УДК 004

К вопросу о защите от Intel Management Engine

Д. Ю. Счастный
Закрытое акционерное общество "ОКБ САПР", Москва, Россия

Intel Management Engine (IME) — встроенная проприетарная подсистема чипсетов Intel, обладающая неограниченным доступом к ресурсам компьютера. В качестве мер, ограничивающих потенциальное вредоносное воздействие IME на систему, предлагается использовать проверяемые аппаратные средства на всех каналах взаимодействия СВТ с внешним миром.

Ключевые слова: Intel Management Engine, резидентный компонент безопасности, служебный носитель, секрет особого назначения, транзит, новая гарвардская архитектура.

С 2008 г. Intel начала встраивать в свои чипсеты отдельную специализированную подсистему Intel Management Engine, которая сразу привлекла внимание специалистов по информационной безопасности. "Встроенная во многие платформы на основе наборов микросхем Intel® — это небольшая, имеющая малое энергопотребление компьютерная подсистема, называемая Intel® Management Engine (intel® ME). Intel® ME выполняет различные задачи, пока система находится в режиме сна, во время процесса загрузки и нормальной активности. Эта подсистема должна функционировать корректно для достижения наивысшей производительности и функциональности вашего ПК" [1] — это цитата с русскоязычной версии сайта Intel (с оригинальным вариантом можно ознакомиться [2]), описывающая IME. IME имеет не контролируемый ни аппаратными (на уровне процессора), ни программными (на уровне операционной системы (ОС)) средствами доступ к оперативной памяти компьютера, к встроенному сетевому адаптеру, к контроллерам PCI, PCIe, usb и прочей периферии [3]. Полностью исходный код IME недоступен для независимых исследований и анализа. Предпринимаются попытки дизассемблирования кода IME и последующего анализа, которые даже приводят к нахождению недокументированных возможностей [4], ошибок и уязвимостей [5]. Компания Intel признает эти уязвимости и даже выпускает обновления, их устраняющие [6]. Необходимо отметить, что найденные уязвимости признаются ФСТЭК и вносятся в Банк данных угроз безопасности информации [7—11]. По поводу одной из этих уязвимостей ФСТЭК России даже выпустила информационное письмо [12], предписывающее до появления обновления, нейтрализующего уязвимость, принять ряд жестких организационных мер, снижающих вероятность эксплуатации уязвимости.

Таким образом, можно констатировать, что внутри любого современного компьютера, построенного на базе чипсета от компании Intel, есть, по сути, еще один компьютер с неизвестным функционалом, имеющий неограниченный доступ к ресурсам основного компьютера. Есть три принципиальных пути снижения вероятности несанкционированной работы IME: отказаться от СВТ с чипсетами Intel, воздействовать на IME (удалить, запретить, модифицировать, внедрить собственный код) или изолировать IME от внешнего мира.

Отказ от СВТ с чипсетами Intel и переход на другие аппаратные платформы представляется наиболее правильным путем решения проблемы. К тому же имеются альтернативные защищенные аппаратные варианты [13]. Однако зачастую в силу различных организационных моментов (отсутствие необходимого программного обеспечения под другую аппаратную платформу, отсутствие специалистов, способных провести переход на другие аппаратные платформы, необходимость переобучения сотрудников работе с другой программной и аппаратной средой и т. п.) отказ от привычных инструментов (а СВТ — это инструмент) невозможен.

Все описанные в открытых источниках попытки пойти по второму пути и воздействовать каким-либо образом на IME не завершились успехом. Удаление IME приводило к неработоспособности СВТ. Штатного механизма отключения не существует. Попытки нештатного отключения [14] не дают стопроцентной уверенности в том, что эта подсистема полностью отключена. Внедрение собственного кода IME затруднено в силу закры-

Счастный Дмитрий Юрьевич, заместитель генерального директора.
E-mail: DimaS@okbsapr.ru

Статья поступила в редакцию 11 мая 2018 г.

тости технологии и предпринимаемых компанией Intel усилий по защите от такого внедрения. Компания Intel осознает все возможности, которые получает код, исполняющийся в IME, и разработала сложную криптографическую систему его защиты. По факту в IME может исполняться только код, подписанный на ключах Intel.

