УДК 004.056.53

АНАЛИЗ СРЕДСТВ ДОВЕРЕННОЙ ЗАГРУЗКИ В БОРТОВЫХ ВЫЧИСЛИТЕЛЯХ

Деменкова Т.А., Боронников А.С.

МИРЭА – Российский технологический университет, 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail: demenkova@fit.mirea.ru, boronnikov-anton@mail.ru

Компетенции цифрового проектирования востребованы во всех высокотехнологичных компаниях в России и в мире и полностью соответствуют глобальным трендам IV промышленной революции и цифровой экономики. Работа посвящена важной проблеме из этой области и относится к исследованию средств доверенной загрузки, применяемых в бортовых вычислителях. Приведены основные виды атак несанкционированного доступа на уровне микропрограмм BIOS и UEFI, состав средств модулей доверенной загрузки и алгоритм работы, а также решения, предложенные разработчиками бортовой аппаратуры с использованием данной технологии защиты информации.

Ключевые слова: доверенная загрузка, информационная безопасность, бортовой вычислитель.

ANALYSIS OF TRUSTED LOAD FACILITIES IN ON-BOARD COMPUTERS

Demenkova T.A., Boronnikov A.S.

MIREA - Russian Technological University, 119454, Russia, Moscow, 78 Vernadsky Avenue, e-mail: demenkova@fit.mirea.ru, boronnikov-anton@mail.ru

Digital design competencies are in demand in all high-tech companies in Russia and worldwide and fully correspond to the global trends of the 4th industrial revolution and the digital economy. The work is dedicated to an important issue from this area and refers to the study of trusted downloads used in on-board computers. The main types of unauthorised access attacks at the BIOS and UEFI firmware level, the composition of the means of trusted loading modules and the work algorithm, as well as solutions proposed by the developers of on-board equipment using this information security technology are presented.

Keywords: trusted download, information security, onboard computer.

Основу бортовых вычислителей составляют процессорные модули. Управляющим ядром модуля является микропроцессорная система достаточно большой вычислительной мощности, компактного размера, высокой надежности, низкого энергопотребления и с поддержкой необходимого количества интерфейсов. Одной из основных проблем использования современных микропроцессоров в таких системах является обеспечение выполнения контроля целостности файлов и данных до загрузки операционной системы [1]. Именно здесь на помощь приходят так называемые средства доверенной загрузки.

В классическом сценарии загрузки вычислительного модуля первая исполняемая микропрограмма после подачи питания – это BIOS (Basic Input/Output System, базовая система ввода вывода). BIOS хранится в энергонезависимой памяти, как правило в микросхеме EEPROM или flash-памяти. Главное назначение BIOS состоит в обеспечении инициализации и тестирования на низком уровне аппаратных компонентов компьютера и передаче управления загрузчику операционной системы.

Практика показывает, что злоумышленники нередко выбирают в качестве компонента для заражения тот, который загружается раньше всех. Поскольку на ранней стадии загрузки системы BIOS запускается с высоким уровнем привилегий, то вирус очень трудно обнаружить. В этих условиях внедрение вредоносного кода на уровне микропрограммного обеспечения может позволить нарушителям получить полный контроль над всей системой. Помимо этого, вирус может использоваться для вторичного заражения системы даже после переустановки операционной системы или замены винчестера [2].

Атаки на ранней стадии загрузки системы условно можно разделить на два типа:

1) атаки на BIOS;
2) атаки на загрузчик.

Первые заключаются в подмене исходного кода BIOS на вредоносный. Вторые – во внедрении так

называемого буткита (*bootkit*), который является разновидностью руткита (*rootkit*), имеет общее свойство с загрузочным вирусом, однако содержит компоненты, которые внедряются в ОС еще до ее загрузки.

Между тем стоит заметить, что атаки на традиционный BIOS не выступают первоочередной задачей нарушителей. Связано это со слабой стандартизацией BIOS, то есть он очень зависим от системы. Поэтому разработать и внедрить универсальный механизм атаки весьма затруднительно [3].

Однако отметим, что в современных системах на смену традиционному BIOS пришел UEFI (Extensible Firmware Interface) – интерфейс между операционной системой и микропрограммами, управляющими низкоуровневыми функциями оборудования. Условно разница между BIOS и UEFI заключается в том, что BIOS исполняется в 16-битном реальном режиме работы микропроцессора, а UEFI – в современном 64-битном защищенном режиме. Появление хорошо стандартизированного интерфейса упростило разработку легальных программ, но в то же время снизилась сложность задачи внедрения вирусов для злоумышленников на уровне микропрограмм. Хотя ключевой возможностью UEFI стал механизм SecureBoot, который осуществляет проверку компонентов ОС криптографическими методами, но тем не менее известны случаи внедрения шпионского ПО на уровне данного интерфейса. Таким образом, механизм SecureBoot стоит рассматривать только как один из вариантов обеспечения безопасной загрузки системы. Другими средствами защиты от несанкционированного доступа в систему должны быть средства доверенной загрузки.

