Комплексный план научных исследований «Системное программирование и информационная безопасность»

Краткие сведения о КПНИ

Сроки выполнения: 2018-2020 гг.

Цель: создать новые перспективные подходы к обеспечению информационной безопасности, нацеленных на минимизацию угроз безопасности, связанных с ошибками в программно-аппаратном обеспечении.

Ожидаемые результаты: технологии и инструменты моделирования и анализа требований безопасности, анализа проектов аппаратуры, исходного и бинарного кода программ для выявления и минимизации рисков эксплуатации уязвимостей.

Основные участники: ИСП РАН, ФИЦ ИУ РАН, МИАН, НИИСИ РАН, ИПМ РАН и другие академические институты.

Партнеры КПНИ: МГУ, ВШЭ, МГТУ, ГосНИИАС, компании «Касперский», СВЕМЕЛ, РусБИТех.

Бюджет КПНИ: более 40 млн.руб. в год.

Координатор КПНИ: Институт системного программирования РАН

Концепция КПНИ поддерживается рядом отечественных компаний, специализирующихся в области информационной безопасности и создания доверенного ПО, ФСТЭК России, научными центрами силовых ведомств. Концепция КПНИ была поддержана конференцией разработчиков операционных систем OSDAY-2017.

Концепция

Информационная безопасность в современном мире уже давно не сводится к использованию шифров и криптографических протоколов. Основными причинами утечки персональных данных, кражи или подмены данных, сбоев в критической инфраструктуре являются ошибки в программном обеспечении. Ошибки присутствуют на всех уровнях функционального стека, включая программы, взаимодействующие с пользователями, серверы, промежуточное программное обеспечение, служебные компоненты операционных систем и даже прошивки в в аппаратных компонентах компьютеров.

Только за первые 4 месяца 2017 года в базе известных уязвимостей National Vulnerability Database (NVD) , которую поддерживает Национальный институт стандартов и технологии США (NIST), зарегистрированы более 450 критических уязвимостей. Были выявлены разнообразные виды ошибок – исполнение данных, переполнение буфера, прямой доступ в ОЗУ, внедрение команд и т.д. Ошибки были найдены в аппаратном обеспечении, во встроенных и управляющих системах, серверном программном обеспечении, популярных приложениях пользователей.

Новые тенденции в развитии информационных технологий создают новые риски для информационной безопасности. Цифровой мир стремительно расширяется, он становится мобильным, управляет производством и технологическими процессами, охватывает всю среду обитания человека — от бытовых приборов до умных офисов и интеллектуального транспорта. Всё больше информации передается через мобильные сервисы, ранее изолированные системы начинают взаимодействовать и обмениваться информацией, лавинообразно нарастает поток данных и объемы хранения. Внедрение новых парадигм организации распределенных крупномасштабных систем, таких как «Интернет вещей» (Internet of Things, IoT), приведет к новым рискам информационной безопасности, когда через сеть станут доступны практически все предметы, окружающие человека.

В результате бурного роста информационно-коммуникационных технологий все большее количество кода становится доступно для внешнего воздействия, поэтому ошибки в программных системах открывают возможности для новых видов атак. Также бурно развиваются аппаратные платформы, стремительно растет производительность микропроцессоров, что одновременно сопровождается невиданным ранее усложнением программно-аппаратных интерфейсов, и возникают новые векторы атак, направленных на аппаратное обеспечение.

Технологический рывок, вызвавший стремительный прогресс в области ИКТ, привел также к росту спектра различных уязвимостей, угроз и рисков, связанных с неаккуратным использованием, а также с непредвиденными эффектами интеграции разнородных технологий, приводящими к созданию ненадежных и слабо защищенных инфраструктурных систем, подвергающих опасности как находящиеся под их контролем данные и бизнес-процессы, так и жизни и здоровье людей.

