ИСП РАН

Инструмент анализа бинарного кода Aegis

Шамиль Курмангалеев kursh@ispras.ru
Григорий Иванов gregory@ispras.ru

СОДЕРЖАНИЕ

ИСП РАН

ТЕМЫ:

- ✔ Мотивирующий пример
- ✔ Методы поиска ошибок
- ✔ Автоматизация анализа
- ✔ Задачи
- ✔ Темы для курсовых
- ✔ С чем будете работать

✓МОТИВИРУЮЩИЙ ПРИМЕР — НЕКОТОРЫЕ CVE 2021 ГОДА

ИСП РАН

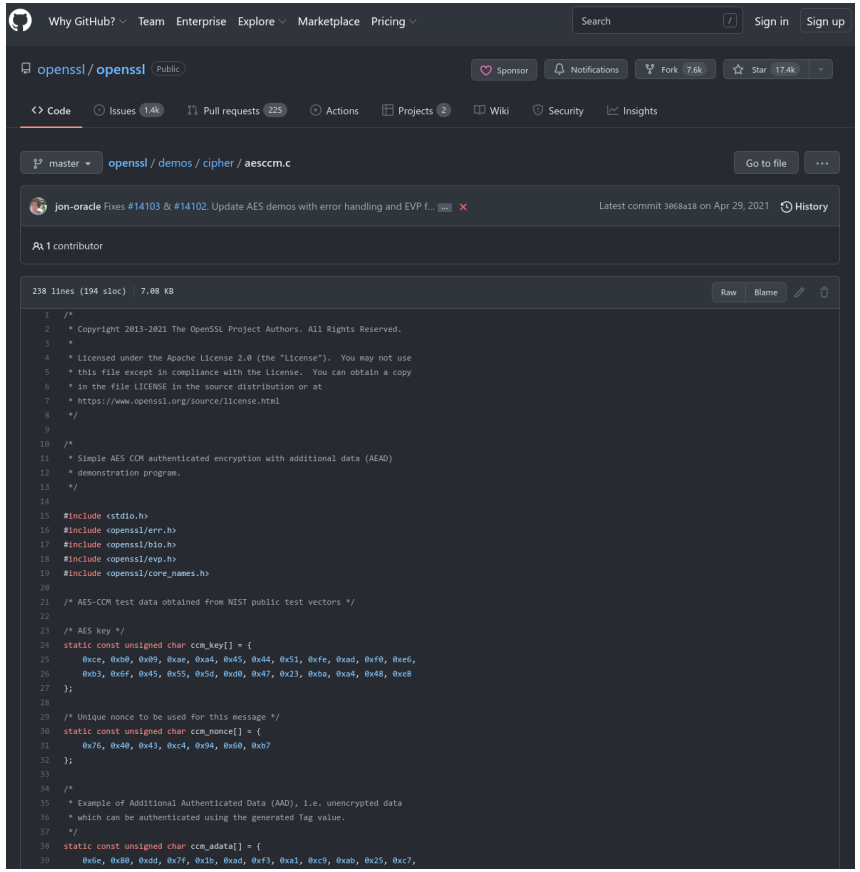
- CVE-2021-34401: NVIDIA Linux kernel distributions contains CodeExec
- CVE-2021-44733: Linux kernel through 5.15.11 contains CodeExec
- CVE-2021-40029: Samba contains CodeExec
- CVE-2021-43217: Windows Encrypting File System (EFS) contains Remote CodeExec
- CVE-2021-3682: qemu contains CodeExec on host

✓ МЕТОДЫ ПОИСКА ОШИБОК

ИСП РАН

- ~~По исходному коду~~
- ~~По бинарному~~

? → **Полноценное исследование**



* не является промышленным инструментом или не удовлетворяет требованиям

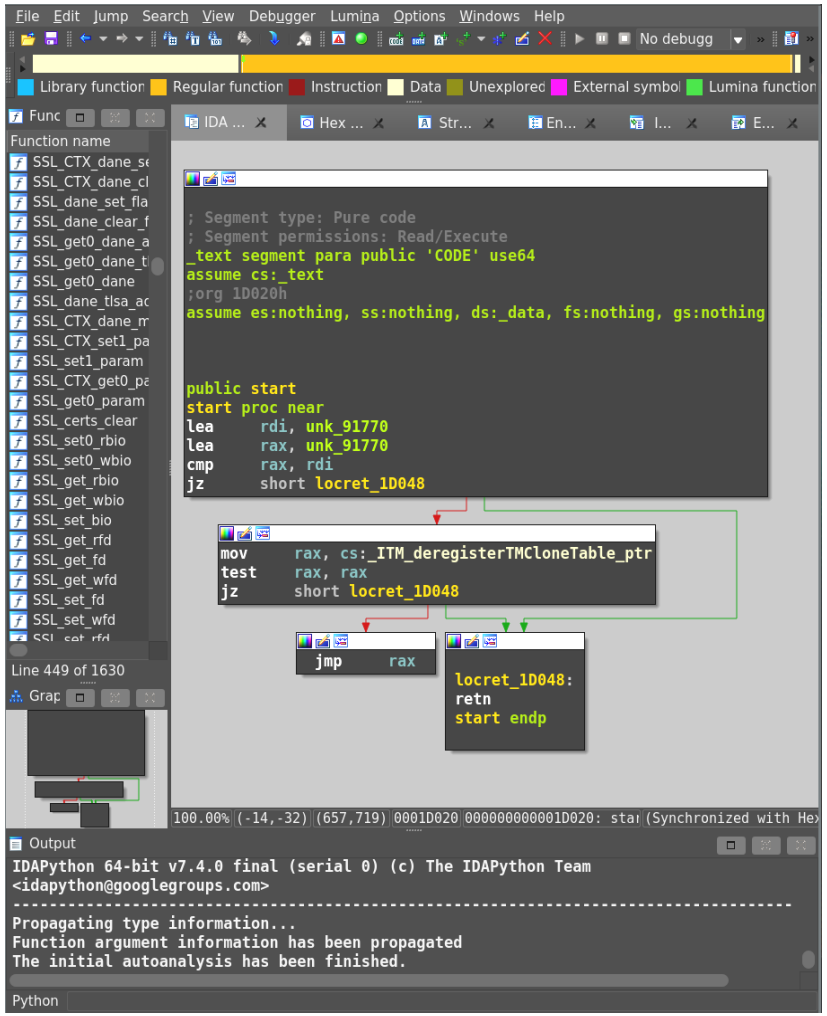
GIT: История коммитов, патчи на уже известные CVE, открытые ISSUE