Понятие «доверенная загрузка» означает, что ОС на вычислителе может загружаться только с определенного достоверного носителя (к примеру, с жесткого диска) после идентификации и аутентификации пользователя. Загрузка же с других носителей должна блокироваться. В соответствии с требованием доверенная загрузка должна обеспечивать:

- блокирование попыток несанкционированной загрузки нештатной ОС или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной ОС;
- контроль доступа пользователей к процессу загрузки ОС;
- контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

Рассматриваемый класс средств защиты информации подразделяется на три вида (рис.1):

1) уровень BIOS;
2) уровень платы расширения;
3) уровень загрузочной записи.



Рис.1. Виды средств доверенной нагрузки

К первой группе относят программные средства, один из модулей которых встраивается непосредственно в микропрограмму системной платы. Для работы таких средств не требуется установка специализированных плат, что существенно упрощает ввод защиты системы в эксплуатацию.

Вторая группа СДЗ плат расширения всегда аппаратно-программная. Это самые популярные модули на российском рынке. В частности, лидирующие позиции занимают следующие комплексы, представленные в таблице 1 [4, 5, 6, 7].

Таблица 1. Примеры СДЗ уровня плат расширения.

СДЗ	**Описание**
ПАК «Соболь»	1) выбор форматов исполнения; 2) аутентификация пользователей; 3) блокировка загрузки ОС со съемных носителей; 4) контроль целостности программной среды; 5) контроль целостности системного реестра Windows; 6) сторожевой таймер; 7) регистрация попыток доступа к ПЭВМ; 8) контроль конфигурации.
Аккорд-АМДЗ	1) защита ресурсов ПЭВМ от лиц, не допущенных к работе на ней, на основе идентификации пользователей по персональным идентификаторам до загрузки ОС; 2) аутентификация пользователей по паролю длиной до 12 символов;

	3) блокировка загрузки с отчуждаемых носителей; 4) контроль целостности технических и программных средств до загрузки ОС; 5) контроль целостности объектов файловых систем; 6) регистрация на ПЭВМ до 126 пользователей; 7) регистрация контролируемых событий в системном журнале; 8) администрирование встроенного ПО комплекса; 9) регистрация, сбор, хранение и выдача данных о событиях, происходящих в ПЭВМ в части системы защиты от несанкционированного доступа.
МАКСИМ-М1	1) контроль доступа при первоначальном запуске ПЭВМ, до перехода к ОС (идентифицирует и аутентифицирует пользователя двухфакторным методом); 2) ведёт нестираемые журналы: проверки подлинности пользователей, контроля целостности (сохранность данных гарантируется за счет энергонезависимой памяти); 3) проверяет в реальном времени срок действия пользовательских данных (ключи, служебная информация); 4) контролирует аппаратные и программные средства защищаемой системы (оперативную память, жёсткие диски, файловую систему и журналы ФС, реестр Windows); 5) защищает от подбора пароля.
АПМДЗ	1) идентификация и аутентификация пользователей до начала загрузки ОС; 2) предотвращение обхода АПМДЗ и загрузки ПЭВМ с любых внешних носителей, кроме штатного носителя; 3) регистрация попыток несанкционированного доступа в журнале событий; 4) контроль целостности конфигурации ПЭВМ, ядра и загрузочных модулей ОС, программного обеспечения и данных с поддержкой файловых систем FAT, NTFS, EXT2, EXT3, а также реестра Windows; 5) передача информации о пользователе, прошедшем аутентификацию, в СЗИ поддерживаемой ОС; 6) возможность настройки параметров политики безопасности.

Последняя группа СДЗ уровня загрузочной записи основана на шифровании boot-секторов логических разделов жестких дисков, что позволяет скрыть данные при несанкционированной загрузке вычислителя. В отличие от вышеперечисленных средств, здесь не обеспечивается защита от загрузки нештатных ОС. В качестве примера может служить Trusted Boot Loader фирмы «Код Безопасности».

В бортовых вычислителях в основном применяют СДЗ второй группы, то есть в виде плат расширения. АПМДЗ – аппаратно-программный модуль доверенной загрузки на российском рынке компьютерной безопасности существует достаточно давно. В настоящий момент его нельзя отнести к категории новинок в сфере информационных технологий. Но, тем не менее, АПМДЗ является проверенным годами комплексом защиты от злоумышленников. В состав АПМДЗ входят: плата расширения (стандарта семейства шины PCI, возможно исполнение в формате PMC); средства идентификации пользователя (USB-ключи, смарт-карты, идентификаторы iButton); сопутствующее программное обеспечение для различных видов операционных систем.

