ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

НА СЛУЖБЕ ОБОРОННО-ПРОМЫШЛЕННОГО КОМПЛЕКСА

ИННОПОЛИС 2015

WWW.ITOPK.RU

Секция 5:
Информационная безопасность

Тема доклада:
Доверенная отечественная аппаратно-программная платформа – основа разработки отечественных доверенных систем

Докладчик:
к.ф.-м.н. Грюнталь Андрей Игоревич, заведующий отделом математического обеспечения ФГУ ФНЦ НИИСИ РАН

Проблемы безопасности киберинфраструктуры РФ

Характеристика киберинфраструктуры РФ

В настоящее время функционирование государственных институтов России, банковской сферы, её промышленного, нефтегазового и энергетического комплексов полностью зависит от работоспособности созданной за последние 20 лет киберинфраструктуры, включающей компьютеры, коммуникационные сети, контроллеры управления машинами и оборудованием.

В условиях рынка эта киберинфраструктура формировалась в РФ на основе массовых коммерческих аппаратных и программных продуктов зарубежных компаний, которые обладали наилучшими показателями производительность/стоимость, но обеспечивали при этом только экономически приемлемый уровень безопасности и надёжности. Это означает, что в коммерческих компьютерах, серверах и программном обеспечении были, есть и будут уязвимости, создающие реальную угрозу работоспособности киберинфраструктуры, а следовательно, и функционированию государственных структур, промышленного и финансового секторов.

Стратегия двойного сокращения

Конкурентная борьба на рынках ЭВМ, ЭКБ и ПО приводит к стратегии «двойного сокращения», состоящей в том, что сокращается время жизни производимого продукта и сокращается время разработки нового продукта с новой функциональностью.

Безопасная и надёжная аппаратно-программная платформа, для которой требования безопасности и надёжности являются первичными, не может и не должна создаваться на основе стратегии «двойного сокращения» и первичности показателя «производительность/стоимость».

Следствием приоритета требований рынка является возрастающая сложность коммерческих аппаратно-программных платформ, которая является основным препятствием на пути обеспечения их безопасности.

Первичность требований рынка вступает в противоречие с требованиями информационной безопасности информационных систем (ИС).

Россия, имея аналогичные по сути проблемы безопасности киберинфраструктуры, что и США, принципиально ограничена в части возможностей их решения. Прежде всего потому, что российским специалистам недоступны детальные данные ни о возможностях, ни об уязвимостях элементной базы (Intel, AMD, Cisco, и т. д.) и программного обеспечения.

Решением этой проблемы является создание отечественной доверенной аппаратно-программной платформы, для которой требования обеспечения информационной безопасности является первичным.

Отечественная доверенная аппаратно-программная платформа

Требования к доверенной платформе

Отечественная доверенная аппаратно-программная платформа должна базироваться на отечественной электронной компонентной базе, отечественном программном обеспечении, отечественных электронных модулях и ЭВМ. Составные части доверенной платформы должны соответствовать следующим требованиям:

- отечественная электронная компонентная база:
  - микросхемы отечественной разработки;
  - изготовление пластин на отечественном предприятии;
  - корпусирование микросхем на отечественном предприятии;
- отечественное программное обеспечение должно содержать следующие компоненты:
  - операционная система;
  - инструментальные средства (компиляторы, отладчики, высокоуровневые технологические средства);
  - общесистемное программное обеспечение (СУБД, ГИС, графические пакеты);
- электронные модули и ЭВМ
  - оригинальный дизайн электронных модулей;
  - изготовление на отечественном предприятии;
  - оригинальный дизайн корпуса ЭВМ;
  - изготовление ЭВМ на отечественном предприятии.

Разработка, включая все виды испытаний, должна осуществляться отечественным коллективом специалистов на территории РФ в соответствии с требованиями нормативных документов. Это обеспечит сертификацию тех аспектов, которые относятся к процедуре разработки.

Документация на программное обеспечение должна включать все исходные тексты и процедуры генерации исполняемого кода из исходных текстов.

Кибербезопасность и методы защиты

Кибербезопасность

Одним из аспектов доверенных систем является требование защиты от кибернападений.

Кибербезопасность невозможно обеспечить или оценить постфактум путём анализа исходных тестов программ и аппаратуры уже созданных систем и их компонентов. Кибербезопасность закладывается на начальных этапах разработки и создания этих систем, что собственно и гарантирует их безопасность.

