Мои проекты и курсы в SPRINT Lab

Юрий Лифшиц

Математический институт им. В.А.Стеклова
Российской Академии Наук

27 октября 2005

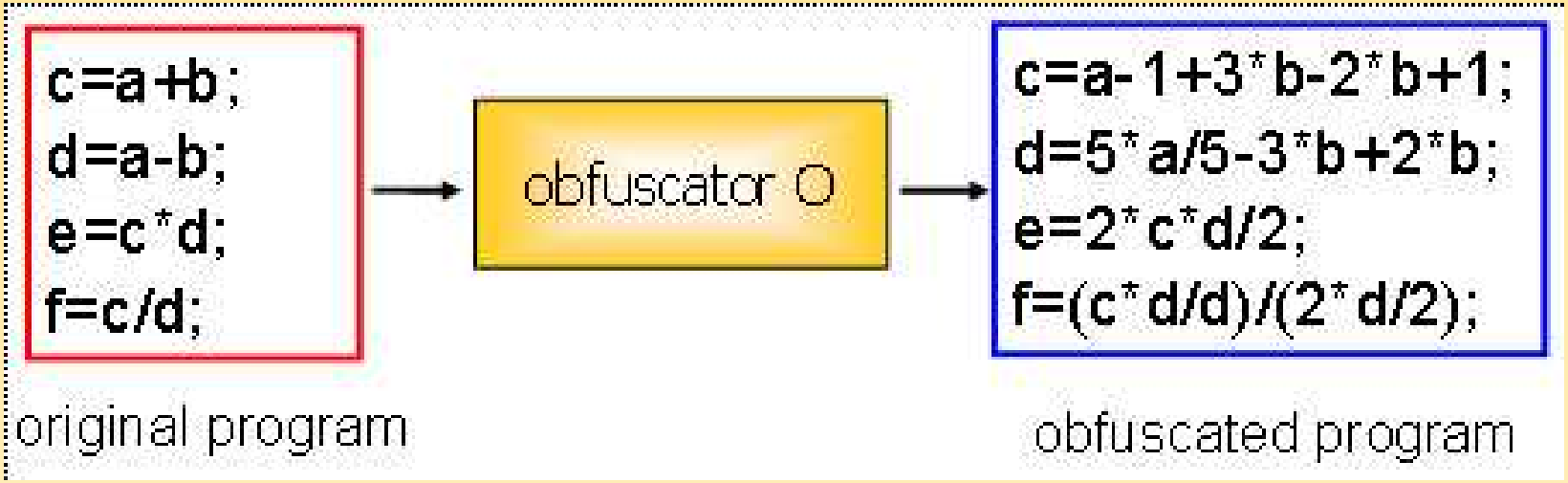
План доклада

1. **Проект “Запутывание программ”**
2. **Учебные курсы**
   - Запутывание программ
   - Современная криптография
3. **Инициативы и пожелания**
   - Возможные проекты
   - Личный взгляд на работу лаборатории

План лекции

1. **Проект “Запутывание программ”**
2. Учебные курсы
   - Запутывание программ
   - Современная криптография
3. Инициативы и пожелания
   - Возможные проекты
   - Личный взгляд на работу лаборатории

Что такое обфускатор



Чему посвящен проект?

Тема проекта:

Запутывание (обфускация) программ: как переписать программу так, чтобы в ней нельзя было разобраться, но чтобы она по-прежнему работала?

Чему посвящен проект?

Тема проекта:

Запутывание (обфускация) программ: как переписать программу так, чтобы в ней нельзя было разобраться, но чтобы она по-прежнему работала?

Задачи проекта:

Провести классификацию применений обфускации
Разобраться в текущих методах
Представить результаты в виде единого обзора

Характеристики проекта

- Два месяца, 15 участников
- Спецкурс и семинар
- Основная работа: обзор “Методы запутывания программ”
- Сайт проекта: обзоры, доклады, конспект лекций
- Научная школа в Москве (28-30 Апреля 2005)

Наши достижения

- Научные достижения:
  - Классификация применений запутывания программ
  - Новые модели защиты программ с доказуемой стойкостью
- Представление результатов:
  - Спецкурс “Запутывание программ”
  - Доклады: Штутгарт, Эстония, Москва, ПОМИ, ГУАП, Интел-Петербург, Нижний Новгород
  - Три московских доклада готовятся к публикации в ИСПРАН

План лекции

1. Проект “Запутывание программ”
2. **Учебные курсы**
   - Запутывание программ
   - Современная криптография
3. Инициативы и пожелания
   - Возможные проекты
   - Личный взгляд на работу лаборатории

“Запутывание программ”

Краткая информация:

- Весна 2005
- Первый в мире курс по данной теме
- 30 активных слушателей
- Материалы лекций выложены в интернет
- Семинар “Новые идеи для запутывания программ”

“Современная криптография”

Краткая информация:

- Осень 2005
- Курс основан на материалах ведущих американских вузов
- Около 40 активных слушателей
- Материалы лекций и электронные конспекты выкладываются в интернет
- Семинар “Классическая криптография”
- Курс не имеет полноценных аналогов в учебном плане мат-меха

План лекции

1. Проект “Запутывание программ”

2. Учебные курсы
   - Запутывание программ
   - Современная криптография

3. **Инициативы и пожелания**
   - Возможные проекты
   - Личный взгляд на работу лаборатории

Детектор плагиата

Основная идея:

Написать инструмент, который по двум программам будет определять степень их сходства.

