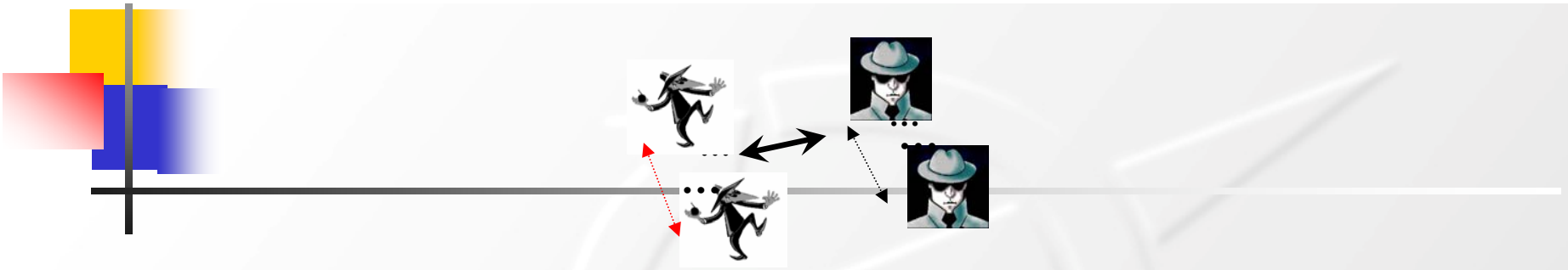


ПОДХОД К ЗАЩИТЕ ПРОГРАММ НА ОСНОВЕ МЕХАНИЗМА УДАЛЕННОГО ДОВЕРИЯ

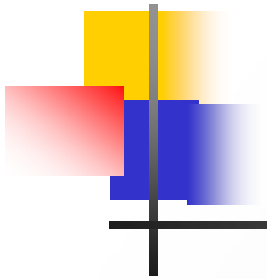
Десницкий В.А., Котенко И.В.

Санкт-Петербургский институт информатики и автоматизации РАН

РусКрипто'2009, 2-5 апреля 2009

Содержание

- Введение
- Механизм удаленного доверия
- Мобильный модуль
- Принцип замещения модуля
- Компонент проверки подписей
- Реакция надежного сервера на взлом клиентской программы
- Атаки на механизм удаленного доверия
- Применяемые методики защиты
- Масштабируемость механизма защиты
- Оценивание методик защиты
- Заключение



Введение

- Взлом программы: несанкционированные изменения кода, вмешательства в работу программы
- Недостатки существующих методов защиты ПО от взломов
  - Усиление существующих приемов защиты исключительно за счет увеличения их сложности => “*гонка вооружений*”
  - Раскрытие противником используемых алгоритмов защиты способствует осуществлению взлома
  - Отсутствие формального доказательства стойкости методов защиты
- Необходимость временных ограничений, накладываемых на работу противника
- Использование SW/HW методов защиты

Цели работы

- Разработка комплексного механизма по защите ПО от взломов
  - Модель защиты “клиент-сервер”, реализующая принцип *удаленного доверия*
  - Определение ограничений противника по времени, необходимого для осуществления взлома, при помощи принципа обновляемого модуля
  - Разработка модели атак на данный механизм
  - Доказательство адекватности данного механизма посредством анализа сложности выполнения атак

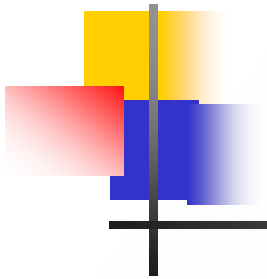
Цели работы

- Гарантировать неизменность и правильность работы программы в потенциально враждебном окружении
- Уведомление о взломе программы
- Невозможность противнику воспользоваться взломанной программой

- Классы задач, для которых применим данный механизм
  - Программы, осуществляющие коммуникации с другими клиентами (*e.g. IP телефония*)
  - Программы, для работы которых требуется поддержка со стороны специализированного удаленного сервера (*e.g. eCommerce, eGovernment*)