Проблема кибербезопасности очень сложна, поскольку исчерпывающее её решение требует защиты от ещё неизвестных методов нападения. Проявление и идентификация очередного вредоносного кода приводит к быстрой ответной реакции, состоящей в выработке программистским сообществом эффективных средств защиты. Поэтому эффективные формы кибернападения всегда новые, ранее неизвестные.

Использование методов поиска уязвимостей в уже разработанных системах, например, методами статического анализа, повышает уровень защищённости к уже известным видам атак, но, вообще говоря, неэффективно при появлении новых методов нападения.

Методы защиты

Применение в информационных системах хотя бы одной программной или аппаратной компоненты, содержащей уязвимость, делает уязвимым всю систему в целом. Поэтому защита должна быть комплексной – программной и аппаратной, причём должна распространяться на различные уровни программ и аппаратуры.

Разработка средства кибернападения требует детального знания структуры объекта нападения.

Структура (исходный код) отечественных микросхем потенциальному противнику неизвестна, микросхемы не могут быть модифицированы, а их свойства остаются постоянными при эксплуатации. Даже в случае отсутствия недекларированных «точек входа» в микросхемах, оставленных разработчиком для отладочных целей, отечественная разработка и изготовление микросхемы гарантируют её защищённость от кибернападения.

Применение зарубежной ЭКБ таких гарантий не даёт. С одной стороны, микросхемы могут иметь уязвимости, связанные со стратегией «двойного сокращения», то есть уязвимости, не замеченные фирмой-изготовителем или неисправленные, если такое исправление приведёт к задержке с выпуском микросхемы. С другой стороны, точки входа могут быть оставлены намеренно, для отладочных целей.

Кроме того, зарубежные серийно выпускаемые микросхемы анализируются специалистами, что приводит к нахождению и опубликованию уязвимостей, которые могут быть использованы для кибернападений. Таким образом, применение отечественной ЭКБ в доверенных системах является необходимым.

Программное обеспечение доверенных систем

Методология создания доверенного ПО

Требования к программному обеспечению доверенных систем аналогичны требованиям к аппаратным средствам. Существенным отличием программного обеспечения от аппаратуры, в смысле требований к информационной безопасности, является то, что программное обеспечение может быть изменено в процессе функционирования системы, что собственно и составляет существо кибератак, связанных с инъекцией кода.

При разработке программного обеспечения целевой функцией является соответствие функциональным спецификациям. Требования к защите от кибернападений являются вторичными, тем более что они плохо формализуются. Поэтому уязвимыми могут быть и хорошо отлаженные системы, длительное время находящиеся в эксплуатации.

Номенклатура средств нападения быстро увеличивается. Поэтому бесперспективной является попытка защититься «от всех видов нападения», рассматриваемая как защита от каждого вида нападения по отдельности. Широкое применение антивирусов и коммерческих средств борьбы с вредоносным кодом эффективно с точки зрения экономической приемлемости. Одна успешная атака может, для критически важных систем, привести к неприемлемому ущербу. Защиту именно от таких кибернападений должны обеспечивать доверенные системы.

Методологический подход при создании доверенных защищённых от кибернападений систем состоит в том, что защищённая информационная системы должна разрабатываться и эксплуатироваться так, чтобы обладать предсказуемым поведением при всех возможных режимах эксплуатации, входных данных и сбоях оборудования.

Основное средство достижения предсказуемости поведения – простота программного обеспечения. Это касается как операционной системы, так и прикладного программного обеспечения. Сложность программного обеспечения не должна превышать тот порог, за которым невозможен наглядный анализ поведения системы.

Наибольший эффект достигается при декомпозиции программного обеспечения по отдельным аппаратным модулям, каждый из которых реализует чётко определённую функциональность.

Кибербезопасность информационной системы базируется на свойствах системы, связанных с возможностью оперативного анализа поведения системы, выявления её нештатного поведения, наличия встроенных в систему средств реакции на кибернападения и парирования последствий кибернападения. Такой анализ возможен при определённой избыточности системы. При этом контролирующие модули системы должны анализировать процесс выполнения приложения и выдавать необходимые парирующие воздействия (контролируемое выполнение).

