УДК 004.3

Привязка облака к земле

Д. Ю. Счастный
ЗАО «ОКБ САПР», Москва, Россия

Рассмотрены сходства и различия задачи обеспечения доверенной вычислительной среды на компьютерах пользователей, использующих ресурсы облачных инфраструктур, и в привычных корпоративных информационных средах. Предложен подход с использованием мобильных средств обеспечения доверенной загрузки как наиболее отвечающий мобильному характеру клиентского рабочего места при применении облачной инфраструктуры.

Ключевые слова: доверенная загрузка операционной системы, аппаратный модуль доверенной загрузки, средства доверенной загрузки.

Как театр начинается с вешалки, так и защита облачной инфраструктуры начинается с обеспечения доверенной среды на компьютерах пользователей. Безусловно, облачная инфраструктура является огромной мощной системой, которая объединяет множество сложных подсистем. Не вызывает сомнения тот факт, что в театр люди ходят не для того, чтобы пообщаться с гардеробщиком. Но зачастую отсутствие внимания организаторов театрального зрелища к подобным околотеатральным мелочам смазывает общее впечатление от выхода в театр. И если в театре подобное невнимание в худшем случае приведет к испорченному настроению зрителей, то работа пользователей в недоверенной среде с облачной инфраструктурой может привести к утечкам пользовательских данных и даже к финансовым потерям пользователей.

Типичным заблуждением является мысль о том, что если данные хранятся и обрабатываются в облаке, то защищать клиентские места не нужно. Это заблуждение присуще и организаторам облаков, и пользователям. Да, данные хранятся и обрабатываются в облаке, но пользователь с ними работает со своего рабочего места, он данные получает из облака, как-то их использует и сохраняет обратно в облако. Процесс изменения данных, переход их из одного состояния в другое производит пользователь на своем рабочем месте. И именно здесь важно обеспечить корректность функционирования программного обеспечения: пользователь должен работать именно с тем программным обеспечением, которое правильно подключится к нужного облаку, корректно визуализирует получаемые из облачной инфраструктуры данные, правильно обработает вводимые пользователем данные и сохранит результат именно в том облаке, в котором необходимо. Сбой на любом из перечисленных выше этапов может привести к утечкам пользовательских данных, даже несмотря на то, что облако защищено в центре. На компьютерах пользователей должна быть создана доверенная среда.

Самым простым и надежным средством обеспечения гарантии того, что клиентское программное обеспечение осталось неизменным и соответствует эталону, является Аппаратный модуль доверенной загрузки (АМДЗ). АМДЗ — это специализированный контроллер, устанавливаемый в слот расширения материнской платы компьютера (в настоящее время чаще всего для этой цели используются слоты PCI-Express и mini PCI-Express), стартующий до загрузки операционной системы компьютера и самостоятельно проводящий процедуры контроля целостности программного (исполняемых и конфигурационных файлов, реестра, документов и т. д) и аппаратного (состав жестких дисков, их настройку, наличие плат расширения и т. д.) обеспечения. Дополнительно АМДЗ проводит аппаратную (с помощью ТМ-идентификатора или смарт-карты) идентификацию пользователя с последующей аутентификацией по паролю. Применение АМДЗ удобно для пользователя (он привычно прислоняет смарт-карту и вводит пароль) и необременительно для администратора (достаточно один раз настроить контроллер и он каждый день надежно и быстро происходит все контрольные процедуры, обеспечения корректную и безопасную работу компьютера с настроенной пользовательской средой). Стартуя до запуска операционной системы клиентского рабочего места, АМДЗ позволяет создать доверенную среду на

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

Статья поступила в редакцию 14 июня 2014 г.

компьютере пользователя. АМДЗ широко применяется в корпоративной среде и его также можно применять в облачной инфраструктуре.