Механизм удаленного доверия

- Клиентская программа, выполняющаяся в пределах ненадежного (*untrusted*) хоста
- Надежный (*trusted*) сервер, функционирующий на удаленном хосте
- Мобильный модуль (*mobile module*)
  - Монитор
    - Непрерывно выполняет набор верификаций кода программы, ее состояния, используемых данных, библиотек
    - Выполняет специальные вычисления, чувствительные к изменениям программы
    - Собирает некоторую дополнительную информацию о программе
  - Генератор подписей
    - Регулярная отправка надежному серверу данных, характеризующих результаты работы верификаций
    - Подписи отправляются в зашифрованном виде
    - Обеспечение идентификации клиента сервером



Мобильный модуль

- Модуль не поставляется с программой
- Динамически загружается во время загрузки программы с сервера
- Регулярное замещение модуля

- Взаимопроникновение кода модуля и кода клиентской программы
- Максимально возможное равномерное распределение кода модуля по коду программы

Принцип замещения модуля (1/2)

- Замещение для повышения взлома-устойчивости программы
  - Создание сервером новой версии модуля, который содержит обновленные версии функций верификации
  - Доставка модуля клиентской программе
  - Установка в выполняющуюся программу без ее перезагрузки или приостановки
- Изменения кода модуля
  - Изменение ключа шифрования
  - Изменение алгоритма работы модуля
  - Изменение выборки верифицируемых данных
  - Изменение количественных и качественных характеристик модуля и др.

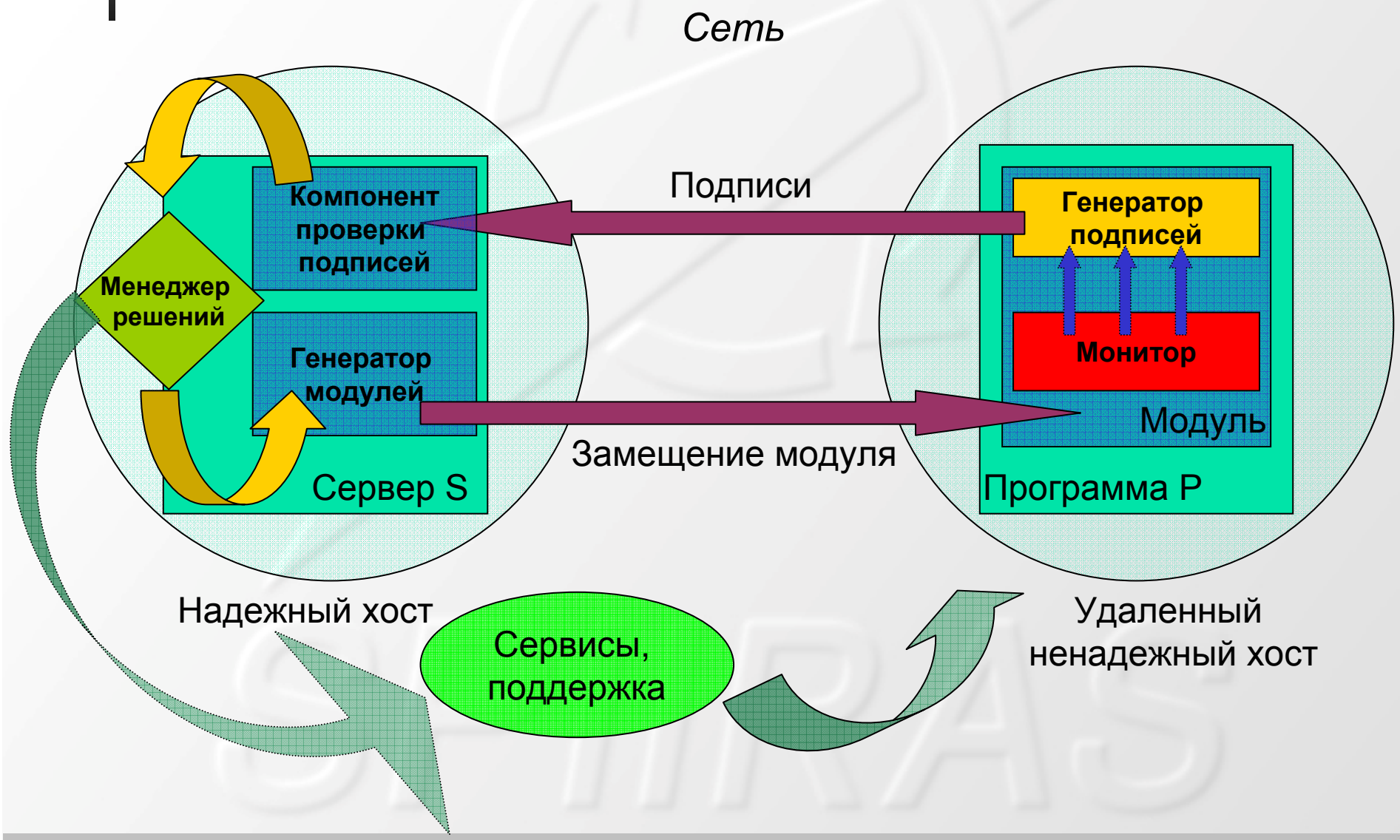
Принцип замещения модуля (2/2)

