователю), и часто маскирующих свое существование или существование других программ. Термин rootkit представляет собой соединение слова root (традиционное название привилегированной учетной записи в Unix-подобных операционных системах) и слова kit (обозначающего программные компоненты, реализующие инструмент). Установка руткита может быть автоматической, либо злоумышленник может установить его, получив доступ root или администратора. Получение такого доступа является результатом прямой атаки на систему. После установки становится возможным скрыть вторжение, а также сохранить привилегированный доступ. Полный контроль над системой означает, что существующее программное обеспечение может быть изменено, в том числе и то, которое в противном случае могло бы быть использовано для обнаружения или обхода [3].

Буткит – это тип вредоносного ПО, используемый для заражения MBR или UEFI системы, которые отвечают за запуск/загрузку ОС путем конфигурирования аппаратных компонентов и запуска загрузчика. Поскольку Bootkit загружается/запускается до загрузки ОС, после заражения системы удалить его практически невозможно, разве что отформатировать все устройство хранения данных [9]. Буткиты часто путают с руткитами. Основное их различие состоит в том, что буткиты начинают свою работу еще до загрузки ОС. Они имеют такой же уровень контроля, как и легальные загрузчики, – главную загрузочную запись (MBR), загрузочный сектор логического диска или UEFI и вмешиваются в процесс загрузки ОС, что позволяет им отслеживать, изменять процесс загрузки, а также внедрять, к примеру, вредоносный код в обход механизмов защиты. Зачастую буткиты создают условия для бесшумного внедрения руткитов уровня ядра [4].

Существует несколько средств и методов, которые используются для защиты загрузочных секторов от атак и внедрения вредоносного ПО. Одним из основных является UEFI Secure Boot (Безопасная загрузка UEFI). Прежде стоит сказать, что такое UEFI. UEFI (Unified Extensible Firmware Interface) – микропрограмма, встроенная в материнскую плату. Пришла на смену BIOS. Как и последний, управляет оборудованием на низком уровне и дает возможность выполнить начальную настройку запуска компьютера. Унифицированный расширяемый интерфейс микропрограммного обеспечения (UEFI) – это уровень абстракции между операционной системой и базовой платформой, обеспечивающий загрузку и выполнение служб персонального компьютера. Эта абстракция обеспечивает единый набор функций, переменных и поведения среды для широкого спектра устройств и не зависит от архитектуры.

UEFI Secure Boot – это схема проверки подписи, которая проверяет двоичные файлы, такие как драйверы и загрузчики перед выполнением. Secure Boot содержит базу данных ключей и хэшей, которые могут обновляться производителями или настраиваться владельцами устройств для защиты от вредоносного ПО во время загрузки. Расширенная поддержка Trusted Platform Module (TPM), более длинные хэши измерений и хранение журнала аудита также присутствуют для создания записи целостности загрузки, включающей состояние Secure Boot. Некоторые производители предлагают собственные решения для обеспечения безопасности загрузки, которые интегрируются с UEFI для защиты процесса загрузки.

Secure Boot работает с использованием криптографических контрольных сумм и подписей. Каждая программа, загружаемая микропрограммой, содержит подпись и контрольную сумму, и прежде, чем разрешить ее выполнение, микропрограмма проверит, что программа является надежной, проверив контрольную сумму и подпись. Когда SB включена в системе, любая попытка выполнить недоверенную программу не будет разрешена. Это предотвращает запуск неожиданного/неавторизованного кода в среде UEFI. Большинство аппаратных средств x86 поставляются с завода с предустановленными ключами Microsoft. Это означает, что встроенное программное обеспечение этих систем будет доверять двоичным файлам, подписанным Microsoft. Большинство современных систем поставляется с включенной SB – по умолчанию они не будут запускать неподписанный код, но можно изменить конфигурацию прошивки, чтобы либо отключить SB, либо включить дополнительные ключи подписи. Большинство программ, которые должны работать в среде UEFI – это загрузчики, но существуют и другие. Есть также программы для работы с обновлениями прошивки перед запуском операционной системы (например, fwupdate и fwupd). Таким образом, это технология безопасности, которая обеспечивает проверку цифровых подписей загружаемых программ и драйверов на этапе загрузки компьютера. UEFI Secure Boot гарантирует, что только программное обеспечение, подписанное доверенным сертификатом, может быть загружено и выполнено на компьютере, что помогает предотвратить атаки, связанные с изменением загрузочного кода или внедрением вредоносного ПО в загрузочную область [5].

