*Елькин В. М., АО “Электроавтоматика”*

**Контроль недоверенного процессора**

    При проектировании современных доверенных систем, акцент, как правило ставится на том, чтобы тем или иным способом обеспечить защищенность компьютерной системы от влияния извне (инсайдер в этом смысле тоже влияет извне, так как находится снаружи от атакуемого компьютера).

Теоретических предпосылок для такого сужения трактовки доверенности вычислительной среды нет. «...Понятие “доверенная вычислительная система” (ДВС) было введено в [1] в развитие понятия «изолированная программная среда» (ИПС) [2]. Было показано, что ДВС — это система, все узлы которой аутентифицированы и целостность их установлена. Также было показано, что обеспечение целостности и аутентификация должны выполняться специальным средством, которое получило название «резидентный компонент безопасности» (РКБ), для которого были перечислены свойства, и доказана лемма о размещении РКБ в ДВС» [3].

Несмотря на очевидность утверждения о том, что в доверенной вычислительной системе *все* должно быть доверенным [там же], часто упускается из виду такая важная уязвимость, как недоверенный процессор. Существующими на сегодняшний день РКБ решить задачу защиты от влияния недоверенного процессора нельзя, так как их (РКБ) функциональность сосредоточена на защите, во-первых, ОС, а во-вторых, от несанкционированных воздействий извне, а не *изнутри*.

С точки же зрения угроз, привносимых в систему недоверенным процессором, ОС является фактором весьма второстепенным. Процессор может использовать ее уязвимости, но может обходиться и без них, используя другие каналы для организации утечки данных.

    В данной статье мы не будем касаться аппаратных закладок, направленных на умышленную порчу обрабатываемой информации, для обхода оных можно разработать программные алгоритмы коррекции и этого будет вполне достаточно. Куда интереснее будет рассмотреть вопрос защиты от аппаратных закладок, направленных на хищение информации и передачу ее третьим лицам.

Не секрет [4, 5], что на данный момент не существует доверенных отечественных процессоров достаточной производительности и разумной стоимости. Поэтому целесообразным решением будет все же построение системы таким образом, чтобы продолжать обрабатывать информацию на недоверенном процессоре, но при этом исключить утечку информации.

    Итак, для безопасной обработки информации, подлежащей защите, на недоверенном процессоре следует изолировать его при помощи доверенных средств для того, чтобы создать некоторого рода «песочницу» или своеобразную «клетку», исключающую возможность передачи данных в ее обход. А именно:

* с точки зрения исполняемого на процессоре кода на СВТ должна быть установлена доверенная ОС. Доверенная ОС в данном конкретном случае нужна для того, чтобы исключить возможность использования процессором уязвимостей самой ОС для хищения информации;
* с точки зрения контактов процессора с внешним миром – нужно чтобы они происходили через своего рода прослойку – РКБ, который будет проверять, возможно ли для процессора в данный момент времени совершить данную операцию или нет.

    РКБ в этой схеме необходим для контроля каналов обмена данными процессора с устройствами ввода/вывода.

Суть предлагаемого подхода сводится к тому, что в момент обработки информации, требующей защиты, после соответствующего сигнала от специализированного программного обеспечения система будет переводиться в защищенный режим и РКБ начнет принудительно отключать каналы обмена информацией и (возможно) дополнительно контролировать те, которые не должны быть отключены в данном режиме. При этом процессор, получая доступ к защищаемой информации, физически не способен передать ее во внешний мир в обход РКБ, который в свою очередь такую попытку пресечет. После завершения обработки информации, подлежащей защите, так же по команде из ОС система может быть переведена в незащищенный режим, в котором РКБ не накладывает никаких ограничений на работу процессора с периферией, что положительно сказывается на производительности и удобстве системы.

Некоторым аналогом (на функциональном уровне) этого способа можно считать “Ноутбук руководителя” [6, 7], однако данное решение не подразумевает ограничения работы процессора с периферией на аппаратном уровне, а соответственно не дает гарантии отсутствия утечки.

На данный момент не представляется возможным путем небольших изменений адаптировать для решения приведенной задачи какой-либо из существующих РКБ. Требуется разработка такой структуры построения СВТ, в которой РКБ будет подключен к шине и/или в разрыв каналов ввода/вывода информации.