Как видно, данное оборудование устанавливается непосредственно на рабочее место вычислительной системы пользователя (далее оператора). Это может быть либо сервер, либо АРМ (автоматизированное рабочее место). В частности, для установки АПМДЗ может потребоваться какой-либо стандарт шины семейства PCI. Но так как в основном разъемы объединительной платы, входящей в состав серверов или АРМ, исполняются в стандарте VME или CompactPCI, то основным решением является АПМДЗ конструктивного исполнения в формате PCI-PMC (PMC – мезонинная плата, вставляемая в основную (носитель) и располагающаяся параллельно). В качестве примера можно привести процессорный модуль К42 компании ЗАО «Компонент-АСУ» и АПМДЗ «Центурион-М» от АО «ЦНИИ ЭИСУ».

Система считывания идентификатора выводится на рабочее место оператора (возможен вывод на коммутационную коробку или пульт управления). АПМДЗ при инициализации позволяет зарегистрировать учетную запись администратора, который может регистрировать пользователей, имеет доступ к журналу системных событий и управлению некоторыми системными объектами. Рассмотрим алгоритм работы АПМДЗ:

1) Оператор должен пройти идентификацию (приложить персональный идентификатор к считывающему устройству);

2) Процесс аутентификации (в основном требуется ввести пароль);

3) Если первые два пункта прошли успешно, то МДЗ выполняет процесс проверки целостности аппаратной и программной части системы (все еще до загрузки ОС);

4) Далее, если ОС загружается не из доверенного источника информации, то активируется блокировка НСД и производится запись об этом в специальном журнале системных событий;

5) Если по истечении некоторого установленного времени после включения управление не было передано плате МДЗ, то включается сторожевой таймер, который ограничит доступ к системе;

6) После загрузки ОС сохраняется совместное функционирование внешних приложений и постоянный мониторинг действий пользователей.

Основная проблема, которая может возникнуть с установкой АПМДЗ, заключается в следующем: в качестве идентификатора к модулю доверенной загрузки используется USB-ключ, а первой микропрограммой выступает «традиционный» BIOS. Так как по сравнению с UEFI-интерфейсом BIOS имеет ограниченный функционал, то «обнаружение» USB-портов происходит только во время загрузки ядра операционной системы. Но АПМДЗ загружает ОС только после успешного процесса идентификации и аутентификации. В связи с этим порт не может считать USB-ключ, тем самым доступ к системе закрыт. Многообразие вредоносного программного кода, функционирующего на уровне BIOS/UEFI, указывает о серьезной необходимости защиты. Результаты проведенных исследований и предложенные решения в области средств доверенной загрузки могут использоваться при разработке бортовых вычислительных комплексов, а также позволяют расширить круг используемой элементной базы с возможностью предусмотреть защиту от возможных атак на микропрограммном уровне. Исследования проведены на оборудовании ЦКП РТУ МИРЭА.

Работа выполнена при поддержке Министерства науки и высшего образования Российской Федерации (проект № FSFZ-2020-0022).

Список литературы

1. Счастный Д.Ю. Перспективы развития средств доверенной загрузки. Взгляд разработчика//Вопросы защиты информации.2017. №3. С.27–28.

2. Лыдин С.С. О средствах доверенной загрузки для аппаратных платформ с UEFI BIOS // Вопросы защиты информации. 2016. №3. С. 45–50.

3. Авезова Я.Э., Фадин А.А. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности. 2016. №1(14). С. 24–30.

4. ПАК «Соболь» [Электронный ресурс]. – Режим доступа: https://www.securitycode.ru/products/pak_sobol/ (дата обращения 16.01.2020)

5. Аккорд-АМДЗ. [Электронный ресурс]. – Режим доступа: http://www.accord.ru/amdz.html (дата обращения 20.01.2020)

6. МАКСИМ-М1. [Электронный ресурс].: https://rusbitech.ru/products /szi/ apmdz- maksim/?cultureKey= (дата обращения 20.01.2020)

7. АПМДЗ «Центурион». [Электронный ресурс]. – Режим доступа: http://cniieisu.ru/projects/basic-technologies (дата обращения 20.01.2020)

References

1. Happy D.Y. Prospects for development of means of the entrusted loading. View of the developer// Information Protection Polls. 2017. № 3. C.27–28.

2. Lydin, S.S. About means of the entrusted boot for hardware platforms with UEFI BIOS // Information protection questions. 2016. №3. C. 45–50.

3. Avezova, Ya.E.; Fadin, A.A. Issues of the trusted boot provision in the physical and virtual environments (in Russian) // Cyber security issues. 2016. №1(14). C. 24–30.

4. Sobol, PJSC [Electron resource]. - Access mode: https://www.securitycode.ru/products/pak_sobol/ (circulation date 16.01.2020).

5. Accord-AMDZ. [Electronic resource]. - Access mode: http://www.accord.ru/amdz.html (circulation date 20.01.2020).

6. MAXIM-M1. [Electronic resource].: https://rusbitech.ru/products /szi/ apmdz- maksim/?cultureKey= (circulation date 20.01.2020)

7. APMDZ Centurion. [Electronic resource]. - Access mode: http://cniieisu.ru/projects/basic-technologies (circulation date 20.01.2020).