Доверенный платформенный модуль (TPM) представляет собой неотъемлемую часть системы безопасности компьютера, обеспечивая надежную защиту от широкого спектра угроз. Размещенный на материнской плате, TPM активно взаимодействует с остальными компонентами компьютера через системную шину, обеспечивая безопасность на уровне аппаратного обеспечения. Основной задачей TPM является обеспечение конфиденциальности и целостности данных путем хранения и управления криптографическими ключами, цифровыми сертификатами и другой чувствительной информацией. Он также обеспечивает механизмы для аутентификации пользователей и устройств, что помогает предотвратить несанкционированный доступ к системе. TPM также может быть использован для обеспечения безопасного запуска компьютера, гарантируя, что только доверенное программное обеспечение может быть загружено и выполнено при запуске системы. Это помогает предотвратить вредоносные атаки еще на этапе загрузки операционной системы. Кроме того, TPM может предоставлять механизмы для создания и хранения цифровых подписей, обеспечивая надежность и подлинность данных и приложений. Это становится особенно важным в условиях роста киберугроз и необходимости обеспечения конфиденциальности важных информационных ресурсов.

Компьютеры, оснащенные модулем TPM, имеют возможность создавать криптографические ключи и зашифровывать их таким образом, что они могут быть расшифрованы только модулем TPM. Данный процесс, часто называемый сокрытием ключа (wrapping key) или привязкой ключа (binding key), помогает защитить ключ от раскрытия. В каждом модуле TPM есть главный скрытый ключ, называемый

ключом корневого хранилища (Storage Root Key, SRK), который хранится в самом модуле TPM. Закрытая часть ключа, созданная в TPM, никогда не станет доступна любому другому компоненту системы, программному обеспечению, процессу или пользователю. Компьютеры, оснащенные модулем TPM, также могут создавать ключи, которые будут не только зашифрованы, но и привязаны к определенной системной конфигурации. Такой тип ключа может быть расшифрован только в том случае, если характеристика платформы, на которой его пытаются расшифровать, совпадает с той, на которой этот ключ создавался. Данный процесс называется «запечатыванием» ключа в модуле TPM. Дешифрование его называется «распечатыванием» (unsealing). Модуль TPM также может запечатывать и распечатывать данные, созданные вне модуля TPM. При использовании запечатанного ключа и такого программного обеспечения, как BitLocker Drive Encryption, можно обеспечить блокировку данных до тех пор, пока они не будут перенесены на компьютер с подходящей аппаратной или программной конфигурацией. При использовании модуля TPM закрытая часть пар ключей хранится вне памяти, доступ к которой имеет операционная система. Ключи могут быть запечатаны модулем TPM, при этом точное решение о том, является ли система надежной, будет принято до того, как ключи будут распечатаны и готовы к использованию. Поскольку модуль TPM для обработки инструкций использует собственное встроенное программное обеспечение и логические схемы, его работа не зависит от операционной системы. Благодаря этому обеспечивается его защита от возможных уязвимостей внешнего программного обеспечения. Таким образом, TPM является специальным аппаратным устройством, которое используется для обеспечения безопасности компьютерной системы. Он может использоваться для хранения криптографических ключей, выполнения аппаратной аутентификации и обеспечения целостности загрузочного процесса. TPM может быть использован в сочетании с другими методами защиты, такими как UEFI Secure Boot, для усиления безопасности загрузочных секторов [6].

Таким образом, данная работа описывает структуру главной загрузочной записи, типы атак на нее и важность ее защиты от несанкционированного доступа и модификации. В документе представлен обзор наиболее распространенных видов атак на область загрузки устройств, а также методов защиты, таких как UEFI Secure Boot и Trusted Platform Module.

Список использованных источников:

1. Главная загрузочная область – [Электронный ресурс] Электронные данные. – Режим доступа: https://studfile.net/preview/9565397/page:3.

2. Главная загрузочная запись – [Электронный ресурс] Электронные данные. – Режим доступа: https://shorturl.at/brJK7.

3. Rootkit [Электронный ресурс] – Электронные данные. – Режим доступа: https://en.wikipedia.org/wiki/Rootkit.

4. Буткиты: эволюция и способы обнаружения – [Электронный ресурс] Электронные данные. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/Bootkits-evolution-and-methods-of-detection.

5. Secure Boot – [Электронный ресурс] Электронные данные. – Режим доступа: https://wiki.debian.org/SecureBoot#What_is_UEFI_Secure_Boot.3F.

6. Что такое TPM – [Электронный ресурс] Электронные данные. – Режим доступа: http://al-tm.ru/stati/stati-po-setyam/trusted-platform-module.

UDC 004.056.52

ACCESS CONTROL BY BLOCKING MBR BOOT

Sirotkin E.A.[1], Pliska U.S. [2]

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Rogov M.G. – Assistant of the Department of Informatics

Annotation. This article examines the importance of protecting the computer's boot sector in the context of information technology and computer security. Considerable attention is paid to describing the use of modern access control methods through boot blocking, such as UEFI Secure Boot and TPM, in order to ensure the security of the boot process of computer systems. Current threats that are present in the context of MBR security are mentioned.

Keywords. MBR, UEFI Secure Boot, TPM, computer security, boot sector, boot attacks, malware protection, UEFI, bootkit, rootkit, secure boot, digital signature, hardware, secure startup.