При использовании такой схемы на РКБ нового типа может быть возложена также и роль привычных устройств защиты информации. Например при такой глубокой интеграции РКБ в схемотехнику СВТ для него не станет проблемой взять на себя функции аппаратного модуля доверенной загрузки (АМДЗ) и шире – средства доверенной загрузки (СДЗ) [8, 9]. Защищенный режим функционирования СВТ с таким РКБ отлично подойдет для защищенной работы с удаленным ресурсом в концепции доверенного сеанса связи (ДСС) [10, 11]. А в носимых исполнениях СВТ есть возможность возложения на РКБ функций идентификатора пользователя (токена) в случае применения в системах с соответствующей архитектурой.

    В заключении нужно отметить, что при построении отечественных защищенных систем зачастую используют не только недоверенный процессор, но и чипсет [4]. Описанный подход позволяет решить проблему путем расширения функционала РКБ для контроля не только процессора, но и чипсета, однако вопрос требует дополнительной проработки для корректного определения перечня компонентов чипсета и их связей, которые могут стать каналами утечки и поэтому подлежат контролю.

    Вторым “тонким” местом можно считать то, что на данный момент полный список каналов обмена информацией процессора с внешним миром до конца не сформирован (хорошей иллюстрацией этого может послужить [12]), хотя “проблема периферии” давно теоретически осознана [4, 13, 14. С. 809–811].

    Однако сформулированная концепция позволяет наметить возможное направление разработки группы решений для борьбы с озвученными уязвимостями, детали и даже архитектура которых могут зависеть от состава конкретной системы [15], ядро же защиты будет к нему инвариантно.

Список литературы:

1. *Конявский В. А.* Управление защитой информации на базе СЗИ НСД "Аккорд". М., 1999. – 325 c.
2. *Щербаков А. Ю.* Хрестоматия специалиста по современной информационной безопасности. Palmarium academic publishing. 2016. Том 1. – 265 c.
3. *Конявский В. А.* Доверенные системы как средство противодействия киберугрозам. Базовые понятия. // Information Security/Информационная безопасность. М., 2016. № 3. С. 40–41.
4. *Конявский В. А.* Компьютерная техника: плач по импортозамещению // Защита информации. Inside. Спб., 2017. № 5. С. 26–29.
5. *Елькин В.М., Счастный Д.Ю.* Гарантированное отключение периферии: общая постановка задачи // Вопросы защиты информации. 2017 №4, С. 55–57.
6. *Счастный Д. Ю.* Ноутбук руководителя // Комплексная защита информации. Материалы XX научно-практической конференции. Минск, 19-21 мая 2015 г. – Минск: РИВШ, 2015. С. 112–113.
7. Ноутбук руководителя [Электронный ресурс]. URL: <http://accord.ru/bossnotebook.html> (дата обращения: 13.04.2018).
8. Аккорд-АМДЗ [Электронный ресурс]. URL: <http://accord.ru/amdz.html> (дата обращения: 13.04.2018).
9. *Счастный Д. Ю.* Перспективы развития средств доверенной загрузки. Взгляд разработчика // Вопросы защиты информации, 2017. № 3. С. 27–28.
10. *Конявский В. А.* Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем – на старт, внимание, МАРШ! // Комплексная защита информации. Материалы XV международной научно-практической конференции (Иркутск (Россия), 1–4 июня 2010 г.). М., 2010.
11. Доверенный сеанс связи [Электронный ресурс] URL: <http://proterminaly.ru/trust_access.html> (дата обращения: 13.04.2018).
12. *Кравец В. В.* Клавиатура – устройство вывода? // Блог компании «Перспективный мониторинг» [Электронный ресурс] URL: <https://habrahabr.ru/company/pm/blog/352868/> (дата обращения: 13.04.2018).
13. *Конявский В. А.* Развитие средств технической защиты информации // Комплексная защита информации. Сборник материалов XII Международной конференции (13-16 мая 2008 г., Ярославль (Россия)). М., 2008. С. 109–113.
14. *Конявский В. А., Лопаткин С. В.* Компьютерная преступность. Т. II. М., 2008. – 840 с.
15. *Счастный Д. Ю.* Техническая защита информации в эпоху Intel Management Engine // Комплексная защита информации. Сборник материалов конференции (Суздаль 22–24 мая 2018 г.). (в печати).