УДК 004

Концепция персонального устройства контроля целостности вычислительной среды

А. А. Алтухов
ЗАО «ОКБ САПР», Москва, Россия

Рассмотрен процесс обеспечения доверенной загрузки, и выявлена концептуальная особенность, учитывая которую можно реализовать более выгодное решение по обеспечению доверенной загрузки ОС для определенного класса задач. Предложена архитектура решения, и описано аппаратное устройство, обеспечивающее основную функциональность. Приведен класс целевых задач нового решения, и предложен пример возможной оценки целесообразности его использования.

Ключевые слова: парадигма доверенных вычислений, доверенная вычислительная среда, доверенная загрузка, модуль доверенной загрузки, сервера.

Вот уже четверть века можно наблюдать эволюцию парадигмы доверенных вычислительных систем. Если внимательно проследить динамику развития, то движущая сила прогресса в области обеспечения безопасности технологии обработки информации, — развитие информационных технологий. Конфликт действующей парадигмы доверенных вычислений и желания использовать новые возможности информационных технологий приводит к пересмотру и совершенствованию парадигмы доверенных вычислений.

Все начиналось с функционально-замкнутой среды (ФЗС). Спустя некоторое время в результате примирения информационных технологий и необходимости обеспечения безопасности появилась концепция изолированной программной среды (ИПС). Развитие концепции ИПС привело к доверенной вычислительной среде (ДВС). Развитие ДВС вылилось в концепцию доверенного сеанса связи (ДСС) или обеспечение временной доверенной среды для решения конкретных задач. Следует отметить, что ДСС хоть и является логическим продолжением ДВС, но не заменяет ее полностью, а лишь позволяет решать некоторый спектр задач, которые достаточно тяжело решаются в рамках ДВС [2].

Концепция ДВС на настоящий момент является основной парадигмой доверенных вычислений. В рамках этой концепции одной из основных задач обеспечения безопасности является обеспечение целостности вычислительной среды, где под целостностью вычислительной среды понимается стабильность работы в течение рассматриваемого периода времени в требуемом диапазоне состава объектов и процессов, их взаимосвязей и параметров функционирования [3].

Для создания ДВС обязателен резидентный компонент безопасности (РКБ). Одной из возможных реализаций РКБ является аппаратный модуль доверенной загрузки (АМДЗ). Доверенная загрузка — это загрузка операционных систем только с заранее определенных носителей после успешного завершения специальных процедур проверки целостности технических и программных средств ПК (с использованием методов пошагового контроля целостности) и аппаратной идентификации/аутентификации пользователя [1].

Обратим внимание на один интересный момент. В моменты времени, когда защищаемое средство вычислительной техники (СВТ) выключено, АМДЗ не обязательно должен находиться в составе СВТ. Перед стартом АМДЗ обязан быть в составе СВТ, после успешного завершения процесса доверенной загрузки (после создания доверенной среды) наличие АМДЗ в составе СВТ уже не является необходимым*. Иными словами, для обеспечения ДВС РКБ должен быть в составе СВТ лишь на момент старта СВТ. Во все остальные моменты РКБ не выполняет эту функцию. Учитывая вышеописанную особенность, вполне естественно использовать один РКБ для группы СВТ. Так как РКБ — это аппаратное устройство, встраиваемое в состав СВТ, то возникает вполне

Алтухов Андрей Андреевич, инженер-программист.
E-mail: altuhov@okbsapr.ru

Статья поступила в редакцию 14 июня 2014 г.

*Обратим внимание на тот факт, что в данном контексте подразумевается именно устройство *в качестве* модуля доверенной загрузки. На практике устройство, выполняющее функции модуля доверенной загрузки, может использоваться в ОС и для других задач, например, в качестве датчика случайных чисел, устройства электронной подписи или даже защищенного носителя, но все это не функции аппаратного модуля доверенной загрузки.