Уже есть прототип: программа Сергея Оршанского

Детектор плагиата

Основная идея:

Написать инструмент, который по двум программам будет определять степень их сходства.

Уже есть прототип: программа Сергея Оршанского

Менторы со стороны Intel

Максим Курзенев

Александр Орлов

Детектор плагиата

Основная идея:

Написать инструмент, который по двум программам будет определять степень их сходства.

Уже есть прототип: программа Сергея Оршанского

Менторы со стороны Intel

Максим Курзенев

Александр Орлов

В перерыве пройдет оргсобрание проекта!

Шифрование вычислителений

Основная идея:

Написать инструмент, который преобразует вычислительную задачу в набор малопонятных подзадач для дальнейшего исполнения на недоверяемых компьютерах

Шифрование вычислителей

Основная идея:

Написать инструмент, который преобразует вычислительную задачу в набор малопонятных подзадач для дальнейшего исполнения на недоверяемых компьютерах

Ментор со стороны Intel

Игорь Одинцов

Защита мобильных агентов

Основная идея:

Мобильный агент — программа, работающая в интересах пользователя на чужих компьютерах

Наша задача: скрытие стратегий поведения мобильного агента

Защита мобильных агентов

Основная идея:

Мобильный агент — программа, работающая в интересах пользователя на чужих компьютерах

Наша задача: скрытие стратегий поведения мобильного агента

Задача входит в проект, поданный в РФФИ

Перспективные результаты

Результаты в других областях:

- Новый алгоритм для формальной верификации программ
- Алгоритм поиска подпоследовательностей в сжатых текстах

Мысли и инициативы

Как я понимаю задачи лабортории:

- **Социальная миссия:** повышение качества образования
- **Исследования:** взаимодействие ученых и индустрии
- **Рекрутинг:** стажировка студентов в Intel

Мысли и инициативы

Как я понимаю задачи лабортории:

- **Социальная миссия:** повышение качества образования
- **Исследования:** взаимодействие ученых и индустрии
- **Рекрутинг:** стажировка студентов в Intel

(Преодолимые) проблемы:

- Нет программы поддержки **разработки** курсов
- Барьер **конфидециальности**
- Лаборатория не стала **сообществом**

Мысли и инициативы

Как я понимаю задачи лабортории:

Социальная миссия: повышение качества образования
Исследования: взаимодействие ученых и индустрии
Рекрутинг: стажировка студентов в Intel

(Преодолимые) проблемы:

Нет программы поддержки **разработки** курсов
Барьер **конфидециальности**
Лаборатория не стала **сообществом**

Инициативы:

Приглашенные лекции сотрудников Intel
“Computer Science in Russia”
Задуматься о принципах взаимодействия бизнес-наука в масштабах города

Я благодарен:

Г.Ф.Дейкало и коллективу сотрудников вычислительного центра

за доброжелательность и “скорую помощь” в любой момент

Я благодарен:

Г.Ф.Дейкало и коллективу сотрудников вычислительного центра

за доброжелательность и “скорую помощь” в любой момент

В.И.Кияеву

за поддержку всех моих начинаний

Я благодарен:

Г.Ф.Дейкало и коллективу сотрудников вычислительного центра

за доброжелательность и “скорую помощь” в любой момент

В.И.Кияеву

за поддержку всех моих начинаний

Л.В.Нестеренко, И.Калошину, И.Одинцову, М.Курзеневу и А.Орлову

за интерес к нашим результатам и движение к значимому проекту

Я благодарен:

Г.Ф.Дейкало и коллективу сотрудников вычислительного центра

за доброжелательность и “скорую помощь” в любой момент

В.И.Кияеву

за поддержку всех моих начинаний

Л.В.Нестеренко, И.Калошину, И.Одинцову, М.Курзеневу и А.Орлову

за интерес к нашим результатам и движение к значимому проекту

Всем участникам проектов и слушателям курсов

за активное участие

Последний слайд

Контакт: **Юрий Лифшиц**
e-mail: yura@logic.pdmi.ras.ru
web: http://logic.pdmi.ras.ru/~yura/

SPRINT Lab Obfuscation project:
http://ilab.math.spbu.ru/obfuscate/

Спецкурсы:
http://logic.pdmi.ras.ru/~yura/obfuscation.html
http://logic.pdmi.ras.ru/~yura/crypto.html

Последний слайд

Контакт: **Юрий Лифшиц**
e-mail: yura@logic.pdmi.ras.ru
web: http://logic.pdmi.ras.ru/~yura/

SPRINT Lab Obfuscation project:
http://ilab.math.spbu.ru/obfuscate/

Спецкурсы:
http://logic.pdmi.ras.ru/~yura/obfuscation.html
http://logic.pdmi.ras.ru/~yura/crypto.html

Спасибо за внимание!
Вопросы?