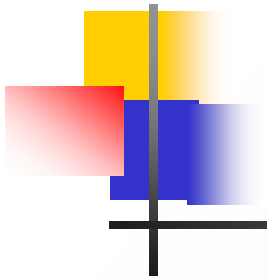
- Изменение модуля от версии к версии
  - Уникальность модуля - различие для каждого клиента
  - Не повторяемость модуля для каждого запуска программы
- Цель замещения – не дать противнику достаточного времени для осуществления взлома программы
- Требование: приблизительное (оценочное) время взлома программы не должно уменьшаться при условии что противник взломал все предыдущие версии модуля

Определение периода замещения модуля

- Теоретический метод
  - На основе оценивания вычислительной/временной сложности выполнения атак на данный механизм, оценивая сложность осуществления всех вовлеченных в атаку действий
  - *E.g. сложность обратной разработки, де-обфускации и пр.*
- Экспериментальные и статистические методы, учитывающие человеческий фактор
  - Экспертные оценки на основе опыта
  - Эмпирические данные

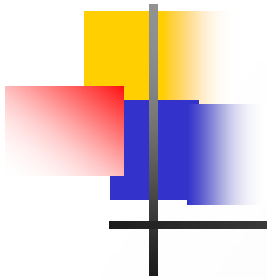
Схема модели защиты





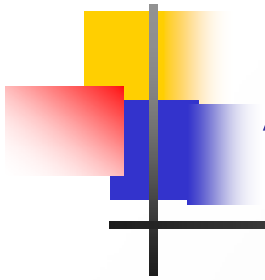
Компонент проверки подписей

- Получение подписей от клиента и их дешифрирование
- Интерпретация и анализ полученной информации
- Принятие решения о том, было ли совершено вмешательство в работу клиентской программы
  - Программа считается некорректной, если хотя бы одна верификация завершилась с отрицательным результатом