Таким образом, в случае невозможности отказа от использования СВТ с чипсетами Intel остается путь изоляции IME от внешнего мира. В описанной парадигме (неконтролируемый компьютер с неограниченными возможностями по доступу к ресурсам основного компьютера **внутри** этого основного компьютера) с подсистемой IME связаны следующие виды угроз:

- получение несанкционированного удаленного управления;
- несанкционированная передача конфиденциальных данных за пределы основного СВТ.

В качестве возможных каналов для реализации обеих угроз в современных компьютерах на базе чипсетов Intel могут выступать Ethernet и USB. Отметим, что в упомянутом информационном письме ФСТЭК [12] рекомендуется исключить неконтролируемые каналы связи, обеспечить защиту от несанкционированного использования USB-портов средств вычислительной техники (в том числе при помощи их опечатывания, а также отключения путем применения соответствующих настроек базовой системы ввода-вывода) и настроить межсетевые экраны соответствующим образом.

Подключаемые к USB-портам устройства (флешки, клавиатуры, мыши, токены, сканеры, принтеры, плоттеры, телефоны, фотоаппараты, жесткие диски) могут быть как каналом несанкционированного управления, так и приемником для несанкционированной передачи данных. При этом выполнять нештатные действия они могут в теневом режиме, незаметно для пользователя, подключившего их к USB-порту, параллельно с основным функционалом. По факту даже самая простая флешка представляет собой компьютер с собственным процессором и собственной памятью. Известен целый класс атак, называемый BadUSB, в основе которого лежит модификация firmware USB-устройств для выполнения несанкционированных действий процессором этих USB-устройств. Кроме того, существуют варианты реализаций штатных протоколов взаимодействия USB-устройств [15] с нештатными расширениями, которые могут быть использованы и как скрытые каналы управления, и как нелегальные хранилища для конфиденциальной информации.

На первый взгляд (учитывая многочисленные публикации о разнообразных DLP-системах), вопрос защиты от несанкционированного использования USB-устройств давно решен и его можно считать закрытым. Однако это не касается случая с IME. Необходимо помнить, что IME имеет прямой доступ к периферии (в том числе и к USB-контроллерам), минуя приложения и драйвера ОС. Программные агенты DLP-систем, функционирующие в ОС, могут определять наличие подключенных к портам устройств с некоторой задержкой, необходимой ОС для проведения работ по инициализации стека драйверов и извещения соответствующих агентов о подключении устройств к портам. Последующий контроль за обменом данными с устройством агенты DLP-систем могут проводить не ниже драйверов ОС, при этом IME может взаимодействовать с подключенными USB-устройствами напрямую через firmware USB-контроллера.

Следовательно, для нейтрализации такой угрозы средство контроля должно быть аппаратно независимым от целевой системы. В качестве такого средства контроля может выступать либо доверенный вычислитель, установленный непосредственно в подключаемое средство (по сути, являющийся частью этого USB-устройства), либо доверенный вычислитель, подключаемый в разрыв канала взаимодействия устройства и СВТ.

Устройства с интегрированным в них доверенным вычислителем существуют (служебные носители (СН) "Транзит" и "Секрет" [16]). Эти устройства служат для хранения данных и характеризуются невозможностью несанкционированного изменения firmware. В контексте взаимодействия с IME их можно считать доверенными: они не создадут скрытый канал управления и на них нельзя незаметно вынести конфиденциальные данные за пределы СВТ.

В качестве доверенного вычислителя, подключаемого в разрыв канала, могут быть разработаны либо переходники, с одной стороны подключаемые к USB-порту СВТ, а с другой — предоставляющие штатный USB-разъем для подключения к ним целевых устройств, либо USB-хабы, также подключаемые к USB-порту СВТ, к которым с другой стороны одновременно подключается несколько целевых устройств. Одним из основных свойств таких вычислителей должна быть невозможность несанкционированного изменения их firmware. Функциональное наполнение подобных устройств может быть самым разнообразным: они могут быть простыми фильтрами на уровне vid/pid подключаемого устройства, могут проводить процедуры аппаратной аутентификации подключае-

мых устройств по протоколам, аналогичным протоколам СН "Секрет", могут быть фильтрами протоколов взаимодействия, контролирующими четкое соответствие стандартам каждого подключаемого устройства.