Обеспечение информационной безопасности становится сквозной технологией цифровой экономики и информационного общества. Вызовы, связанные с конфиденциальностью, целостностью, доступностью данных и защитой коммерческой тайны и частной жизни, возникают во всех областях информационных технологий. Данная КПНИ предназначена найти системный ответ на возникающие вызовы и строить более надёжные и безопасные системы.

Цель данного комплексного плана научных исследований заключается в создании новых перспективных подходов к обеспечению информационной безопасности, нацеленных на минимизацию угроз безопасности, связанных с ошибками в программно-аппаратном обеспечении.

Реализация КПНИ «Системное программирование и информационная безопасность» позволит разработать и использовать более систематические и строгие технологии обеспечения безопасности программ и аппаратуры, что, в свою очередь, позволит создавать более безопасные и надежные программно-аппаратные системы.

В работу КПНИ «Системное программирование и информационная безопасность» должны быть вовлечены академические и университетские центры компьютерных наук, а так же ведущие отечественные ИТ-компании. Симбиоз исследовательских центров и индустрии

позволит создавать инструменты и технологии, максимально адекватные задачам и потребностям индустрии.

Задачи информационной безопасности в рамках КПНИ «Системное программирование и информационная безопасность»

Информационная безопасность является неотъемлемым свойством программно-аппаратной системы. Требования информационной безопасности должны закладываться в архитектуру системы ещё на этапе проектирования, анализ и поиск ошибок должны осуществляться на протяжении всего цикла разработки. Так как современные системы, по большей части, создаются из повторно-используемых компонентов или библиотек, то безопасность системы в целом в значительной мере определяется безопасностью и надёжностью используемых компонентов.

В рамках КПНИ исследования и разработки будут сосредоточены на решении нескольких задач обеспечения информационной безопасности:

- **Минимизация рисков возникновения уязвимостей при разработке аппаратного обеспечения.** В рамках КПНИ будут идти исследования и разработки, направленные на минимизацию числа ошибок при разработке микропроцессоров и устройств, а также выявлении закладок в приобретенных дизайнах аппаратуры.

  Планируется разработка средств анализа архитектуры микроэлектронных устройств и средства анализа описаний аппаратуры на специализированных языках (HDL, hardware specification language).

  Предполагается разработка рекомендаций, методов и программных инструментов, затрудняющих внесение НДВ в аппаратуру, разработанную на отечественных предприятиях, но производимую вне территории РФ.

- **Минимизация рисков уязвимостей при разработке программного обеспечения.** Минимизация рисков возникновения уязвимостей на этапах проектирования и разработки ПО, а также минимизации рисков атак через дефекты, обнаруженные на этапе эксплуатации ПО.

  В рамках КПНИ предполагается разработка новых методов и технологий обеспечения безопасности и надежности в жизненном цикле разработки программного обеспечения. В рамках этого направления предполагается создать набор инструментальных средств для моделирования, анализа и верификации программ, включая безопасные компиляторы (в том числе кросс-компиляторы с языков C/C++ для отечественных многоядерных микропроцессоров и отечественной операционной системы реального времени), средства статического анализа программ на различных языках, дедуктивной верификации алгоритмов и программ, динамического анализа, автоматизированного тестирования, эмуляции и кросс-отладки для отечественных многоядерных процессоров и т. п.,.

- **Обеспечение информационной безопасности на этапе эксплуатации:** разработка новых методов защиты развернутых и функционирующих систем и компонентов.

В рамках КПНИ могут вестись исследования и разработки защиты компонентов ОС и приложений средствами виртуализации, внедрение в существующие системы средств контроля целостности, мониторинга и выявление вторжений и т. п.

- **Создание доверенной базы для безопасных систем:** создание аппаратно-программных компонентов для доверенных вычислений (доверенная загрузка, защищенное хранилище, особые режимы процессора и т.п.), новых безопасных и надёжных компонентов системного уровня для различных приложений, включая операционные системы реального времени, сетевые стеки, системы хранения и обработки данных.