Реакция надежного сервера на взлом клиентской программы

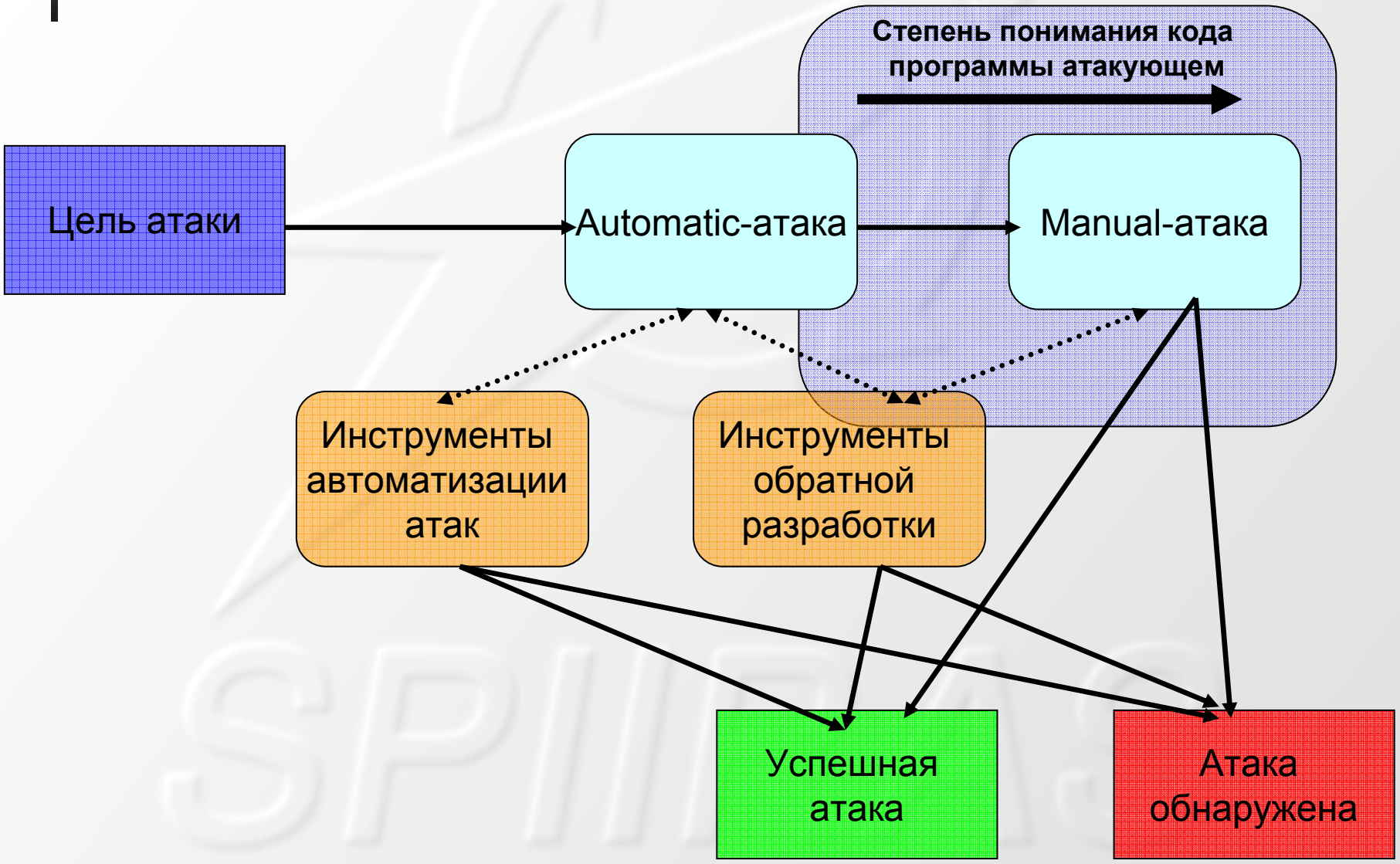
- Сервер прекращает предоставление данному клиенту любых сервисов, программных обновлений, сопровождения
- Информирование владельца авторских прав на данное ПО о взломе
- Возможность отправки клиенту команд по выполнению определенных действий, препятствующих дальнейшему функционированию клиентской программы



Атаки на механизм удаленного доверия

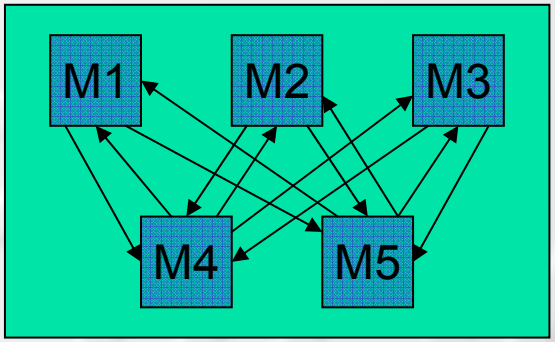
- Reverse-engineering атака и прямое изменение кода программы
- Изменение окружения выполнения, *e.g. при помощи эмуляторов и отладчиков*
- Динамическое изменение состояния программы
- Атака клонирования
- Перехват и подмена сетевых сообщений, содержащих подписи

