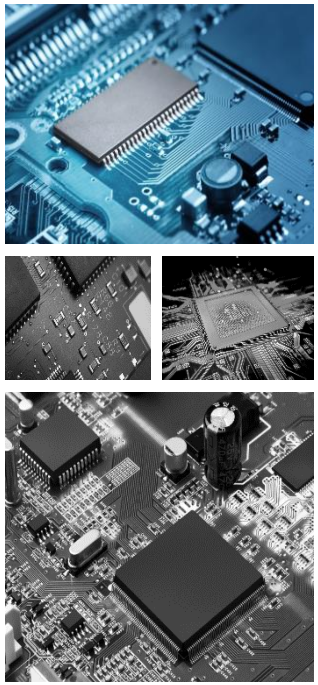
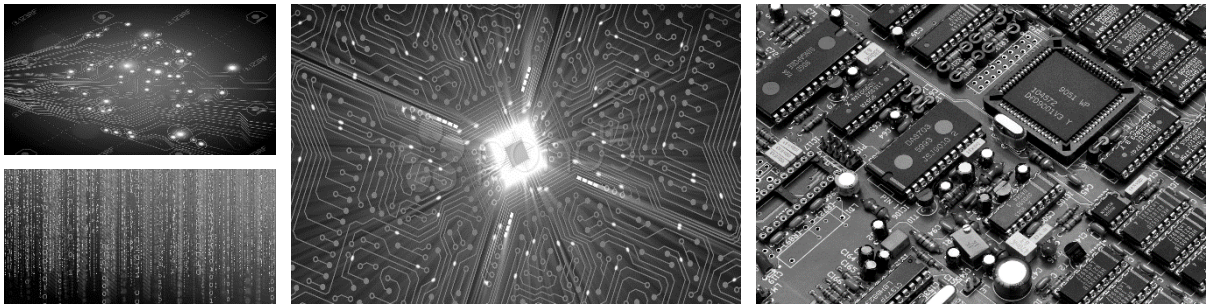
ИнЧип Технологии

Разработка электронных компонентов и аппаратуры





SAFENET как основа создания доверенной вычислительной среды для проектов НТИ

г. Москва,
21 февраля 2017 г.

Борис Кривошеин
Исполнительный директор ООО «ИнЧип Технологии»

Приоритетные направления и проекты SAFENET

Устройства, применяемые для обеспечения безопасности

- Интеллектуальные камеры с обработкой потоковой информации (AeroNet + AutoNet)
- Системы биомониторинга и биокриптографии (NeuroNet + HealthNet)

Прикладные системы для решения задач безопасности

- Системы биометрического контроля (все *Net)

Защищенные системы передачи данных

- Квантовые коммуникации и бесканальные технологии передачи состояний (все *Net)
- Технологии оптической связи (все *Net)
- Мультиагентные операционные системы и системы связи (все *Net)
- Сетевые платформы для автономных устройств, беспилотного транспорта и промышленного интернета (AeroNet + AutoNet + MariNet + EnergyNet)

Безопасность платформ управления и приложений

- Защищенная платформа для обработки больших массивов данных (все *Net)
- Защищенная ОС для критически важной инфраструктуры IoT (все *Net)

Архитектура безопасности информационных и киберфизических систем

Безопасность объектов:

- Люди
- Транспротные средства
- Промышленная инфраструктура
- Финансовые ресурсы
- Окружающая среда
- … … …

Причины уязвимостей в информационных системах

- Преднамеренно внедренные не декларированные возможности в аппаратуре и ПО (**backdoors**)
- Непреднамеренные не декларированные возможности, возникшие в результате ошибок разработчиков и недостатков технологии проектирования (**exploits**)
- **Скрытые уязвимости**, связанные с неполной оценкой рисков и источников угроз
- **Сбои и отказы аппаратуры**, выполняющей функции безопасности

Степень доверия к реализации информационной системы

- **Оценка и верификация** технических средств, методов и процессов, реализующих политику информационной безопасности

- **Операционная гарантированность**:
  - Безопасная архитектура системы;
  - Контроль целостности системы;
  - Отсутствие неконтролируемых каналов передачи информации;
  - Доверенное администрирование;
  - Доверенное восстановление после сбоев

- **Технологическая гарантированность**:
  - Контроль проектирования, реализации и сопровождения системы

Классы функциональных компонентов безопасности по ISO/IEC 15408-2

- FAU – средства аудита безопасности
- FCO – средства коммуникаций
- FCS – средства криптографической поддержки
- FDP – средства защиты данных пользователя
- FIA – средства идентификации и аутентификации
- FMT – средства управления безопасностью
- FPR – средства защиты конфиденциальности
- FPT – средства защиты компонентов, выполняющих функцию безопасности
- FRU – средства управления использованием ресурсов и конфигурацией
- FTA - средства управления доступом
- FTP – доверенные каналы управления и передачи данных

Доверенная вычислительная среда = доверенная аппаратная платформа + доверенное ПО

Риски со стороны аппаратуры:

- Недокументированные возможности ЭКБ
- Неточность модели аппаратной архитектуры или ее реализации
- Неправильная оценка параметров при расчёте надёжности

Риски со стороны ПО:

! По критериям анализа рисков ПО является более уязвимым элементом системы, чем аппаратура

- Ложные оценки: полная доступность исходного кода обеспечивает только минимальный уровень доверия
- Отсутствие или неполнота верификации кода
- Высокий уровень доверия к ПО возможен только при использовании доверенной среды проектирования и сопровождения в течение всего жизненного цикла

Распространение угроз безопасности

- Уязвимости и недекларированные возможности «нижних» уровней остаются доступными на «верхних», и тем самым создают «сквозные» угрозы безопасности.
- Для построения доверенной вычислительной среды (ДВС) необходим контроль безопасности, начиная с самого нижнего уровня (аппаратных ядер)

Организация разработки доверенных ПАК

- Сквозная модель угроз, с учётом возможных уязвимостей на всех уровнях программно-аппаратного стека
- Поддержка на аппаратном уровне базовых механизмов защиты (запрет исполнения данных, установка режима Read-Only для исполняемого кода и пр.)
- Режим контролируемого уровня безопасности: любой компонент программно-аппаратного стека является не более доверенным, чем компоненты уровней ниже

Взаимодействие сообществ разработчиков аппартного и программного обеспечения доверенных вычислительных систем (ДВС)

- Выработка общих **методик** построения и **критериев** оценки доверенных программно-аппаратных систем
- Разработка концепции «сквозной» **технологии защиты** ДВС, учитывающей все известные модели угроз
- Создание **промышленной экосистемы** отечественных разработчиков аппаратуры и ПО
- Разработка и внедрение **отраслевых стандартов** ДВС

Контакты

ООО «ИнЧип Технологии»
Россия
105005 Москва
ул. Радио 24 к.1
T +7 499 281 65 63
E contact@inchip.tech
http://www.inchip.tech