  Предполагается разработка требований к микроконтроллерам в части системных функций, используемых низкоуровневым ПО для защиты информации и разграничения доступа, такими как, управление аппаратными ресурсами, обеспечение доверенной загрузки встроенными аппаратными средствами микроконтроллера, реализация корня доверия.

- **Создание доверенной базы для облачных вычислений:** создание компонентов защищенной инфраструктуры, обеспечивающей конфиденциальность и целостность данных в облачной среде, разработка новых криптографических методов, таких как гомоморфное шифрование, защищенная распределенная файловая система, защищенные нереляционные хранилища данных и т.п.

Минимизация рисков уязвимостей при разработке аппаратного обеспечения

По мере развития технологий в окружающем человека мире появляется всё больше устройств, находящихся под управлением микропроцессоров и программного обеспечения. С ростом числа внедрений решений на базе IoT, как считают эксперты, всё больше атак будет направлено не только на ПО, но и на аппаратное обеспечение (микпроцессоры, сетевые карты, USB устройства), входящее в инфраструктуру «интеллектуального транспорта», «умных домов», автоматизированных систем управления производством.

Обеспечение надежной платформы для разрабатываемых систем – на этой задаче фокусируется КПНИ в части работы с аппаратурой. Современные процессы разработки микропроцессоров и периферийных устройств на начальных этапах имеет много общего с разработкой ПО, так как большинство оборудования разрабатывается как программы на специализированных языках программирования, которые называются языками описания аппаратуры (HDL). Необходимо развивать методы анализа описания аппаратуры, моделирования угроз, выявления уязвимостей и проведения испытаний с упором на проверку требований информационной безопасности.

Помимо собственно аппаратуры ещё один источник уязвимостей для аппаратных систем кроется во встраиваемом ПО, не только выполняющем загрузку компьютера, но и работающем в большинстве периферийных устройств. Регулярно публикуются бюллетени об обнаружении уязвимостей во встраиваемом ПО тех или иных устройств. Анализ такого ПО и выявление в нем уязвимостей и НДВ является важной задачей обеспечения общей информационной безопасности программно-аппаратных систем.

Минимизация рисков уязвимостей при разработке программного обеспечения.

Для минимизации рисков информационной безопасности, вызванных ошибками при разработке программных систем, необходимо адекватное развитие системного программирования и методов обеспечения информационной безопасности — развитие методов разработки и анализа безопасного и надежного ПО. Такие методы должны быть реализованы в виде комплексных технологий создания и сопровождения безопасных программных систем, включая инструменты поддержки всех деятельностей в рамках жизненного цикла системы для достижение нужных уровней ее безопасности и надежности. В качестве важной прикладной задачи мы рассматриваем создание отечественной платформы для кросс-разработки ПО для отечественных процессоров, удовлетворяющей требованиями к информационной безопасности для систем реального времени.

Спектр развиваемых технологий в этой области должен включать все перспективные направления. С одной стороны, владение всем разнообразием технологий построения безопасных систем является необходимым условием технологической независимости страны и устранения намечающегося запаздывания в освоении новых зарубежных разработок. С другой стороны, умение использовать все многообразие таких техник необходимо для успешного развития комплексных технологий поддержки жизненного цикла безопасных систем на различных технологических платформах, часто включающих достаточно специфические инструменты разработки ПО.

Результатом исследований в указанной области системного программирования должны стать инструментальные средства, средства разработки и анализа программ — компиляторы, средства анализа, моделирования и верификации.

Обеспечение информационной безопасности на этапе эксплуатации

Поддержка защищенности ПО начинается с гарантий того, что не произошла подмена или модификация программ в процессах передачи и установки ПО, включает задачи выпуска своевременных обновлений, а также задачи выявления аномального поведения и защиты систем и компонентов от эксплуатации в нештатных режимах.