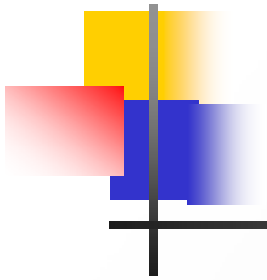
Сценарий действий атакующего



Возможные улучшения механизм удаленного доверия

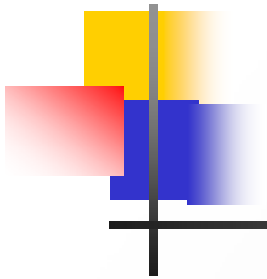
- Выполнение части верификаций на стороне сервера
- Само-верификация монитора
- Модель с несколькими мониторами, где каждый из них может верифицировать остальные мониторы





Используемые методики защиты

- Local-методы
  - Методы обфускации кода
  - Crypto guards
- Remote-методы
  - Методы на основе удаленной аттестации (remote attestation)
    - Проверка инвариантов
    - Проверка корректности потока управления (CFG)
  - Динамическое замещение (dynamic replacement)
  - Slicing-подход
- HW-методы

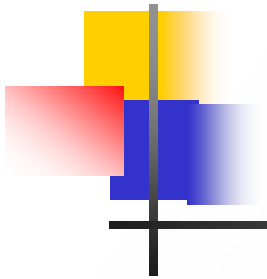


Масштабируемость механизма защиты

- Производительность системы
- Реализация механизма на практике
- Минимизация вычислений на стороне доверенного сервера
- Сложность методик защиты и верификаций на серверной стороне
- Масштабируемость механизма защиты
- Задача достижение компромисса
  - Суммарная Степень защиты *vs.* Масштабируемость

Оценивание ресурсоемкости

- Оценка ресурсоемкости каждой из предложенных методик защиты
- Метрики
  - Оценивание затрачиваемого времени ЦП
    - *Speed* – оценка скорость работы методики
    - *Throughput* – оценивание затрат ресурса ЦП при распараллеливании
  - Оценивание расходов памяти
- Теоретический подход
- Эмпирические исследования
  - Использование инструментов оценки производительности систем



Оценивание защитных методик

- Выделение для каждой из методик наиболее затратных процедур на серверной стороне
- Возможные оптимизации методик защиты
  - Повышение производительности механизма
    - Выполнение части серверных вычислений заранее, до момента запуска клиентской программы
    - Выделение части вычислений, общих для некоторых групп клиентов

Степень защиты

- Определение степени защиты, предоставляемой каждой из методик
  - Экспертные оценки
  - На основе эмпирических данных
- Политики безопасности в управлении клиентами
  - ограничение количества одновременно обслуживаемых клиентов
  - Непродолжительное снижение предоставляемого уровня безопасности механизма защиты
  - Регулирование на основе репутаций

Выбор методик защиты

- Выбор конкретных методик в зависимости от объема доступных ресурсов доверенного сервера
- Прямая задача
  - При фиксированном объеме выделяемых ресурсов, превышение которого недопустимо, и заданном допустимом количестве клиентов, которое может обслуживать сервер, требуется выбрать подходящие методики защиты и тем самым определить уровень безопасности, который может быть обеспечен
- Обратная задача
  - Исходя из выбранных методов, определить максимально допустимое количество клиентов, которое сервер способен обслуживать корректным образом

Заключение

- Выработаны принципы защиты ПО от взломов на основе принципа удаленного доверия
- Рассмотрены атаки на механизм защиты
- Изучение вопросов масштабируемости механизма
- Дальнейшая работа
  - Оценивание масштабируемости, предложенных методик защиты
  - Оценивание степени защиты методик
  - Создание программных прототипов
  - Доказательства адекватности механизма

Контактная информация

Десницкий Василий Алексеевич (СПИИРАН)
desnitsky@comsec.spb.ru
http://comsec.spb.ru/Desnitsky
Котенко Игорь Витальевич (СПИИРАН)
ivkote@iias.spb.su
http://comsec.spb.ru/Kotenko/

Благодарности

Работа выполнена при финансовой поддержке РФФИ (проект №07-01-00547), программы фундаментальных исследований ОНИТ РАН и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST (контракт № 021186-2) и других проектов.