УДК 004.3

Доверенная вычислительная среда на планшетах Dell. "МАРШ!"

В. В. Кравец
Федеральное государственное унитарное предприятие «Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации»,
ЗАО «ОКБ САПР», Москва, Россия

Предложен способ организации доверенной вычислительной среды, доверенной загрузки и доверенного сеанса связи на планшетных компьютерах Dell с использованием устройства "МАРШ!". Рассмотрены основополагающие принципы, использованные в данной модели решения.

Ключевые слова: "МАРШ!", доверенная загрузка, доверенный сеанс связи, Windows Embedded, планшет.

Планшетный компьютер уже давно перестал быть редкой и уникальной вещью. Чем больше людей его используют, тем шире круг задач, которые нужно выполнять с помощью планшета. Времена, когда планшеты использовались исключительно для игр, прошли — теперь это полнофункциональный рабочий инструмент. Планшет по форм-фактору — **миникомпьютер**, но это не означает, что его достаточно защищать "**мини-защитой**".

Планшет не привязан к конкретному месту, а значит, физическая охрана и большинство организационных мер не поможет.

Планшет изначально задуман как неизменяемая аппаратная платформа, поэтому установить в него что-либо (например, защитную плату) самостоятельно нельзя, да и места под нее не предусмотрено.

Планшет изначально задуман как инструмент максимально комфортного построения персональной вычислительной среды, поэтому никаких встроенных ограничений на скачивание и установку любых программ и данных в нем нет и быть не может, наоборот, огромная бизнес-инфраструктура поощряет пользователя постоянно "улучшать" свое программное окружение, иногда даже не заботясь о том, чтобы ставить его в известность об этих улучшениях.

Следовательно, добиться ситуации, чтобы "родная" вычислительная среда планшета была доверенной в любой момент времени, невозможно. Но раз ее нельзя создать, то ее можно привнести извне. Именно такой подход и использует программно-аппаратный комплекс "МАРШ!".

Кравец Василий Васильевич, аспирант, программист.
E-mail: vkravec@okbsapr.ru

Статья поступила в редакцию 14 июня 2014 г.

С точки зрения железа, "МАРШ!" — это микроконтроллер, позволяющий осуществлять криптографические операции, и внешняя память с управляемым доступом. В этой памяти размещается эталонный образ операционной системы, и аппаратно запрещаются любые изменения. Пользователь, загрузившись с устройства "МАРШ!", гарантированно получает исходную эталонную среду, даже если в ходе предыдущего сеанса работы он ее как-то модифицировал (вольно — установив что-либо сознательно, или невольно — подцепив где-то вирус).

Данная операционная система изолирована от той среды, которая изначально находится в планшете. Это означает, что "МАРШ!" не может повлиять на ту среду, что в планшете, и "родная" операционная система не повлияет на "МАРШ!". Т. е. пользователь может без ограничений использовать любые "небезопасные" ресурсы, устанавливать любые программы и вообще "делать все, что нельзя", но как только он подключает "МАРШ!" и загружается с него, он снова получает "стерильную" среду, на которую никак не влияют все "улучшения", привнесенные в основную систему. При этом работа в ОС, загруженной с "МАРШ!", не окажет влияния на изменения основной ОС, когда он отключит "МАРШ!", все они будут в силе, ничего не "сбросится".

Типовое применение мы видим в том, что, загрузившись с устройства "МАРШ!", пользователь получит возможность в защищенных условиях установить удаленное соединение с нужным ему сервером (терминальный сервер, ферма виртуальных машин, Web-приложение) и спокойно поработать, не беспокоясь о вирусах, недоверенных компонентах и прочих потенциально вредоносных факторах, гарантировать отсутствие которых на своем планшете он в общем случае не может. Такой подход мы называем **доверенный сеанс связи.**

Планшеты Dell с операционной системой Windows 8 идеально подходят для бизнес-задач. В первую очередь это связано с тем, что почти все бизнес-приложения реализованы под операционную систему Windows, и на планшете можно использовать ровно те же самые приложения, не ожидая когда их портируют на Android, пользоваться привычным интерфейсом, кроме того, в планшетах Dell есть 3G модуль, что отвязывает пользователя от необходимости находиться в зоне действия Wi-Fi сети. Чтобы сохранить это преимущество, в качестве эталонной операционной системы в устройстве "МАРШ!" используется **Microsoft Windows Embedded 8 Standard**.

Это модульная операционная система бинарно совместима с Windows 8. Модульность подразумевает то, что можно выбрать только необходимые для работы компоненты, исключив лишнее. Чем меньше количество компонентов, тем проще проверить исходный образ на отсутствие уязвимостей. Бинарная совместимость приложений означает, что все те приложения, которые запускаются на Windows 8, запустятся и на WE8S, разрешая, таким образом, например, работу "толстым" клиентам приложений.

Заметим, что выбор операционной системы зависит не только от желания пользователей, но и от возможностей используемой аппаратной базой. В планшетах из-за их форм-фактора зачастую используются довольно специфические компоненты, для которых бывает довольно сложно найти соответствующие драйверы. Производитель планшета обычно решает эту задачу прозрачно для пользователя — последний получает готовый продукт, в котором все работает. Но если запускать на этом устройстве другую ОС, то надо быть готовым к решению проблем совместимости с комплектующими. Нельзя на 32-битном процессоре запустить 64-битную операционную систему. Да и отсутствие, например, Wi-Fi модуля пользователя не обрадует. Выбирая для "МАРШ!" ОС, бинарно совместимую с изначальной ОС планшета, мы заведомо получаем систему, для которой можем обеспечить работоспособность всех ее составляющих.

Сценарий работы при использовании планшета Dell, укомплектованного устройством "МАРШ!", выглядит примерно так.

Пользователь работает без подключения устройства так, как он привык, без ограничений.

При необходимости решения задачи, для которой требуется доверенная вычислительная среда, например, подключение к корпоративной почте или терминальному (физическому или виртуальному) серверу, обрабатывающему информацию ограниченного доступа, или виртуальному рабочему месту, пользователь подключает "МАРШ!" и загружается с него.

В привычном программном окружении пользователь стартует защищенную сессию с необходимым ему ресурсом и выполняет необходимые операции.

Важно, что если удаленный ресурс, к которому подключается пользователь, защищен ПАК СЗИ НСД "Аккорд", то "МАРШ!" может выступать в роли аппаратного идентификатора пользователя в "Аккорде". Но при необходимости может быть поддержано и использование других идентификаторов.

После завершения выполнения задачи, требующей защищенного режима, пользователь отключает "МАРШ!" и возвращается в привычную, незащищенную среду.

Представляется, что в условиях заметной потребности рынка в решении, сочетающем удобство планшетов с защищенностью классических рабочих мест, планшет Dell с устройством "МАРШ!" является оптимальным решением, не изображающим принятие защитных мер, а обеспечивающее безопасность работы.

Trusted computing environment solution on the Dell's tablet PCs. "MARSH!"

V. V. Kravec
All-Russia Scientific Research Institute of Computer Technology and Informatization Problems , OKB SAPR JSC, Moscow, Russia

The article presents approach to trusted computing environment, trusted startup and trusted communication session on the Dell's tablet PCs using device "MARSH!". Paper introduces core principles of trusted startup that were used in the described solution model.

Keywords: "MARSH!", trusted startup, trusted communication session, Windows Embedded, tablet pc.

Received June 14, 2014