Необходимость применения АМДЗ глубоко проработана в научных трудах [1—3] и подтверждается давней практикой применения. Настолько глубоко и давно, что ФСТЭК разработал и выпустил отдельный документ, посвященный требованиям к средствам доверенной загрузки (СДЗ) [3]. В этом документе подробно рассматриваются различные типы СДЗ, выделяются классы их защиты, специфицируются профили защиты СДЗ. При всем описываемом многообразии и различиях СДЗ их объединяет одно общее свойство — считается, что они должны быть постоянно установлены в защищаемые компьютеры. Но для обеспечения доверенной загрузки и последующего создания доверенной среды зачастую достаточно применения мобильных средств защиты, в частности, средства защиты информации от несанкционированного доступа "Инаф" или средств обеспечения доверенного сеанса связи (СОДС) "МАРШ!".

Отличий "Инафа" от АМДЗ ровно два: он устанавливается в usb-разъем компьютера, а не PCI-Express, и идентификация/аутентификация пользователя здесь является опцией. Остальной функционал этих устройств одинаков, т. е. с помощью "Инафа" можно также проверить целостность программного и аппаратного обеспечения компьютера и создать доверенную среду на компьютерах пользователей облачной инфраструктуры. Мобильность, которая присуща "Инафу", позволяет реализовывать разнообразные сценарии работы корпоративных пользователей с облаками без снижения общего уровня защищенности клиентских мест. В частности, можно позволить пользователю быть не привязанным к конкретному рабочему месту в пределах офиса. Для этого достаточно создать в пользовательском устройстве "Инаф" набор контролируемых компьютеров и обеспечить на этих компьютерах доступ к корпоративному облаку. При включении любого такого компьютера пользователь должен будет подключить "Инаф" в usb-порт компьютера свое устройство, оно получит управление до старта основной операционной системы, выполнит все необходимые контрольные процедуры и в случае их успешного завершения предоставит пользователю защищенный доступ к корпоративному облаку.

"Инаф" позволяет пользователю стать мобильным, но только в пределах офиса. СОДС "МАРШ!" позволяет расширить границы мобильности далеко за пределы офиса за счет изменения логики контроля неизменности программного обеспечения и соответствия его эталону. Суть решения СОДС "МАРШ!" состоит в том, что пользователь носит с собой не средство контроля целостности среды, а саму среду в недоступном для изменения виде. У пользователя есть устройство с интерфейсом usb размером со стандартную флешку. И по сути своей являющееся флешкой, но имеющей ряд особенностей. Во-первых, с этого устройства можно загружать компьютер. Во-вторых, операционная система, которая будет загружаться на компьютере, хранится на диске в режиме "только для чтения". В-третьих, в этой операционной системе предустановленно все необходимое программное обеспечение для доступа к облачной инфраструктуре как на прикладном, так и системном уровне. Таким образом, корпоративные пользователи облачной инфраструктуры могут с любого компьютера работать с облаком из доверенной среды.

Создание корпоративного облака, равно как и создание театра, — сложный, трудоемкий, длительный процесс, закладывающий фундамент для последующего еще более сложного, не менее трудоемкого и гораздо более продолжительного процесса эксплуатации. И для того, чтобы процесс эксплуатации облака был успешным (равно как и театр был популярным), мало создать ЦОДы, организовать правильное управление их защитить. Нужно предоставить пользователям удобное и защищенное средство доступа к этому облаку, чтобы пользователи могли комфортно и безопасно получать необходимые им услуги. А не сидели в шубах на галерке.

Литература

1. *Конявский В. А.* Управление защитой информации на базе СЗИ НСД "Аккорд". — М.: Радио и связь, 1999. — 325 с.
2. *Конявский В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией. — Минск: Серия «Библиотека журнала "УЗИ"», 2004. — 327 с.
3. Требования к средствам доверенной загрузки, утвержденные приказом ФСТЭК России от 27 сентября 2013 г. № 119 (зарегистрирован Минюстом России 16 декабря 2013 г., рег. № 30604).

Clouds attached to the land

D. Yu. Schastny
OKB SAPR JSC, Moscow, Russia

The article is devoted to the differences and the commons between trusted computing environment building task in cloud infrastructures and corporative information systems of different types. The approach based in mobile trusted startup tools using is offered as the mostly convenient to the mobile character of client workplace usual for cloud systems.

Keywords: trusted boot, trusted startup hardware module, trusted startup tools.

Bibliography — 3 references. Received June 14, 2014

* * *