Работы в части создания доверенной платформы

Состав компонентов доверенной платформы

НИИСИ РАН проводит работы по разработке и серийному производству компонентов доверенной аппаратной платформы. К ним относятся:

- микросхемы (микропроцессоры, коммутаторы, другие микросхемы);
- процессорные и дополнительные электронные модули;
- ЭВМ;
- базовое программное обеспечение (операционные системы реального времени, инструментальные средства, общесистемные средства).

Разработка компонентов доверенной платформы осуществляется в соответствии с ГОСТ и с установленными процедурами испытаний.

Микросхемы

Серийно производятся универсальный микропроцессор 1890ВМ6Я и микропроцессор сигнальной обработки 1890ВМ7Я с архитектурой КОМДИВ. Проектные нормы микропроцессоров - 0.18 мкм. Микропроцессоры поддерживают коммуникационную среду RapidIO, обеспечивающую передачу данных со скоростью 1 Гбайт/сек.

Рабочая частота: 270 МГц – для 1890ВМ6Я, 200 МГц – для 1890ВМ7Я. На задачах сигнальной обработки пиковая производительность микропроцессора 1890ВМ7Я составляет около 8 Гфлопс.

Разработана технология создания вычислительных систем, содержащих десятки и сотни микропроцессоров. Для создания многопроцессорных систем разработаны и серийно выпускаются коммутаторы 1890КП3Я и 1890ВГ18Ф.

Процессорные модули и ЭВМ

На основе этих микропроцессоров разработаны и серийно выпускаются процессорные модули БТ23/33-64 РИО и БТ23/33-128 РИО, др. На базе этих процессорных модулей разработаны и серийно поставляются ЭВМ различной номенклатуры.

ЭВМ с коммуникационной средой RapidIO

ЭВМ «Багет-ВМС.А»

Микропроцессоры:

1890ВМ6Я - 4 шт.

1890ВМ7Я - 30 шт.

ОЗУ - 32 Гбайт

Пиковая производительность - 249,6 Гфлопс

Коммутационная система – RapidIO:

внутренняя магистраль – параллельный RapidIO;
внешние каналы – сериальный RapidIO 18 по 1 Гбайт/с

Группа исполнения: наземная

ЭВМ с коммуникационной средой RapidIO

БЦВМ «Багет-МФ»

Микропроцессоры:

1890ВМ6Я - 2 шт.

1890ВМ7Я - 5 шт.

ОЗУ - 6 Гбайт

Пиковая производительность - 44,8 Гфлопс

Коммутационная система – RapidIO:

внутренняя магистраль – параллельный RapidIO;

внешние каналы – сериальный RapidIO 3 по 1 Гбайт/с

Группа исполнения: авиационная

Операционные системы реального времени

Семейства операционных систем реального времени – ОС РВ Багет 2.X и ОС РВ Багет 3.X

В НИИСИ РАН разработаны два семейства операционных систем реального времени – ОС РВ Багет 2.X и ОС РВ Багет 3.X.

Прикладной программный интерфейс ОС РВ Багет 2.X базируется на стандарте IEEE Std 1003.1 (POSIX).

Прикладной программный интерфейс ОС РВ Багет 3.X базируется на спецификации ARINC 653 и стандарте IEEE Std 1003.1 (POSIX). Для ОС РВ Багет 3.X спецификация ARINC 653 выбрана в качестве основной. Стандарт POSIX используется в той мере, в какой это не противоречит спецификации ARINC 653.

Эти операционные системы соответствуют требованиям, предъявляемым к системам жёсткого реального времени, представляют собой оригинальные разработки (не используют заимствованные коды). Портированы на ЭВМ отечественной разработки . Зарубежный опыт применялся путём использования стандартов API операционных систем (стандартов на прикладной интерфейс операционных систем).

Для этих ОС разработаны инструментальные и общесистемные средства (Си-компилятор, отладчик, трассировщик, графические пакеты), базирующиеся на программных продуктах с открытыми кодами. В среду ОС портированы геоинформационная система и СУБД «Линтер».

ОС РВ, инструментальные и общесистемные средства составляют отечественный полнофункциональный комплект программ, обеспечивающий создание вычислительных комплексов, работающих в масштабе реального времени.

Важное техническое средство обеспечения «доверенности» семейств ОС РВ Багет 2.X и ОС РВ Багет 3.X – кросс-разработка. Среда исполнения и среда разработки разделены. Таким образом, законченное приложение лишено штатных средств, которые можно потенциально использовать для инъекции вредоносного кода.