очевидное ограничение: невозможность использовать РКБ для выполнения своей функции более чем для одного СВТ в один момент времени. Следует отметить, что это ограничение является следствием более общего: поскольку РКБ — физическое устройство, для возможности его использования на разных СВТ необходимо осуществлять операцию "переноса" с одного СВТ на другое. Процесс "переноса" можно разделить на три части: деинсталляция, перенос и инсталляция. Будем исходить из предположения, что процессы инсталляции/деинсталляции являются взаимно обратными процессами и достаточно простыми (подключение/отключение в/из разъема СВТ). Очевидно, что для оценки "простоты" необходимо ввести соответствующую метрику. Выбранная метрика зависит от конкретных задач, в рамках которых нужно провести оценку. Следует отметить лишь тот факт, что любое действие (в частности деинсталляция/перенос/инсталляция) связанно с некоторыми затратами. В каких единицах измерять затраты — это уже вопрос к метрике. Можно измерять затраты в единицах времени, человекочасах или денежных единицах на один человекамесяц. Важен, тот факт, что чем меньше затраты тем "проще" операция. Иными словами "простота" операции — это количественно выраженные затраты чего-либо по абсолютной шкале. Процесс "переноса" РКБ с одного СВТ на другое так же связан с определенными затратами. Например, в качестве метрики будем брать затраченное время на выполнение операции. Несмотря на свою простоту, затраченное время на выполнение операции является довольно удобной метрикой. С одной, его достаточно легко померить или оценить из параметров системы (здесь и далее под системой СВТ будем понимать группу из N СВТ, для которых доверенную загрузку будем обеспечивать с помощью одного РКБ). С другой стороны, зная затраченное время, можно оценить и другие метрики, например, финансовые затраты на выполнение конкретной операции. Как отмечалось ранее, операции инсталляции/деинсталляции будем считать "много проще" (на выполнение нужно затратить много меньше времени), чем операцию "переноса". Не нарушая общность, будем считать, что операция "переноса" одинаково затратная для двух любых СВТ из системы СВТ. Предположим, что для того чтобы подряд совершить доверенную загрузку ОС на одном СВТ, также необходимо совершить операцию переноса. Общие затраты в период времени будут равняться произведению затрат одной операции "переноса" на количество этих операций (количество доверенных загрузок ОС на СВТ), совершенных в данный временной период.

Можно сделать вывод, что в качестве альтернативы существующей модели "NРКБ для NCBT" предлагается использовать новую модель "1 РКБ для NCBT" с ограничением "только последовательного использования", а также с дополнительными затратами на операции "переноса". Таким образом, использование модели "1 РКБ для NCBT" возможно лишь в задачах, не требующих одновременного включения 2 и более СВТ. Эффективное использование модели "1 РКБ для NCBT" возможно лишь при небольших* затратах на операции "переноса".

Рассмотрим актуальную задачу, для решения которой возможно использовать новый вариант РКБ в рамках модели "1 РКБ для NCBT".

На настоящий момент времени большой процент СВТ, требующих защиты, является серверными машинами. Для серверов характерны два момента, связанных с их эксплуатацией:

– временной интервал одного сеанса работы сервера (от включения до выключения) в среднем является долгим (как минимум по отношению к длине сеанса работы ПК);

– физическое обслуживание серверов — задача не из простых, поэтому для серверов характерно групповое физическое расположение в одном месте (серверные).

Выдвинем два предположения, являющихся следствием вышеописанных особенностей эксплуатации серверов:

- инициация сеанса работы СВТ типа сервер — не частая процедура;
- территориально близко (в пределах одного помещения) расположены несколько СВТ.

Поставим задачу — обеспечить ДВС для всех СВТ. Безусловно, решение данной задачи возможно с помощью установки АМДЗ в каждый СВТ, но попробуем предложить решение, учитывая специфику именно этой задачи.

Обратим внимание, что из первого предположения следует тот факт, что количество операций "переноса" (в среднем равное количеству доверенных загрузок ОС на одном СВТ, которое не превосходит количество включений/перезагрузок СВТ, умноженное на количество серверов) является небольшим числом.

Из второго предположения можно сделать вывод о небольшом времени, затрачиваемом на одну операцию "переноса", так как время, затрачивае-

* Для того чтобы судить о величине затрат, необходимо их с чем-то сравнивать. Один из возможных вариантов — это сравнить затраты на операцию "переноса" со стоимостью покупки и обслуживания NРКБ из модели "N РКД для NCBT".

мое на операцию "переноса", прямо пропорционально расстоянию между СВТ.

Учитывая все вышесказанное, можно заключить, что общие затраты на операции "перенос" в рамках конкретной задачи вполне могут быть небольшими. При этом одновременный старт одного и более серверов не является необходимым. В итоге получаем реальную задачу, в рамках которой вполне применима модель "1 РКБ NСВТ".

Определившись с ограничениями, в которых применим новый вариант РКБ, и, описав конкретную актуальную задачу, необходимо понять, что из себя должен представлять РКБ, работающий в предложенной новой модели. Какую функциональность он должен обеспечивать? Каково его физическое устройство?

Физически устройство представляет собой автономно функционирующее высокозащищенное примитивное подключаемое к СВТ посредством интерфейса USB* устройство, обладающее защищенной памятью, доступ к которой осуществляется через активный элемент (контроллер).

Для возможности обеспечения доверенной загрузки устройство, обеспечивающее ее, должно, как минимум, провести все необходимые проверки, которые осуществляет АМДЗ, а именно:

- контроль целостности технических средств компьютера;
- контроль целостности программных средств (файлов системного и прикладного ПО).