Другой аспект информационной безопасности на этапе эксплуатации систем заключается в том, что в мире неуклонно повышается уровень интеграции систем, возникновение систем систем (SoS, Systems of Systems). Помимо новых качеств, возникающих в результате объединения систем, приводит также к росту спектра различных уязвимостей, угроз и рисков, связанных с неаккуратным использованием, а также с непредвиденными эффектами интеграции разнородных технологий. В результате могут возникнуть ненадежные и слабо защищенные распределенные и информационные системы, подвергающие опасности как находящиеся под их контролем данные и бизнес-процессы, так и жизни и здоровье людей.

Создание доверенной базы для безопасных систем

Системное программное обеспечение — операционные системы, сетевые стеки, системы хранения, промежуточное программное обеспечение и т. п. — является базой, на которую опираются все другие программные системы, и тем самым является базой не только собственно информационных технологий, но и всех технических сложных систем, включая

системы критичные по безопасности и стратегически важные системы государственной инфраструктуры. Тем самым важнейшие характеристики информационной безопасности ИКТ-решений, а также надежность, быстродействие, отказоустойчивость, существенным образом определяются соответствующими характеристиками системного ПО. Уязвимости в системном программном обеспечении дезавуируют все механизмы защиты на уровне приложений.

Важную роль в создании защищенных компонентов системного ПО играет аппаратура. Большинство современных микропроцессоров содержат специализированные расширения, поддерживающие различные аспекты защиты ПО – доверенные модули (TPM, trusted platform module), реализующие хранилище ключей, шифрование, цифровую подпись областей памяти и т.п., расширения доверенной загрузки, специальные режимы работы процессоров, такие как SMM в x86 или TrustZone в ARM. Для создания защищенных отечественных платформ необходимо разрабатывать соответствующие расширения в микропроцессорах, а также компоненты в операционных системах.

В результате исследований в этой области должны быть разработаны надежные компоненты критических инфраструктур, относящиеся к системному программному обеспечению, такие как доверенные аппаратно-программные компоненты, операционные системы реального времени, сетевые стеки, системы хранения, промежуточное ПО (middleware) и т.п.

Создание доверенной базы для облачных вычислений

Широкое внедрение облачных технологий привело к возникновению принципиально новых вызовов информационной безопасности. Традиционная модель «защиты периметра» создаёт высокие риски в случае компрометации облачной инфраструктуры «изнутри» - уязвимость в реализации облачного сервиса или виртуальной машины потенциально даёт возможность злоумышленникам доступ к данным клиентов облака. Требуются исследования и разработки новых методов защиты конфиденциальности и целостности данных в условиях масштабной распределенной инфраструктуры, таких как гомоморфное шифрование, защищенные распределенные хранилища, защищенные нереляционные базы данных и т.п.

Современные облачные инфраструктуры строятся из композиции большого числа компонентов, каждый из которых имеет собственные настройки безопасности и политики доступа. Для обеспечения безопасности облака в целом необходимо, чтобы настройки и политики безопасности компонентов облачной инфраструктуры были согласованы друг с другом и давали требуемый уровень защиты, поэтому в рамках КПНИ можно разработать новые методы моделирования и анализа общей конфигурации облака, совместимости политик безопасности отдельных компонентов.

Направления научных исследований КПНИ «Системное программирование и информационная безопасность»

Для реализации целей настоящей комплексной программы и решения задач поставленных задач информационной безопасности исследования и разработки будут идти по следующим основным направлениям:

- ***Развитие методов дедуктивного анализа в контексте моделирования, анализа и доказательств требований безопасности.***

  Под дедуктивным анализом мы объединяем направления современного Computer Science, которые традиционно относятся к формальным методам, и связаны с задачами спецификации требований, анализом требований и доказательством выполнения требований в моделях или исходном коде программ.

  В контексте информационной безопасности дедуктивный анализ позволяет выявлять ошибки в политиках безопасности, провести анализ архитектуры ПО, формально и строго доказывать корректность ключевых элементов инфраструктуры безопасности.

