Не надо оплачивать уязвимости

Текст: Валерий Конявский, д.т.н., профессор НИУ ВШЭ и НИЯУ МИФИ, зав. кафедрой «Защита информации» МФТИ (ФизТех), научный руководитель ФГУП ВНИИПВТИ, научный консультант ОКБ САПР.

Уязвимость – это обратная сторона универсальности. Именно поэтому пропадают вещи из ячеек камеры хранения. Именно поэтому возможен угон автомобиля, именно поэтому нельзя использовать обычные флешки в качестве служебных носителей.

Все усилия, предпринимаемые по защите или охране чего-либо, сводятся к тому, чтобы сделать предмет защиты менее универсальным – чтобы к замку подходил не любой ключ, чтобы машину мог открыть и завести не любой водитель, чтобы флешка работала не на всех компьютерах и в руках не любого пользователя.

Валерий Конявский

Уязвимая архитектура

Все современные средства вычислительной техники (СВТ, компьютеры) разработаны как универсальные вычислительные машины, которые частично (с конечной памятью) моделируют машину Тьюринга, «универсальный исполнитель». Это не только дает нам псевдо неограниченные возможности (принципиально выполнима любая задача – хватило бы времени и памяти), но и толкает на экстенсивный путь развития. Не хватает памяти – добавим. Не хватает времени – увеличим тактовую частоту, количество ядер, виртуализируем ресурсы, наконец.

Пытаясь защититься от вредоносных хакерских программ, человечество уже более 60-ти лет разрабатывает программы, традиционно относимые к области защиты информации – средства идентификации, аутентификации, авторизации, контроля целостности, антивирусные программы, криптографические средства и так далее. Использование этих средств отчасти приносит положительный эффект, но очень и очень отчасти.

Если универсальная машина выполняет любые программы, то, очевидно, она выполнит и вредоносную программу. Универсальность обеспечивается архитектурно, самой «конструкцией» машины Тьюринга, как мыслимой в абстракции, так и реализованной на практике, то есть машина Тьюринга архитектурно уязвима. Архитектурно уязвимы и все виды компьютеров, которые мы используем, потому что они разрабатывались так, чтобы быть максимально универсальными. Мы эксплуатируем компьютеры, а хакеры – эксплуатируют эту уязвимость. Этой уязвимостью мы платим за универсальность наших компьютеров.

Все имеет свою цену. Однако есть один очень существенный нюанс: в большинстве случаев нам не нужна универсальность компьютера. Для чего универсальная машина, способная выполнить любую задачу, например, в банкомате? Разве не должен компьютер в банкомате, напротив, выполнять строго ту задачу, которая ему предписана, и больше ничего?

Банкомат (с точностью до модели) устроен очень просто. В его составе есть диспенсер (в нем лежат деньги и из него деньги выдаются), компьютер и периферийное оборудование. Компьютер взаимодействует с процессинговым центром (например, по IP-протоколу), и USB-кабелями соединен с диспенсером и другим периферийным оборудованием.

При работе с банкоматом с пластиковой карты считывается ее номер, с клавиатуры – PIN, все это передается в процессинговый центр, где и выполняется авторизация. Если все в порядке – проверяется запрашиваемая сумма. Затем компьютером банкомата формируется команда на выдачу денег, которая передается в диспенсер.

Сейчас это – обычный x86-компьютер с ОС Windows. Конечно, и то, и другое можно использовать, но это не лучший выбор.

Разве для выполнения простейших операций нужен мощный универсальный компьютер?

Разве надежности бытового компьютера хватает для выполнения финансовых операций?

Конечно, если произошел сбой, ничего не мешает перезагрузить бытовой компьютер, но что, если перезагрузка этого бытового компьютера, используемого в банкомате, придется как раз на время Вашей операции?

Это пример крайний, однако, он иллюстрирует ключевой момент – для решения профессиональных задач целесообразно использовать профессиональный инструмент, а не универсальную палку-копалку.

Это значит, что мы не должны платить уязвимостью за универсальность наших служебных СВТ, так как в их универсальности мы не заинтересованы.

Вывод очевиден, компьютеры должны быть разделены на универсальные и специальные. И разделены не организационно (назначением одних такими, а других – другими), а технически.

Поскольку архитектуру нельзя изменить программно, то никакие программные средства не помогут нам надежно защититься от хакеров, эксплуатирующих архитектурную уязвимость. Игра «кто кого» продолжается уже много лет, давая работу сотням тысяч специалистов по информационной безопасности, но не спасая нас от потерь.

Как закрыть архитектурную уязвимость?

