ДОВЕРЕННАЯ СРЕДА

УДК 004.056.53

Доверенная загрузка и контроль целостности архивированных данных. Часть и целое. (*Обзор*)

А. А. Алтухов
Закрытое акционерное общество "ОКБ САПР", Москва, Россия

Показана необходимость контролировать отдельные элементы, входящие в состав архивов. Приведены конкретные примеры, показывающие актуальность проблемы.

Ключевые слова: доверенная загрузка, модуль доверенной загрузки, средство доверенной загрузки, резидентный компонент безопасности, доверенная вычислительная среда, доверенные вычисления, контроль целостности.

Модель доверенной вычислительной среды (ДВС) (см. [1], с. 204) остается одной из актуальных и практически применимых субъектно-объектных моделей защиты технологии электронного обмена информации. Вместе с тем нельзя отрицать, что развитие парадигм доверенных вычислений и субъектно-объектных моделей не стоит на месте [2]. Целый класс задач электронного обмена информации решается в рамках подхода доверенного сеанса связи (ДСС) [3—8]. Однако развитие происходит не только за счет разработки новых парадигм, но и за счет улучшения и совершенствования уже существующих. В частности, идет развитие в рамках субъектно-объектной модели ДВС. Появляются предложения по новым реализациям и функциональному составу резидентного компонента безопасности (РКБ) [9, 10], наличие которого предполагается в ДВС (см. [1], с. 1).

Не следует забывать и о средствах доверенной загрузки как наиболее распространенных реализациях РКБ. Процесс обеспечения доверенной загрузки по-прежнему является одним из основных способов решения проблемы защиты информации от несанкционированного доступа и организации доверенной вычислительной среды. Одной из наиболее популярных и проверенных временем реализаций РКБ является средство доверенной загрузки (СДЗ), в частности аппаратные (программные) модули доверенной загрузки (А(П)МДЗ), или, в терминологии отечественных регуляторов, средство доверенной загрузки уровня платы расширения. Средство доверенной загрузки — программно-техническое средство, которое осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы, контроль целостности своего программного обеспечения и среды функционирования (программной среды и аппаратных компонентов средств вычислительной техники), а также не препятствует доступу к информационным ресурсам в случае успешных контроля целостности своего программного обеспечения и среды функционирования, проверки подлинности пользователя и загружаемой операционной системы [11—14].

Большинство современных и проверенных временем систем защиты информации от несанкционированного доступа включает в себя компонент, обеспечивающий доверенную загрузку. Он является фундаментальной составляющей многих систем защиты [15], которые выполняют самые различные функции безопасности (аудита, аутентификации, разграничения доступа и прочие функции безопасности), в операционных системах (ОС) [16, 17], средствах виртуализации [18, 19], системах управления базами данных, электронном документообороте и т. д.

Контроль целостности элементов среды является одной из основ создания ДВС (см. [1], с. 219). Следовательно, одна из основных групп функций, которые должны быть реализованы РКБ, — это функции контроля целостности: контроль целостности технического состава ЭВМ и локальной вычислительной сети (ЛВС), контроль целостности ОС, контроль целостности прикладного программного обеспечения (ППО) и данных (см. [1], с. 266). Необходимость вышеописанных функций не противоречит нормативным документам отечественных регуляторов. В список основных угроз безопасности информации, нейтрализация которых должна быть обеспечена, входят: нарушение целостности программной среды средств вычислительной техники и (или) состава компонентов

Алтухов Андрей Андреевич, программист 2 категории группы программирования ПО СЗИ.
E-mail: altuhov@okbsapr.ru

Статья поступила в редакцию 26 июня 2016 г.

аппаратного обеспечения средств вычислительной техники в информационной системе, нарушение целостности программного обеспечения средства доверенной загрузки (см. [11], с. 5).

Все множество функций контроля можно сгруппировать в три класса:

- контроль целостности технических средств ЭВМ,
- контроль целостности системных областей жестких дисков,
- контроль целостности отдельных файлов и программных средств.

Последняя в списке группа и отвечает за осуществление контроля целостности ОС и необходимых программных компонентов, в том числе и иных средств защиты и элементов комплексов защиты, работающих после СДЗ в ДВС.

Данная функция реализуется как пошаговый контроль целостности объектов файловых систем для различных файловых систем: FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, Ext4, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX, ReiserFS (см. [1], с. 266; [15]). Иными словами, для возможности контроля целостности загружаемой операционной системы необходимо осуществлять контроль целостности исполняемых файлов и файлов конфигурации, необходимых и влияющих на загрузку ОС. Следует отметить, что на практике конкретные типы файловой системы соответствуют конкретной операционной системе.