В качестве инструментальной системы используется ОС Linux.

Операционные системы реального времени

Семейства операционных систем реального времени – ОС РВ Багет 2.X и ОС РВ Багет 3.X

Начало разработки семейства ОС РВ Багет 2.X – 1998 г., выпуск первого издания (ОС РВ Багет 2.0) – 2000 г. Текущая версия (ОС РВ Багет 2.6) прошла государственные испытания в ноябре 2014 г.

Объем ОС РВ Багет 2.6 в строках на языке программирования Си – около 1 млн.

Начало разработки семейства ОС РВ Багет 3.X – 2004 г., выпуск первого издания (ОС РВ Багет 3.0) – 2008 г. Текущая версия (ОС РВ Багет 3.3) прошла государственные испытания в ноябре 2014 г.

Объем ОС РВ Багет 3.3 в строках на языке программирования Си – около 2 млн.

Начиная с 2000 г. ОС РВ семейства Багет 2.X и ОС РВ семейства Багет 3.X поставлены в более чем 100 организаций промышленности.

Коллектив разработчиков этих операционных систем осуществляет постоянное сопровождение и консультации по использованию ОС РВ и по разработке и эксплуатации прикладного ПО.

Следует отметить отсутствие инцидентов, связанных с нарушением безопасности, за весь период эксплуатации семейств ОС РВ Багет 2.X и ОС РВ Багет 3.X.

Таким образом, обеспечен высокий уровень защиты от кибернетических атак.

Универсальность (соответствие API операционных систем требованиям стандарту IEEE Std 1003.1 (POSIX) и спецификации ARINC 653), а также наличие инструментальных общесистемных средств обеспечивает разработку на платформе этих ОС широкой номенклатуры информационных систем различного назначения.

Операционная система реального времени ОС РВ Багет 3.3

Назначение и условия применения ОС РВ Багет 3.3

Операционная система реального времени Багет 3.3 (ОС РВ Багет 3.3) предназначена для создания программного обеспечения вычислительных систем, комплексов и средств автоматизированного управления, работающих в режиме реального масштаба времени. ОС РВ Багет 3.3 разработана на основе оригинальных программных кодов группой разработчиков НИИСИ РАН.

ОС РВ Багет 3.3 может применяться на ЭВМ с отечественными микропроцессорами 1890ВМ5Ф 1890ВМ6Я, 1890ВМ7Я, разработанными НИИСИ РАН, а также на ЭВМ с микропроцессорами RM7000.

Средства повышения надежности и живучести

ОС РВ Багет 3.3 поддерживает средства защиты памяти, соответствующие спецификации ARINC 653 и стандарту POSIX. Средства защиты памяти блокируют доступ прикладной программы к данным операционной системы, а также обеспечивают защиту фрагментов кода прикладной программы от ошибок времени исполнения.

Одним из методов повышения надежности и живучести применяемых в ОС РВ Багет 3.3 является разбиение системы на слабо взаимодействующие части. При возникновении ошибки в одной части системы это позволяет сохранить работоспособность остальных частей и восстановить работоспособность той части, в которой произошел сбой.

При проектировании приложение разбивается на несколько процессов, слабо взаимодействующих друг с другом. Все процессы используют виртуальную адресацию, базирующуюся на аппаратно реализованном механизме виртуальной памяти, что исключает доступ одних процессов к памяти других.

Для хранения системных данных (описатели потоков, семафоров и др.), относящихся к конкретному процессу, ОС РВ использует сегмент системных данных этого процесса. В силу этого ошибки в системных данных одного процесса не влияют на работу других процессов.

Средства межпроцессного взаимодействия, соответствующие спецификации ARINC 653, обеспечивают работоспособность приложения и системы в целом в случае «зависания» отдельных пользовательских процессов.

ОС РВ Багет 3.3 предоставляет разработчику прикладных систем (интегратору) требуемые спецификацией ARINC 653 средства контроля длительности выполнения прикладных и системных процессов, что обеспечивает гарантированный ресурс процессора для каждой программы (ARINC-процесса).

Операционная система реального времени ОС РВ Багет 3.3

Обработка ошибок в ОС РВ Багет 3.3

ОС РВ Багет 3.3 содержит средства диагностики и протоколирования ошибок, содержит средства восстановления работы приложений при сбоях. Диагностика ошибок осуществляется аппаратурой, операционной системой и прикладной программой. Обработка ошибок выполняется операционной системой и прикладной программой.