Если уязвимость в архитектуре – то и совершенствовать нужно архитектуру.

Классическими являются две архитектуры – архитектура фон-Неймана, и гарвардская архитектура. Примером первой являются практически все настольные компьютеры, примером второй – практически все планшетные компьютеры и телефоны.

Отличительной особенностью архитектуры фон-Неймана является то, что команды и данные не разделяются, они передаются по единому общему каналу.

Гарвардская архитектура предполагает наличие разных каналов для команд и данных.

Такая схема взаимодействия требует более сложной организации процессора, но обеспечивает более высокое быстродействие, так как потоки команд и данных становятся не последовательными, а параллельными, независимыми.

Однако, и в случае компьютера фон-Неймановского типа, и компьютера с гарвардской архитектурой организация потоков команд и данных таковы, что архитектурная уязвимость присуща каждому из них. Гибкость, универсальность и в одном, и в другом случае обеспечивается возможностью изменения потока команд и потока данных – независимо от того, в одной памяти они лежат, или разделены. В свою очередь, возможность изменения команд и данных создает и возможность для несанкционированного вмешательства вредоносного программного обеспечения – это и есть основная архитектурная уязвимость, которая блокируется использованием сложных и довольно дорогих СЗИ.

Предложенная нами «новая гарвардская» архитектура отличается тем, что в ней используется память, для которой установлен режим «только чтение».

Конечно, в реальных компьютерах все немного сложнее, но в целом такой режим обеспечивает неизменность ОС аппаратным, физическим способом, а значит, никакие программные действия хакеров не смогут нарушить целостность, а, следовательно, доверенность программной среды. Дополнительным преимуществом такого подхода является то, что вирус не может зафиксироваться в долговременной памяти компьютера, которая функционирует в режиме read only, то есть нет необходимости использовать антивирусные программы. Таким образом, существенно сокращается не только цена приобретения, но и цена владения изделием.

Нельзя не учитывать, что в процессе работы пользователю часто приходится использовать сведения, размещенные в недоверенных средах, например, в Интернете. Однако из доверенной среды нельзя выходить в незащищенный Интернет, так как в результате доверенность может быть нарушена.

Наилучшее разрешение этого противоречия – наличие еще одной ОС, незащищенной, без ограничений по доступу в Интернет. Носителем этой ОС может быть банк памяти с полным доступом.

Наличие на одном компьютере 2-х ОС требует возможности выбора той или иной ОС, в зависимости от потребностей пользователя. Выбор должен осуществляться пользователем. Целесообразно при этом выбор ОС осуществлять переключателем, размещаемом на корпусе устройства.

Условия сохранения доверенности защищенной ОС обеспечиваются тем, что разные ОС не имеют общих информационных ресурсов. Этим определяются следующие требования:

- при работе незащищенной ОС доступ к ПО защищенной ОС отсутствует как на программном, так и на аппаратном уровне;
- обновление защищенной ОС осуществляется только из доверенного источника, с обеспечением целостности и подлинности источника криптографическими методами (монтирование ПО осуществляется только после успешной проверки его электронной подписи, которой оно подписано).

Пример решения

Такое решение получено, и оно защищено уже 5 патентами с 16 пунктами патентных формул. Основанные на этом решении компьютеры выпускаются в виде планшетов, в форм-факторе большой флэшки, в виде телефона и в форм-факторе отчуждаемого активного блока и док-станции.

Линейка включает в себя варианты как с одной (только защищенной) ОС (подтип МКТ), так и с двумя ОС (защищенной и незащищенной) и переключателем (подтип МКTrusT).

Вариант МКТ с одной ОС подходит для сценариев применения, предполагающих работу только в защищенной среде, и ни в какой другой.

В тех же случаях, когда предполагается также применение устройства в частных целях, или служебные задачи предполагают необходимость использования данных из незащищенных ресурсов (допустим, картографической информации), целесообразно применение варианта МКTrusT с двумя ОС.

Микрокомпьютеры разработаны на базе 4-х ядерного Cortex-A9 процессора, причем в его состав включен мощный видеоускоритель, позволяющий воспроизводить файлы FullHD. Ниже приведены его технические характеристики.

CPU: на базе 1,6 ГГц CortexA9 Quard Core;

GPU: Mali400, 2D/3D OpenGL ES2.0/ OpenVG1.1;

RAM: 2GB DRR3;

Flash memory: 8GB ;

Мультимедиа форматы:

Аудио: MP3/WAV/AMR/AAC;

Видео: 3GP, MPEG4, AVI, RMVB, MKV, FLV и т. д.;

Декодирование видео: поддержка 1920x1080p@60fps;

Кодирование видео: поддержка записи в формат H.264 1080p@60fps, 720@100fps;

Поддержка Flash 11.x / HTML5 видео он-лайн;

Игры: встроенный 3D-Ускоритель;

и др.