Одна из задач проектируемого устройства — это возможность использовать его на разных СВТ. Для решения этой задачи устройство должно быть мобильно, т. е. иметь возможность быстрого и удобного переноса с одного СВТ на другое. Свойство мобильности обеспечивается за счет небольших размеров, USB-интерфейса и функциональной возможности работать с несколькими СВТ, без перенастраивания каждый раз с нуля.

Для удобства в дальнейшем будем именовать описываемое устройство мобильным устройством контроля цельности (МУКЦ).

Будем считать, что в пределах поставленной задачи МУКЦ будет рассчитан на одного пользователя, задача которого инициировать старт процедуры создания ДВС на сервере, что логично, так как обычно старт сервера — это задача одного человека (администратора). Таким образом, нет необходимости поддерживать огромное число** пользователей, как это реализовано в АМДЗ. Достаточно всего двух: одной пользовательской учетной записи (оператор, инициирующий старт процедуры создания ДВС с помощью МУКЦ) и одной учетной записи администратора (администратор безопасности, настраивающий МУКЦ и проводящий аудит деятельности оператора).

То, что МУКЦ, в отличие от АМДЗ, должно обладать возможностью работы с несколькими СВТ, влечет за собой еще одну отличительную особенность МУКЦ от АМДЗ: база данных контроля целостности (БД КЦ) должна предусматривать возможность работы с несколькими СВТ. В данном случае можно утверждать, что МУКЦ реализует подход противоположный АМДЗ. Если для АМДЗ нормальным является одно СВТ и много пользователей, то для МУКЦ — один пользователь и много СВТ.

Для МУКЦ появляется новая нехарактерная для АМДЗ сущность — профиль СВТ. Фактически профиль СВТ — это БД КЦ для одного определенного СВТ с набором атрибутов, необходимых для идентификации профиля и сопоставления каждого профиля своему СВТ.

Все необходимые события, так же как и в АМДЗ, должны заноситься в журнал.

Для понимания общей концепции работы устройства перечислим и кратко охарактеризуем режимы работы устройства.

Базовый режим — в данном режиме доступна только та часть памяти устройства, с которой осуществляется загрузка основного ПО МУКЦ. Память доступна только на чтение. Также должна быть предусмотренная операция добавления* в журнал.

После старта СВТ и передачи управления МУКЦ, последнее находится в Базовом режиме. В данном режиме проходят все необходимые проверки самотестирования и пользователю предлагается пройти процедуру аутентификации в устройстве, выбрав желаемый пользовательский режим и введя пароль (ПИН-код) **.

Непривилегированный режим — в данном режиме доступными на чтение становятся БД КЦ и список профилей СВТ. Пользователю предлагается выбрать профиль СВТ, на котором в данный

---

* На сегодняшний день USB интерфейс является стандартом де-факто для подключения мобильных устройств к СВТ.

** Данное ограничение чисто идеологическое. Нет никаких, технических ограничений поддержать возможность работы большего числа пользователей.

* Важно, что возможность добавления в журнал не является доступом к области журнала на запись.

** Аппаратная идентификация не предусмотрена в силу ее избыточности, по той причине, что в силу мобильности устройства нет необходимости пользователю оставлять его в составе СВТ, так как всегда есть возможность после завершения сеанса работы физически извлечь устройство. Хотя технически нет никаких препятствий предусмотреть аппаратную идентификацию пользователей.

момент он инициирует процесс проверки целостности среды. После выбора профиля устройство проводит необходимый контроль целостности и в случае успеха передает загрузку на заранее определенное загрузочное устройство. Если какие-либо проверки оказались не успешны, то сообщается о нарушении целостности и происходит перезагрузка или выключение СВТ.

В привилегированном режиме — после аутентификации появляется возможность перейти к редактированию списка профилей СВТ, где можно добавить новый профиль СВТ (предполагается, что в момент создания работа ведется именно на нем), удалить ненужный или выбрать необходимый профиль СВТ из списка, а после завершения проверок контроля целостности (в отличие от пользовательского режима) существует возможность перейти в среду администрирования, где можно управлять настройками МУКЦ и редактировать СКЦ для выбранного профиля СВТ.

Поскольку устройство, проводящее контроль целостности, не установлено все время в СВТ, обеспечение ДВС и дальнейшей работы в ней возможно только при запуске СВТ с установленным устройством и прохождении всех необходимых проверок.

В общем случае у пользователя есть, как минимум, техническая возможность загрузить СВТ без МУКЦ. В этом случае ДВС не обеспечивается, т. е. нельзя использовать средства, требующие ДВС.