Для осуществления контроля данных (файлов, каталогов и прочих объектов файловых систем) необходимо получить доступ к этим данным. Данные могут находиться как на различных аппаратных носителях (например, не только на обычных жестких дисках, но и на накопителях на магнитной ленте и RAID-массивах), так и на различных файловых системах. В силу того, что СДЗ работает до загрузки ОС и должно быть самодостаточным, для успешного контроля целостности необходимо обеспечить разбор файловых систем.

В соответствии с парадигмой ДВС и требованиями к функции СДЗ нет необходимости контролировать абсолютно все. Под целостностью вычислительной среды понимают стабильность в течение рассматриваемого периода в требуемом диапазоне состава объектов и процессов, их взаимосвязей и параметров функционирования (см. [1], с. 207). Каким будет состав, какими параметры и взаимосвязи и в течение какого периода времени, определяется для каждого конкретного случая. На практике на состав контролируемых параметров (в частности, список контролируемых файлов) могут влиять такие конкретные вещи, как тип операционной системы (см. [20], с. 17; [21], с. 52), функции, выполняемые автоматизированной системой, и т. д. Тонкая настройка достигается за счет возможности контроля отдельных файлов и их атрибутов (см. [21], с. 34).

Есть особые типы файлов, являющихся структурами данных, каждый элемент которых может быть использован различными программами и процессами. Иными словами, несмотря на то что данная структура в файловой системе представлена одним или несколькими элементами, на самом деле она является коллекцией логических элементов. В конкретном случае одни логические элементы влияют на загрузку ОС, а другие нет.

Под коллекцией данных будем понимать некоторый набор логических элементов, которые представлены одним или несколькими объектами файловой системы. Примерами здесь могут служить различные файлы конфигураций, базы данных, образы дисков, архивы и прочие структуры данных.

Одним из примеров подобной коллекции данных является реестр Windows [22]. Поскольку на процесс загрузки операционных систем семейства Windows влияют не только системные файлы, но и реестр, контроля файловой системы недостаточно для того, чтобы убедиться в корректности загрузки этих ОС. Необходимо также проконтролировать неизменность отдельных ветвей реестра.

Штатная работа многих программ в течение одной сессии пользователя предполагает модификацию некоторых веток реестра, которые не влияют на доверенную загрузку. Работа ОС вполне может предполагать изменения реестра в рамках сеанса работы. Таким образом, после завершения работы файлы, в которых содержится реестр, меняются. Попытка контролировать реестр на уровне файловой системы становится несостоятельной, что проявляется в практической невозможности создать рабочую доверенную среду. В этом случае для обеспечения доверенной загрузки ОС семейства Windows необходимо обеспечить возможность контроля отдельных элементов системного реестра (см. [15]; [21], с. 10).

Обобщая вышесказанное, можно выйти на более глобальную идею. Возможность контролировать логические элементы коллекции данных позволит обеспечить возможность более тонкой настройки контролируемых параметров ДВС. В частности, контроль отдельных настроек, занесенных в файл конфигурации (пусть даже несложной структуры, например обычных текстовых INI), позволяет расширить возможности эксперта, определяющего условия функционирования системы доверенной обработки информации. Важно понять, что конкретный объект файловой системы

не является "логически атомарным". Он может содержать различные логические элементы, часть из которых влияет на процесс обеспечения доверенной загрузки, а часть нет. Таким образом, с практической точки зрения встает вопрос определения коллекций данных, влияющих на загрузку ОС и реализацию функциональности СДЗ контроля отдельных логических элементов коллекций данных.

Был приведен пример и показана необходимость контролировать состав коллекции данных, влияющих на загрузку ОС. Коллекция данных является широким понятием, существует потенциально бесконечное количество конкретных примеров. В данной работе предлагается ограничиться рассмотрением некоторых коллекций данных, логическими элементами которых являются файлы.

Под виртуальными дисками будем подразумевать такие коллекции данных, логические элементы которых являются объектами файловых систем: файлы и каталоги. Примерами виртуальных дисков могут служить различные форматы архивов и различные образы дисков.

Говоря об архивах, следует отметить, что традиционно они используются для удобства хранения и переноса информации (например, передачи по каналам связи), а также экономии места, занимаемого на накопителях.

Однако во многих ОС в процессе загрузки используются определенные типы архивов. Рассмотрим некоторые наиболее важные и актуальные примеры.

vSphere Hypervisor или ESXi — это аппаратный гипервизор, который устанавливается непосредственно на физический сервер и разделяет его на несколько виртуальных машин [23]. Формально ESXi является такой же операционной системой, как Windows или GNU\Linux, не считая того, что он создан для выполнения строго конкретной задачи — виртуализации. Не приводя подробной структуры разбиения диска на разделы и перечня файлов, замечу, что в состав файлов ESXi входит файл с именем state.tgz, который является образом файловой системы гипервизора. Данный файл является сжатым tar архивом корневой файловой системы ESXi и необходим для загрузки ОС ESXi.