Средство протоколирования ошибок («трассировщик») обеспечивает запись и протоколирование ошибок времени исполнения. К трассируемым событиям относятся события операционной системы (переключение контекста, посылка сообщений, др.) и события приложения. Для систем реального времени с длительным периодом функционирования, в условиях, когда внешние по отношению к объекту события происходят непредсказуемо, вероятность ошибок планирования (реального времени) довольно высока, а использование традиционных средств интерактивной отладки для выявления таких ошибок затруднительно. Вместе с тем, именно в таких системах могут оказаться полезными средства оперативного анализа данных, собираемых в процессе мониторинга. Решение проблем поиска таких ошибок обеспечивается трассировщиком. Трассировщик содержит средства автоматизированного анализа трассы. Трассировщик также может использоваться при анализе загрузки системы (отдельных процессоров и каналов связи между ними).

Макрооперации tryBegin(), tryCatch(), tryEnd() обеспечивают обработку ошибок на уровне приложения. Макрооперации могут использоваться для обработки следующих ошибок:

- исключительные ситуации;
- переполнение стека;
- ошибки, обнаруженные прикладной программой.

Если ошибка не была обработана с помощью макроопераций tryBegin(), tryCatch(), tryEnd(), то она будет обрабатываться «монитором здоровья» ОС РВ по описанным ниже правилам.

Встроенный в ОС РВ Багет 3.3 «монитор здоровья» обеспечивает обработку ошибок, диагностированных операционной системой или прикладной программой. Реакция на ошибку определяется интегратором на этапе конфигурирования операционной системы и зависит от «тяжести» ошибки и состояния системы.

Операционная система реального времени ОС РВ Багет 3.3

Обработка ошибок в ОС РВ Багет 3.3

Спецификация ARINC 653 определяет действия системы при возникновении ошибки. Реакция на ошибку задается при конфигурировании системы и зависит от конкретного типа ошибки и состояния системы. Спецификация ARINC 653 предусматривает следующие уровни ошибок:

- ошибки уровня модуля;
- ошибки уровня процесса;
- ошибки уровня потока управления.

Ошибки уровня модуля и уровня процесса обрабатываются операционной системой. Ошибки уровня потока управления обрабатываются прикладной программой. В зависимости от уровня ошибки возможны следующие виды реакции:

- рестарт модуля;
- останов модуля;
- рестарт процесса;
- останов процесса;
- игнорирование ошибки;
- приостановка потока;
- посылка сигнала;
- перезагрузка.

Механизм монитора здоровья обеспечивает «самолечение» системы при возникновении ошибок, предусмотренных при конфигурировании.

Итоги работ по доверенной платформе

Требования к доверенным системам

Доверенная система всегда должна выполнять свою миссию и быть защищённой от кибернападений. Необходимое условие доверенности системы – отечественная разработка всех компонентов, аппаратных и программных, выполненная в соответствии с принятыми в РФ процедурами.
Разработка доверенных систем требует специальных методик, направленных на парирование нештатного поведения системы в процессе функционирования (концепция «контролируемого выполнения»).

Полученные результаты

В рамках работ по доверенным системам НИИСИ РАН создал комплект аппаратных и программных изделий, представляющих собой платформу для разработки отечественных доверенных систем. Компоненты этой платформы:

- микропроцессоры и другие микросхемы;
- процессорные и периферийные модули;
- ЭВМ специального назначения;
- базовое программное обеспечение (операционные системы, инструментальные средства и общесистемные средства).

Основные компоненты платформы эксплуатируются около 15 лет.
Разработка выполнялась в соответствии с руководящими документами, обеспечивающими контроль за разработкой и сертификацию законченного изделия.
На базе компонентов доверенной платформы разработаны вычислительные комплексы, содержащие десятки микропроцессоров.
Разработанные аппаратные и программные средства составляют базу для создания широкой номенклатуры доверенных автоматических и автоматизированных систем.

Дальнейшая работа

Проводится разработка нового поколения СВТ, базирующегося на микропроцессорах с частотой 1 ГГц, и базового ПО для этих СВТ. Проводятся работы по реализации концепции «контролируемого выполнения».

ИТОПК
ИННОПОЛИС
2015

Спасибо за внимание!


ИТОПК
ИННОПОЛИС
2015
WWW.ИТОПК.РФ