Ситуация, описанная в предыдущей части в случае с USB-каналами, во многом повторяется и в случае с Ethernet-каналами. Также существуют мощные средства контроля (программные межсетевые экраны), которые оказываются бесполезными в случае необходимости контроля IME. Для качественной защиты межсетевые экраны необходимо делать независимыми от основного СВТ и устанавливать их в разрыв соединения Ethernet-контроллера и локальной вычислительной сети (ЛВС), к которой подключается СВТ, и уже внутри этих вычислителей осуществлять контроль трафика, отфильтровывая нештатные нестандартные сетевые пакеты. Существуют аппаратные межсетевые экраны, но по сложившейся практике применения они устанавливаются на границе периметра ЛВС и защищают сеть целиком, однако не защищают СВТ в ЛВС друг от друга и от подключенного нештатно стороннего СВТ.

Все эти технические средства должны быть тесно вплетены в регламенты и подкреплены строгими организационными мерами. Технологические процессы должны быть выстроены таким образом, чтобы не возникала необходимость подключать к локальным СВТ принтеры, плоттеры, сканеры и прочее важное офисное оборудование. Все неиспользуемые USB-порты должны быть заклеены соответствующими защитными знаками. Пользователи должны быть извещены о запрете на подключение к незаклеенным USB-портам любых устройств, кроме выданных СН или иных разрешенных устройств, или все открытые USB-порты должны обеспечивать подключение устройств только через доверенные USB-хабы. На все Ethernet-соединения должны быть установлены персональные аппаратные межсетевые экраны. Все это оборудование должно быть настроено и поддерживаться в актуальном состоянии в течение всего жизненного цикла системы. Таким образом, логично вернуться к первоначальной постановке задачи и еще раз рассмотреть вариант отказа от использования чипсетов Intel и переход на защищенные альтернативные варианты.

Все перечисленные выкладки относятся к случаю защиты от угроз, связанных с IME, универсальных СВТ, построенных на чипсетах Intel. Если провести анализ предложенных решений, вычленить в них главное (аппаратную независимость), объединить доверенные вычислители в одном и сделать полученное в едином конструктиве, то получится резидентный компонент безопасности (РКБ) [17]. Ситуация очень похожа на ситуацию с настоящими аппаратными модулями доверенной загрузки (АМДЗ), устанавливаемыми на системную шину и самостоятельно принимающими решения. Но в отличие от ситуации с АМДЗ использовать какую-либо системную шину при защите от угроз, связанных с IME, нельзя. Поэтому нужно отказаться от идеи защищать универсальные СВТ и разработать специализированные материнские платы. На этих материнских платах РКБ будет правильным образом физически подключен по всем интерфейсам и будет сам контролировать USB и Ethernet-каналы. Формально это будет единая материнская плата, устанавливаемая внутрь корпуса СВТ, но фактически это будет физическое объединение двух компьютеров (РКБ и чипсета от Intel). В этом случае получится решение, на порядок более простое в эксплуатации, чем набор подключаемых к различным портам устройств при защите универсальных СВТ, так как для пользователя СВТ будет выглядеть, как обычное СВТ с привычным набором портов, а администраторам информационной безопасности не нужно будет контролировать физические порты и корректность подключения доверенных вычислителей к ним.