В качестве примера рассмотрим компьютер МКТ-card long – это доверенный облачный микрокомпьютер с динамически изменяемой архитектурой.

Конструктивно он оформлен как док-станция с отчуждаемым компьютером.

Док-станция содержит 8 USB-портов, выход HDMI, сетевой разъем RJ-45, разъем питания.

Отчуждаемый микрокомпьютер из состава МКТ-card long с подключенной антенной WiFi

Док-станция из состава МКТ-card long с подключенной периферией. В пенале для ключей - отчуждаемый микрокомпьютер

Док-станция коммутируется с периферийным оборудованием через USB, с монитором через HDMI, с сетью – через RJ-45; возможно также использование WiFi при условии разрешения на его применение.

Параметры компьютера аналогичны остальным решениям линейки.

Активная часть компьютера МКТ-card long размещается в отчуждаемом модуле размерами 120*40*10, что позволяет хранить его в стандартном пенале для ключей.

Программное обеспечение размещено в памяти с физически устанавливаемым доступом read only (RO), что исключает его искажения и обеспечивает неизменность среды функционирования.

Функциональное ПО (ФПО) включает клиенты RDP и PC-over-IP, что позволяет обеспечить функционирование в облачной или терминальной инфраструктуре.

Встроены также средства разграничения доступа («Аккорд-ТК»), средства защищенного терминального доступа («Центр-Т»), средства «проброски» токенов и других периферийных устройств на удаленный рабочий стол.

Наличие собственной ОС и вычислительных ресурсов позволяет обеспечить низкую стоимость владения удаленным «облачным» рабочим столом любой необходимой производительности, высокую скорость и надежность загрузки, высокий уровень защищенности.

Обеспечение стабильности среды функционирования криптографии (СФК) позволяет встраивать и применять любые сертифицированные СКЗИ, предназначенные для работы в ОС Android и Linux.

В настоящее время в таком форм-факторе реализован именно МКТ, а не МКTrusT – решение с одной, а не двумя ОС, потому что предполагаемый сценарий использования – создание рабочих мест, не допускающих возможности для пользователей «заниматься своими делами». Однако никакой принципиальной невозможности реализации версии МКTrusT-card нет, если в ней будет выявлена потребность.

Решение для банкоматов

Другой важный сценарий применения отчуждаемого компьютера – это технологические машины, например, упомянутые уже ранее банкоматы.

Сегодня «доверенность» банкоматов обеспечивается только металлическим корпусом. И все. Встроенные камеры и многое другое помогает иногда при расследовании преступлений, но никак их не предотвращает.

Очевидно, что важнейшим является выбор компьютера для банкомата и операционной системы для компьютера.

Если говорить об ОС, то следует сказать, что у ОС Windows огромное количество преимуществ. Например, развитые и доступные большинству программистов средства программирования. Мощные графические средства. Работа с Интернетом и так далее. В общем, универсальность. Но что из этого необходимо для банкомата? Похоже, что здесь большинство преимуществ становятся недостатками. Применение огромной тяжеловесной ОС в банкоматах совершенно избыточно, гораздо целесообразнее здесь применять Линукс.

Очевидно, что и компьютер должен быть специальным, а не универсальным. То, как сейчас, в условиях использования универсального компьютера, производится обновление ПО банкомата, не пугает только тех, кто не знает, как это происходит. Намного защищеннее процедура станет при замене отчуждаемого компьютера целиком на заранее подготовленный в сервисном центре. В этом случае никто, кроме специалистов авторизованного сервисного центра, не сможет изменить состав ПО, даже если получит доступ к отчуждаемому компьютеру, отправленному на замену.

Представляется, что такое повышение защищенности технологического процесса недостижимо с применением универсального компьютера за приемлемую стоимость. В то же время применение компьютеров «новой гарвардской» архитектуры позволит это сделать без критически высоких затрат.

Под влиянием запросов реальности линейка компьютеров МКТ пополняется, ведь ее общая логика такова, что, комбинируя ключевые особенности разных устройств, можно добиться удовлетворения практически любой вообразимой потребности в отношении защищенного клиентского (не путать с «пользовательского») компьютера.

И не придется принимать дорогостоящие меры для блокирования уязвимостей универсальной архитектуры в тех случаях, когда в ней нет нужды.