Еще одним важным примером "виртуальных дисков" является файл initrd. Загрузка ОС на базе ядра Linux обычно предполагает загрузку двух элементов: файла ядра операционной системы и файла, содержащего временную файловую систему (следует отметить, что два вышеуказанных элемента физически могут представлять один файл). Initrd (Initial RAM Disk, диск в оперативной памяти для начальной инициализации) — временная файловая система, используемая ядром Linux при начальной загрузке. Initrd обычно используется для начальной инициализации перед монтированием корневых ("настоящих") файловых систем, которые, как правило, расположены в ПЗУ, например на жестком диске ПЭВМ. Данный подход решает проблему функциональной достаточности модульного ядра ОС во время загрузки: для монтирования файловой системы необходим модуль для работы с диском и файловой системой, а для чтения модулей — файловая система, с которой этот модуль читается [24]. Файл initrd является сжатым архивом cpio.

Еще одним примером является архив типа squashfs (.sfs) — сжимающая файловая система, предоставляющая доступ к данным в режиме "только для чтения". Она используется преимущественно в ОС GNU/Linux. Данная файловая система широко используется в файловых системах, предназначенных "только для чтения" (Live CD), а также в ограниченных по размеру блочных устройствах или системах хранения (во встраиваемых системах и тонких клиентах) [23]. Обычно этот виртуальный диск представлен в виде целого файла-архива, в котором находиться образ корневой файловой системы.

Три приведенных типа архива обладают несколькими общими свойствами:

- являются образами файловой системы, которые необходимы для загрузки и/или работы ОС;
- являются одним объектом файловой системы (файл);
- содержат в себе несколько файлов (являются виртуальными дисками).

Из указанных свойств следует, что изменение любого логического элемента, входящего в состав архива, сопровождается изменением всего файла. В случае, если нет возможности контролировать состав элементов архива по отдельности, то можно только фиксировать изменение файла архива целиком. Изменения в данные файлы могут вноситься как в процессе обновления, так и в процессе работы ОС. Таким образом, штатная работа или обновление ОС, не влияющие на доверенную загрузку и вносящие изменения в вышеперечисленные архивы, будут фиксироваться СДЗ как нарушения контроля целостности, в результате чего будут возникать дополнительные издержки, связанные с фиксацией инцидента и реагированием на него. Описанная проблема возникает из-за отсутствия технической возможности реализовать выбор диапазона состава объектов и процессов, их взаимосвязей и параметров функционирования вычислительной среды в соответствии с конкретной задачей.

Решать указанную проблему можно, подстроив задачи под функциональные возможности СДЗ, тем самым ограничивая функциональные возможности автоматизированных систем и, фактически, сузив возможные варианты реализации ДВС. Однако не следует забывать, что СДЗ является лишь средством, которое должно работать в соответствии с постулатами ДВС [25].

Для организации тонкой настройки контроля целостности параметров вычислительной среды и повышения эффективности работы процессов, реализующих меры защиты, необходимо обеспечить возможность контроля отдельных элементов: файлов и каталогов, входящих в состав архива и влияющих на загрузку ОС.

Возможность контролировать файлы, входящие в состав архивов, добавлена в АМДЗ Аккорд. В интерфейс администрирования была добавлена функциональность работы с виртуальными дисками. Просматривая содержимое файловой системы, пользователь имеет возможность выбрать файлы, которые поддерживаются в АМДЗ, в качестве виртуальных дисков. После подключения выбранного виртуального диска он появляется в списке виртуальных дисков и с ним можно работать таким же образом, как и с физическими дисками, просматривать содержание и ставить конкретные файлы и каталоги на контроль.

Кроме трех перечисленных архивов (Squashfs, tar.gz и cpio), также поддерживаются архивы zip и образы CD/DVD дисков ISO9660.

Литература

1. *Конявский, В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией (Библиотека журнала "УЗИ"; Кн. 2). — Мн.: "Беллитфонд", 2004. — 282 с.

2. "Доверенная гарвардская" архитектура – компьютер с динамически изменяемой архитектурой / Комплексная защита информации: материалы XX науч.-практ. конф., Минск, 19–21 мая 2015 г. — Мн.: РИВШ, 2015. С. 32—37.

3. *Конявский В. А.* Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем — на старт, внимание, МАРШ! / Комплексная защита информации. Материалы XV межд. науч.-практ. конф., Иркутск, 1–4 июня 2010 г. — М., 2010.