  В рамках указанного направления будут вестись исследования и разработки в следующих областях:

  - методы спецификации требований безопасности к программно-аппаратным системам и компонентам,
  - методы моделирования политик безопасности и архитектуры ПО в контексте безопасности,
  - методы моделирования политик безопасности и конфигурации облачных инфраструктур,
  - методы формального доказательства различных свойств, связанных с безопасностью, в описании аппаратуры, моделях и исходных текстах ПО.
  - …

- ***Развитие методов конструирования компиляторов, оптимизации и трансформации кода***.

  К этому направлению мы относим те методы Computer Science, которые связаны с разработкой новых языков, созданием интерпретаторов и компиляторов, эмуляторов и бинарных трансляторов, с оптимизацией и трансформациями кода.

  В контексте информационной безопасности могут применяться к различным задачам. В частности:

  - создание специализированных языков для спецификации требований и политик безопасности,
  - создание доверенных безопасных компиляторов и линкеров для минимизации ошибок в бинарном коде,
  - создание новых надежных и прослеживаемых оптимизаций,
  - методы трансформации кода программ и описаний аппаратуры для защиты реализованных алгоритмов и обрабатываемых данных от анализа (обфускация), для внедрения водяных знаков и защиты от эксплуатации уязвимостей.
  - Разработка и реализация верифицированной платформы кросс-разработки ПО для отечественных многоядерных микропроцессоров и отечественной операционной

системы реального времени, включающей компилятор C/C++, эмулятор и кросс-отладчик, охватывающие аппаратный и программный уровни.

- …

- ***Развитие методов статического анализа***

  К этой группе технологий мы относим методы автоматизированного анализа исходных и исполняемых кодов ПО, при которых код программ не исполняется. Статический анализ позволяет выявлять широкий класс типовых дефектов программ, в том числе на редких путях исполнения, которые затруднительно или просто невозможно обнаружить при традиционном тестировании.

  Развитие методов статического анализа в контексте информационной безопасности позволит выявлять на ранних этапах уязвимости, которые традиционно эксплуатируются в атаках — переполнение буферов, ошибки работы с памятью, разыменование нулевых указателей, ошибки работы с форматными строками и т.п.

  В рамках КПНИ предполагается вести исследования и разработки в следующих областях:

  - методы анализа, учитывающие высокоуровневую специфику языков C, C++, C#, Java, применимые к большим программным системам;
  - методы анализа низкоуровневых компонентов операционных систем, драйверов и т.п.;
  - методы статического анализа динамических языков (Python, Ruby);
  - методы статического анализа бинарного кода;
  - методы статического анализа HDL-описаний (проектов микроэлектронной аппаратуры) на разных уровнях абстракции.

- ***Развитие методов динамического анализа***

  К динамическому анализу мы относим методы, связанные с анализом исполнения кода: динамическое символьное исполнение, а также тестирование, тестирование с использованием моделей, фаззинг.

  Динамический анализ в контексте информационной безопасности позволяет находить критические ошибки и уязвимости в программах и предъявлять входные данные, на которых произошла ошибка, а также выделять уязвимости, приводящие к исполнению произвольного кода. Также возможно проводить глубокий анализ ПО, для которого недоступны исходные тексты. В частности, решаются задачи выявления недокументированных возможностей, восстановления алгоритмов.

  В рамках КПНИ предполагается вести исследования и разработки в следующих областях:

  - гибридные методы анализа, объединяющие статический и динамический анализ;

- методы динамического анализа для различных аппаратных платформ (x86, ARM, MIPS, PowerPC, микроконтроллеры);
- методы тестирования с использованием моделей для ПО и моделей аппаратуры;
- методы фаззинга для ПО и моделей аппаратуры;
- методы тестирования моделей аппаратных модулей.

Помимо исследований и разработок в рамках КПНИ будут созданы учебные курсы для подготовки специалистов в области системного программирования и информационной безопасности. Отсутствие специалистов, компетентных в этой широкой и активно развивающейся сфере знаний, может привести к углубляющемуся отставанию России в данной сфере, а впоследствии и к невозможности не только создания собственных инноваций в ИКТ, но и адекватного осмысления и внедрения уже имеющихся технологий, созданных в других странах, к снижению технологической независимости страны.

