ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР

ПЕРСПЕКТИВЫНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ В ЗАЩИТЕ ИНФОРМАЦИИ

АКАДЕМИК АКАДЕМИИ КРИПТОГРАФИИ
А.П. БАРАНОВ

ОСНОВНЫЕ НАПРАВЛЕНИЯ

- Многопроцессорные кластерные системы, основа защищенных облачных услуг
- Информационная безопасность программного обеспечения (ПО)
- Криптография в массовом применении
- Алгоритмические методы обеспечения безопасности информации в больших системах
- Апостериорная защита на основе мониторинга

Безопасность программно-аппаратных кластерных платформ

- Сертификация высокоскоростной кластерной шины, как основы платформы ЦОД
- Мини кластерные платформы, как основа для больших объемов вычислений при реализации: криптоферм, платформ WF – высокой производительности, типа Crossbeam
- Исследование программно-аппаратных платформ виртуализации совокупности серверов положений. Microsoft Hyper-V
- Исследование и сертификация серверной части технологии VDI
- Исследования и сертификация по устойчивости к компьютерным атакам, глобальных и локальных, балансировщиков нагрузки, распределяющих трафик между приложениями, с учетом географической топологии

ЗАЩИТА ОТ НСД В БАЗОВЫХ ОБЛАЧНЫХ ОС

- Исследование архитектурных принципов построения компонент виртуализации основных платформ. Выделение критических узлов.
- Обеспечение ИБ сверхвысокоемких хранилищ данных, построенных по технологии: специальная ОС плюс эффективная машина базы данных Oracle Exadata, Teradata, ECM
- Разработка системы защищенных, тонких и не очень тонких клиентов для создания мобильных офисов с использованием различных видов телекоммуникаций LTE, GSM, WI-FI в совокупности
- Разработка дешевых АРМ коллективного пользования с тонким клиентом и шифрованием трафика

ОБЩИЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО

- Проблемы валидации ПО и проблема алгоритмического описания деятельности пользователя
- Сертификация средств «быстрого» создания эффективного ПО на основе применения кейс-технологий CAP, Oracle Business Suit
- Проблема верификации ПО в том или ином состоянии предоставления (исходные тексты , исполняемые коды)
- Автоматизация исследования ПО, как в части общих требований ИБ, так и в части оставшихся недоработок (тупиковые ветви, переполнение регистров, люки и т.д.)

ЧАСТЫЕ ПРОБЛЕМЫ ИБ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

- Сохранение наработок прикладного ПО прошлых лет без кардинального переделывания
- Упрощение пользовательских интерфейсов пакетов ПО для массового применения. Возможно большая дефрагментация пакетов. Успех Apple
- Упрощение работы с «Облаком» обычного малоквалифицированного пользователя
- Переработка продуктов обеспечения БИ (в первую очередь ЭП) для массового пользователя. Программные электронные замки, системы антивирусной поддержки и автоматического обновления и т.д., существующие отечественные криптопровайдеры годны только для профессионалов, да и то не очень

ПРОБЛЕМЫ КРИПТОГРАФИИ ПРИ ЕЕ МАССОВОМ ПРИМЕНЕНИИ

- Связь и подтверждение принадлежности личности к цифровому коду (ключу подписи). Идентификация личности по цифровому коду
- Необходима система свой – чужой без хранения ключа клиента в базе опознавателя и без личной явки к опознавателю
- Что обеспечивают, какую ИБ системы поддерживают уровни КС – КА? Нужны непрофессиональные описания подтвержденные или выработанные регуляторами
- Как избежать необходимости перемен или доработки криптоправайдеров при модернизации (патчировании) ОС
- Упрощение или прекращение сертификации прикладного ПО при использовании сертифицированных криптопримитивов. Проблема большого ПО

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ КРИПТОГРАФИЧЕСКИХ ИССЛЕДОВАНИЙ В ОТКРЫТОЙ СФЕРЕ

- Дальнейшее развитие моделей блоков криптосхем и их взаимодействий. Линейные модели , в том числе с искаженными параметрами, исчерпались, модели независимого взаимодействия блоков теперь мало перспективны
- Разработка новых принципов синтеза криптосхем и криптосистем. Подход: «хорошо, потому, что ничего не понимаю и никто не поймет в силу сложности» - плохой
- Оценка ИБ шифраторов при различных видах обрабатываемой информации и их работы в сбойных ситуациях на конкретных аппаратных платформах. Открытые материалы ФСТЭК дают такую возможность исследований
- Развитие теории принятия сигнала в помехах, включая многоканальный прием

Алгоритмические методы обеспечения БИ в больших системах

- Априорная защита и управление распределенными или концентрированными в ЦОДах базами данных
- Управление системой – составляющая компонента БИ. Например, управление системой электронных замков где более 10^5 пользователей
- Проектирование и автоматизация назначения прав доступа в зависимости от различных функциональных процессов и приложений
- Корректировка производственных процессов или законодательных актов под требованиями БИ
- Теория автоматического резервирование средств и ресурсов для обеспечения доступности и устойчивости работы системы в условиях волатильности потребностей

АПОСТОРИОРНАЯ ЗАЩИТА

- Методы и степень защиты самих систем мониторинга и фиксации нарушений
- Мониторинг парольной системы и действий администраторов
- Сертификация систем мониторинга в сфере ФСТЭК РФ
- Разработка моделей и профилей поведения, а также критериев возникновения инцидентов ИБ
- Балансировка конструкции :

  многофакторность мониторинга-

  - локализация обработки в среднем слое

  - концентрация в ЦОД
- Методики определения цены различных видов информации при ее утрате


СПАСИБО
ЗА ВНИМАНИЕ