Литература

1. Часто задаваемые вопросы об утилите проверки Intel® Management Engine [Электронный ресурс]. URL: https://www.intel.ru/content/www/ru/ru/support/articles/000005974/software/chipset-software.html (дата обращения: 08.04.2018).
2. Frequently Asked Questions for the Intel® Management Engine Verification Utility [Электронный ресурс]. URL: https://www.intel.com/content/www/us/en/support/articles/000005974/software/chipset-software.html (дата обращения: 08.04.2018).
3. *Kumar A.* Active Platform Management Demystified: Unleashing the Power of Intel VPro (TM) Technology. Intel Press, 2009.
4. *Горячий М., Ермолов М.* Выключаем Intel ME 11, используя недокументированный режим [Электронный ресурс]. URL: https://habrahabr.ru/company/pt/blog/336242/ (дата обращения: 08.04.2018).
5. Уязвимость Intel ME позволяет выполнять неподписанный код [Электронный ресурс]. URL: https://habrahabr.ru/company/pt/blog/339292/ (дата обращения: 08.04.2018).
6. Intel Q3'17 ME 6.x/7.x/8.x/9.x/10.x/11.x, SPS 4.0, and TXE 3.0 Security Review Cumulative Update [Электронный ресурс]. URL: https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00086&languageid=en-fr (дата обращения: 08.04.2018).
7. BDU:2017-02217: Множественные уязвимости подсистемы Intel Management Engine (ME) микропрограммного обеспечения семейства микросхем Platform Controller Hub, позволяющие выполнить неподписанный код [Электронный ресурс]. URL: https://bdu.fstec.ru/vul/2017-02217 (дата обращения: 08.04.2018).
8. BDU:2017-02527: Множественные уязвимости подсистемы Intel Server Platform Services (SPS) микропрограммного

обеспечения семейства микросхем Platform Controller Hub, позволяющие выполнить неподписанный код [Электронный ресурс]. URL: https://bdu.fstec.ru/vul/2017-02527 (дата обращения: 08.04.2018).

9. BDU:2017-02528: Множественные уязвимости подсистемы Intel Trusted Execution Engine (TXE) микропрограммного обеспечения семейства микросхем Platform Controller Hub, позволяющие выполнить неподписанный код [Электронный ресурс]. URL: https://bdu.fstec.ru/vul/2017-02528 (дата обращения: 08.04.2018).

10. BDU:2017-02532: Множественные уязвимости подсистем Active Management Technology (AMT) и Intel Management Engine (ME) микропрограммного обеспечения семейства микросхем Platform Controller Hub, позволяющие выполнить произвольный код [Электронный ресурс]. URL: https://bdu.fstecru/vul/2017-02532 (дата обращения: 08.04.2018).

11. BDU:2017-02534: Множественные уязвимости подсистем Active Management Technology (AMT) и Intel Management Engine (ME) микропрограммного обеспечения семейства микросхем Platform Controller Hub, позволяющие выполнить произвольный код [Электронный ресурс]. URL: https://bdu.fstec.ruvul/2017-02534 (дата обращения: 08.04.2018).

12. ФСТЭК. Информационное сообщение от 25 октября 2017 г. № 240/22/4900 об уязвимости микропрограммного обеспечения Intel Management Engine.

13. *Конявский В. А., Степанов В. Б.* Компьютер типа "тонкий клиент" с аппаратной защитой данных. Патент на полезную модель № 118773. 27.07.2012. Бюл. № 21.

14. Боремся с дистанционным контролем: как отключить Intel ME [Электронный ресурс]. URL: https://habrahabr.ru/company/pt/blog/302292/ (дата обращения: 08.04.2018).

15. *Кравец В. В.* Клавиатура — устройство вывода? [Электронный ресурс]. URL: https://habrahabr.ru/company/pm/blog/352868/ (дата обращения: 08.04.2018).

16. *Конявский В. А., Щербаков А. Ю.* Специальный съемный носитель информации. Патент на полезную модель № 94751. 27.05.2010. Бюл. № 15.

17. *Конявский В. А.* Управление защитой информации на базе СЗИ НСД "Аккорд". — М.: Радио и связь, 1999. — 325 с.

On the Protection from Intel Management Engine Question

D. Yu. Schastny
Closed Joint Stock Company "OKB SAPR", Moscow, Russia

Intel Management Engine (IME) — is the embedded proprietary Intel chip set subsystem, that has unlimited success to the computer resources. The way of the limiting of its potential harmful influence on the computing system, suggested in the article, is the following: to use some controllable hardware tools on all the channels of the computer and environment communication.

Keywords: Intel Management Engine (IME), resident safety component, official carrier, special secret, transit, new harvard architecture.

Bibliography — 17 references. *Received May 11, 2018*