Значение КПНИ для Российской Федерации

Одна из важнейших проблем, на решение которых нацелено развитие области системного программирования в рамках КПНИ, — отставание от современных потребностей технологий разработки и сопровождения систем с повышенными требованиями к надежности и безопасности. Общая сложность, разнородность программных компонентов, разнообразие технологий, базовых платформ, библиотек и их различных версий, массовое и удаленное использование программных продуктов приводят к нарушениям безопасности, низкому качеству систем и огромному количеству ошибок и уязвимостей в них.

Развитие системного программирования дает прямой вклад в решение задач обеспечения национальной безопасности и повышения надежности сложных интеллектуальных систем, функционирующих на территории Российской Федерации, защиты данных граждан нашей страны, безопасного внедрения новых сервисов и Интернета вещей в России.

Проведение исследований и разработка новых технологий в области системного программирования позволит не только поддерживать технологическую независимость Российской Федерации, но и обеспечивать понимание и своевременное осознанное внедрение технологий, которые так или иначе будут возникать в зарубежных странах, потеря же компетенций в этой области приведет к утрате такого понимания, а, значит, к росту рисков, связанных с приобретением и использованием новых зарубежных технологий.

Прогресс в данной области также является базой для расширения экспорта сложных технических систем и изделий российского производства в энергетике, оборонной и авиакосмической отраслях.

Реализация КПНИ «Системное программирование и информационная безопасность» внесет существенный вклад в следующие задачи национальной безопасности:

- обеспечение защищенности критической инфраструктуры Российской федерации от компьютерных атак и противодействие использованию информационных технологий в целях нанесения ущерба национальным интересам России;

- обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, и другой охраняемой законом информации при использовании информационно-коммуникационных технологий, в том числе в информационно-телекоммуникационной сети Интернет;
- противодействие информационным атакам, затрагивающим национальные интересы Российской Федерации, совершенствование системы подготовки кадров в области информационной безопасности, обеспечение защиты персональных данных граждан;
- создание, развитие и использование современных систем связи для нужд обороны страны, безопасности государства и обеспечения правопорядка
- обеспечение защиты информации в информационных системах и информационно-телекоммуникационных сетях органов государственной власти, включая системы управления экологически опасными производствами, объектами повышенной опасности и критически важными объектами, формирование системы международной информационной безопасности.

Помимо решения технологических задач обеспечения информационной безопасности КПНИ отвечает ещё на один актуальный вызов — недостаточное количество экспертов, способных поддерживать и развивать современные технологии в условиях глобальных процессов развития информационно-коммуникационных технологий. Большинство образовательных и исследовательских организаций неспособны воспитывать команды специалистов, имеющих необходимые знания для глубокого и детального понимания передовых технологий в области ИКТ, а также навыки для создания как аналогов имеющихся, так и новых технологий мирового уровня.

Координатор КПНИ

Институт системного программирования Российской академии наук является ведущим центром компетенции в области системного программирования в России. Разработанные в ИСП РАН технологии и инструменты используются силовыми ведомствами России и разработчиками доверенного программного обеспечения (СВЕМЕЛ, РусБИТех и др.) для повышения информационной безопасности программных и программно-аппаратных комплексов. ИСП РАН тесно взаимодействует с ФСТЭК России в части создания регламентов по обеспечению информационной безопасности программных систем, разрабатываемых в России, и средств поддержки выполнения таких регламентов.

Технологии анализа кода, разработанные в ИСП РАН, широко используются в ведущих мировых лидерах ИТ-отрасли. Например, анализатор Svace является основным средством анализа кода в корпорации Samsung, а технологии статического анализа ИСП РАН являются ядром анализатора Klockwork, который используется в сотнях компаний по всему миру.

ИСП РАН ведёт разработки полного цикла, от фундаментальных исследований до внедрения, по всем направлениям КПНИ. У руководства ИСП РАН есть большой опыт координации проектов в области системного программирования и информационной безопасности.