Если пользователь добросовестный,* то никаких проблем не возникает, доступ к СВТ посторонних личностей ограничен (обычно в серверные доступ разрешен для ограниченного числа лиц), а пользователь не запускает СВТ без МУКЦ. Что же делать в случае, когда пользователей недобросовестный?**

Необходимость наличия МУКЦ в составе СВТ при старте возможно обеспечить как организационными, так и техническими мерами.

Один из возможных вариантов решения заключается в добавлении в СВТ свойства невозможности физического запуска СВТ без подключенного МУКЦ и невозможности передачи управления на устройство загрузки, отличное от МУКЦ. Выработка методов и технологий, позволяющих решать данную проблему, выходят за рамки данной статьи, но следует отметить, что МУКЦ совместно с реализацией данной технологии позволяет получить новый (непривычный) вариант мобильного аппаратного модуля доверенной загрузки.

Логическим развитием вышеописанного способа является обеспечение невозможности использовать решения, требующие ДВС, в случае, если не была обеспечена ДВС. Таким образом, даже если пользователь загрузит СВТ без МУКЦ (иными словами, без создания ДВС), он не сможет навредить ни себе, ни другим (за исключением, быть может, того, что, модифицировав среду, добьется того, что при следующей попытке доверенной загрузки процедуры контроля целостности, проводимые МУКЦ, закончатся неудачей, и придется проводить работы по восстановлению среды).

Технические меры, способные обеспечить невозможность работы пользователя вне доверенной среды, безусловно, важны, но можно обойтись и организационными мерами. Примером может служить регламент старта СВТ ("правильная" последовательность действий).

В случае если контроль процедуры запуска СВТ полностью осуществляется организационными мерами, то необходимо иметь средство мониторинга деятельности персонала. Иными словами, должна быть предусмотрена возможность индикации нарушения процедуры старта СВТ с возможностью идентификации сотрудника, нарушившего процедуру.

Нарушение процедуры старта СВТ можно установить, сравнив записи событий безопасности в журнале МУКЦ с записями журнала стартов СВТ, где отмечены дата и идентификатор сотрудника, запустившего СВТ. Если для конкретного события запуска СВТ в журнале МУКЦ не удается найти необходимые записи событий безопасности в момент времени, соответствующий старту, т. е. все основания полагать, что имело место нарушение процедуры старта СВТ конкретным пользователем. Данная информация может послужить доказательной базой для применения различного рода санкций к сотруднику, нарушившему регламент.

Следует отметить, что предлагаемое устройство без вышеописанных организационных и/или технических дополнений не является аппаратным модулем доверенной загрузки (именно по этой причине в статье оно именуется устройством контроля целостности). Данное устройство является выделенной основной составляющей АМДЗ.

Рассмотренная прикладная задача — не единственная, для которой удачное решение может быть построено на базе МУКЦ.

Обратим внимание на тот факт, что свойство "территориальная близость" рассмотренной группы СВТ часто эквивалентно свойству "принадлежат одному владельцу" или "обслуживаются од-

* Под добросовестным пользователем будем подразумевать пользователя, который не запускает СВТ без МУКЦ.

** Под недобросовестным пользователем будем понимать не только пользователя сознательного нарушающего регламента, но пользователя нарушающего регламент из-за ошибки или не внимательности.

ним администратором". Если учесть последнюю особенность, то выше предложенная задача «про серверы» может быть несколько видоизменена. МУКЦ можно использовать для возможности доверенного запуска ОС, на нескольких терминальных клиентах, что может быть весьма удобно, если пользователь работает (обслуживает) на нескольких станциях.

Еще одной возможной задачей может быть обеспечение доступа к "неперсональным" рабочим станциям или терминалам доступа. Конкретным примером может служить идеология, по которой работники той или иной сферы (например здравоохранения) должны иметь возможность производить необходимые операции на любом произвольном СВТ на территории предприятия.

Основной принцип работы МУКЦ следующий: если в определенный момент времени была настроена ДВС и зафиксированы все необходимые параметры, гарантирующие целостность технологии обеспечения ДВС, то в случае проверки целостности данных параметров гарантировано обеспечение ДВС.

Литература

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

2. *Конявский В. А.* Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем — на старт, внимание, МАРШ!// Комплексная защита информации. Сборник материалов XV Междунар. научн.-практич. конф. (1—4 июня 2010 г., Иркутск (Россия)). — М., 2010. С. 166—169.

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

The idea of personal device to monitor integrity of computer environment

A. A. Altukhov
OKB SAPR JSC, Moscow, Russia

The article discusses the process of providing trusted boot and reveals conceptual feature, which can be used to createmore profitabledevice for special cases. The author has proposed architecture of solution and has described the base device. The author has proposed typical cases for new solution and has offered an example of possible assessment of practicability.

Keywords: trusted computing paradigm, trusted computer environment, trusted boot, trusted startup hardware module.

Bibliography — 3 references. *Received June 14, 2014*