4. *Каннер А. М.* Средство организации доверенного сеанса как альтернатива доверенной вычислительной среде // Информационные технологии управления в социально-экономических системах. — М., 2010. Вып. 4. С. 140—143.

5. *Счастный Д. Ю.* Ноутбук руководителя / Комплексная защита информации: материалы XX науч.-практ. конф., Минск, 19–21 мая 2015 г. — Мн.: РИВШ, 2015. С. 112, 113.

6. Съемный носитель информации. Патент на полезную модель № 102139. 10.02.2011, бюл. № 4.

7. Съемный носитель информации с безопасным управлением доступом. Патент на полезную модель № 123571. 27.12.2012, бюл. № 36.

8. Съемный носитель информации на основе энергонезависимой памяти с расширенным набором функций информационной безопасности. Патент на полезную модель № 130441. 20.07.2013, бюл. № 20.

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

10. *Алтухов А. А.* Контроль доступа на основе атрибутов и оптимизация управления множеством АПМДЗ / Комплексная защита информации: материалы XX науч.-практ. конф., Минск, 19–21 мая 2015 г. — Мн.: РИВШ, 2015. С. 55—60.

11. Профиль защиты средства доверенной загрузки уровня платы расширения четвертого класса защиты ит.СДЗ.ПР4.ПЗ. Методический документ [Электронный ресурс]. URLhttp://fstec.ru/component/attachments/download/661 (дата обращения 10.04.2016).

12. Профиль защиты средства доверенной загрузки уровня загрузочной записи пятого класса защиты ИТ.СДЗ.З35.ПЗ. Методический документ [Электронный ресурс]. URL: http://fstec.ru/component/attachments/download/659 (дата обращения 10.04.2016).

13. Профиль защиты средства доверенной загрузки уровня загрузочной записи шестого класса защиты ИТ.СДЗ.336.ПЗ. Методический документ [Электронный ресурс]. URL: http://fstec.ru/component/attachments/download/660 (дата обращения 10.04.2016).

14. Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода четвертого класса защиты ИТ.СДЗ.УБ4.ПЗ. Методический документ [Электронный ресурс]. URL: http://fstec.ru/component/attachments/download/662 (дата обращения 10.04.2016).

15. СЗИ НСД "Аккорд-АМДЗ" [Электронный ресурс]. URL: http://accord.ru/accord.html (дата обращения 10.04.2016).

16. ПАК Аккорд-Win32(TSE) и ПАК Аккорд-Win64(TSE) [Электронный ресурс]. URL: http://www.accord.ru/acwin32.html (дата обращения 10.04.2016).

17. ПАК СЗИ НСД Аккорд-X [Электронный ресурс]. URL: http://accord.ru/acx.html (дата обращения 10.04.2016).

18. ПАК Аккорд-В. [Электронный ресурс]. URL: http://accord.ru/accord-v.html (дата обращения 10.04.2016).

19. ГиперАккорд [Электронный ресурс]. http://accord.ru/hyper-accord.html (дата обращения 10.04.2016).

20. Программно-аппаратный комплекс "Аккорд-В" (версия 1.3) Руководство по установке [Электронный ресурс]. http://www.accord-v.ru/docs/Accord-V_Installation_Guide.pdf (дата обращения 10.04.2016).

21. Программно-аппаратный комплекс средств защиты информации от НСД для ПЭВМ (PC) "Аккорд-АМДЗ" (Аппаратный модуль доверенной загрузки). Руководство администратора. [Электронный ресурс]. http://www.accord.ru/docs/amdz/AMDZ_L_Admin_manual.pdf (дата обращения 10.04.2016).

22. Regestry [Электронный ресурс]. https://msdn.microsoft.com/en-us/library/ms724871.aspx (дата обращения 10.04.2016).

23. vSphere и vSphere with Operations Management [Электронный ресурс]. http://www.vmware.com/ru/products/vsphere/features/esxi-hypervisor (дата обращения 10.04.2016).

24. Using the initial RAM disk (initrd) [Электронный ресурс]. https://www.kernel.org/doc/Documentation/initrd.txt (дата обращения 10.04.2016).

25. *Li X. R.* A novel over writable and restoring solution of filesystem for NAND flash / 3rd International Conference on Information Technology and Management Innovation, ICITMI 2014; Shenzhen; China; 19, 20 July 2014; V. 631, 632. P. 1057—1060.

The secure boot and integrity control of archived data. Part and the whole. (*Review*)

A. A. Altukhov
Closed Joint Stock Company "OKB SAPR", Moscow, Russia

The article discusses the need to control the individual elements that make up the archives. Specific examples showing the relevance of the problem.

Keywords: secure boot, trusted boot module, trusted boot means, resident security component, trusted computing environment, trusted computing, integrity control.

Bibliography — 25 references. *Received June 26, 2016*