Запутывание программ

Представление исследовательского проекта

Юрий Лифшиц

Сегодня

- План проекта, его цели и сроки
- Введение в теорию запутывания программ (очень краткое)
- Время для вопросов

История проекта

V-2004	Доклад В.А. Захарова на заседании Академии Наук;
IX-2004	Начало семинара "Вокруг запутывания программ";
X-2004	Создание интернет-страницы `http://logic.pdmi.ras.ru/~yura/of.html`;
12-X-2004	Открытие лаборатории СПбГУ-Интел;
25-XI-2004	Презентация проекта.

План проекта

- к Новому году - формирование команды, написание обзора, постановка курсовых работ;
- к 1 февраля - распределение тем курсовых работ;
- 1 марта - 1 мая – спецсеминар и спецкурс;
- 5 мая - отчетный доклад и новая обзорная статья.

Подбор команды: вопросы к аудитории

- Опыт научной работы?
- Студенческие школы?
- Мотивация к исследованиям?
- Сколько усилий готовы потратить?
- Что для вас важно в выборе темы?

Запутывание программ - неформальная постановка

Центральная задача теории запутывания программ заключается в следующем. Нужно придумать алгоритм (написать приложение), которой, получая на вход некоторую программу P, трансформировал бы ее в "запутанную" программу $O(P)$. При этом должны быть выполнены три условия:

- сохранение семантики – те же выходы на тех же входах;
- ограничение на рост потрбляемых ресурсов – размер кода, память и время исполнения, требуемые запутанной программой по сравнению с исходной;
- секретность – увеличение сложности программы, скрыте внутренних параметров.

Научный контекст

- Криптография с открытым ключом, односторонние функции, псевдослучайные генераторы;
- Компиляторы, архитектуры, трансляторы, языки;
- Хакеры и их оружие
- Стеганография
- Защита программного обеспечения - водяные знаки, проверка на неизмененность.

Разделы и направления

- Модель, базовые определения;
- Защита кода;
- Архитектурный подход;
- Алгоритмический подход;
- Оценка секретности - практический и теоретический подходы;
- Классификация атак и распутывание.

State-of-the-art

- Начало академических исследований – 1997 год;
- Количество публикаций – два-три десятка, примерно пять диссертаций;
- География – Вейцамановский институт, университеты Окленда, Принстона, Стэнфорда, Москвы, Аризоны, Оттавы, Варшавы;
- Акценты – трансформация кода, архитектурный подход, попытки алгоритмического подхода;
- Коммерческие программы (obfuscators);
- Международный чемпионат – International Obfuscation C Code Contest.

Запомнить/записать

- Интернет-страница – `http://logic.pdmi.ras.ru/~yura/of.html`;
- Лифшиц Юрий – `yura@logic.pdmi.ras.ru`, +79043310563;
- Рассылка – `swcs@logic.pdmi.ras.ru`; Хотите записаться?
- Сайт лаборатории – `http://se.math.spbu.ru/setlab/`
- Запишитесь ко мне на листок!

С чего начать?

- Осенний семинар (по четвергам) – сегодня, 25 ноября, в 17-20 в ауд. 2528;
- Выбор индивидуального задания – договориться со мной о личном разговоре;
- Большой вводный доклад – завтра, 26 ноября, в 17-30, ПОМИ, ауд. 106.

ВРЕМЯ ДЛЯ ВОПРОСОВ

СПАСИБО ЗА ВНИМАНИЕ!