ИСХОДНЫЙ КОД: комментарии, TODO/FIXME, стат. анализ IDE (восстановление потока данных и управления, графы вызовов, UML-диаграммы), scitools Understand

ИСПОЛНЯЕМЫЕ МОДУЛИ: наличие ASLR, права доступа на секции, секции импорта и экспорта, строки, отладочная информация

ИСПОЛНЯЕМЫЙ КОД: дизассемблер (IDA Pro, Ghidra, r2*, Binary Ninja*), декомпилятор (HexRays, Ghidra-decompiler), анализаторы (Angr, *Miasm)

✓ МЕТОДЫ ПОИСКА ОШИБОК (продолжение)



СБОРКА: Сообщения компилятора (родные и указанные дополнительно), команды линковки, флаги компиляции (+ стат. анализатор gcc)

СТАТИЧЕСКИЕ АНАЛИЗАТОРЫ: Clang, gcc static analyzer, SonarQube, CodeQL (открытые). Svace, Perforce2, Coverity (Закрытые)**

ОТЛАДЧИКИ: gdb, WinDbg, OllyDbg, qemu

ФАЗЗЕРЫ: Afl (+форки), libfuzzer, Syzkaller, hongfuzz, nyx, jacklope, Crusher**

ДИНАМИЧЕСКИЕ АНАЛИЗАТОРЫ: strace, DrMemory, Valgrind, afl-analyze

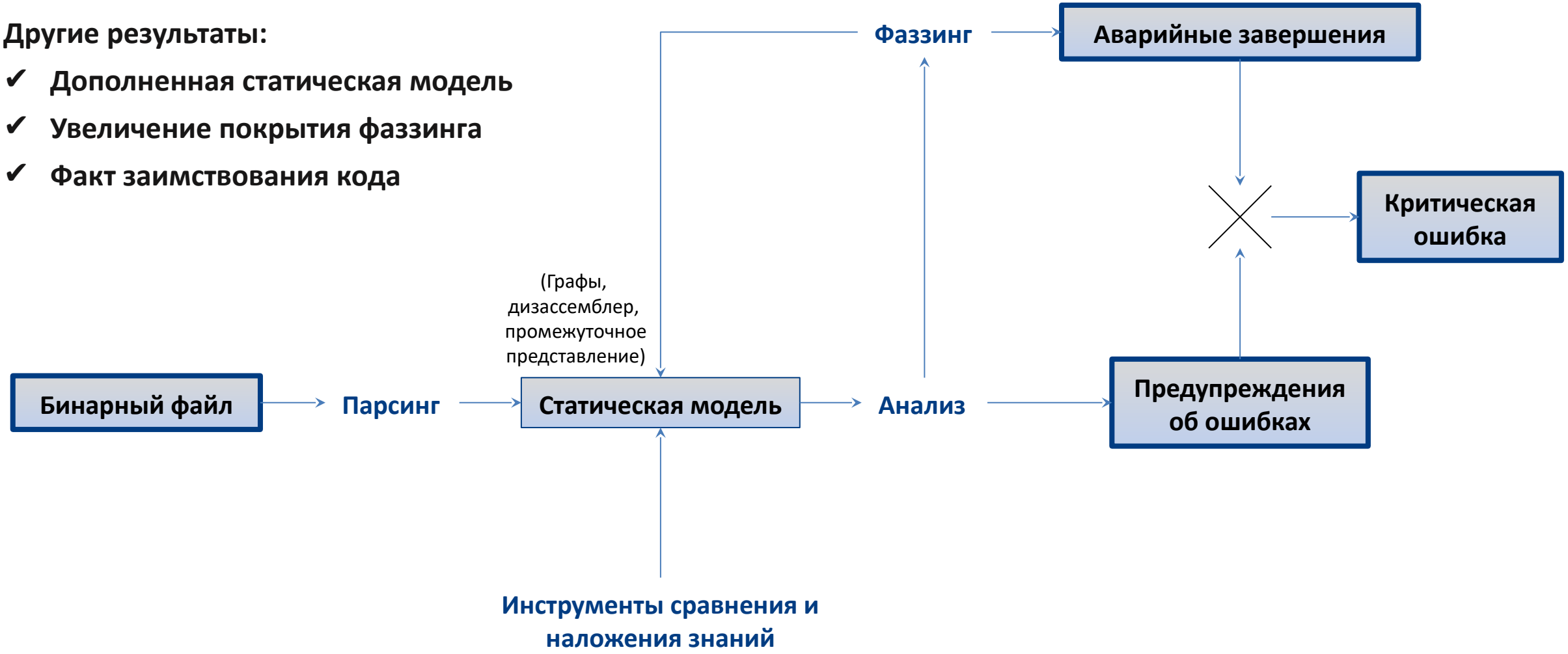
** Разработан и успешно используется в ИСП РАН

✓ АВТОМАТИЗАЦИЯ АНАЛИЗА

ИСП РАН

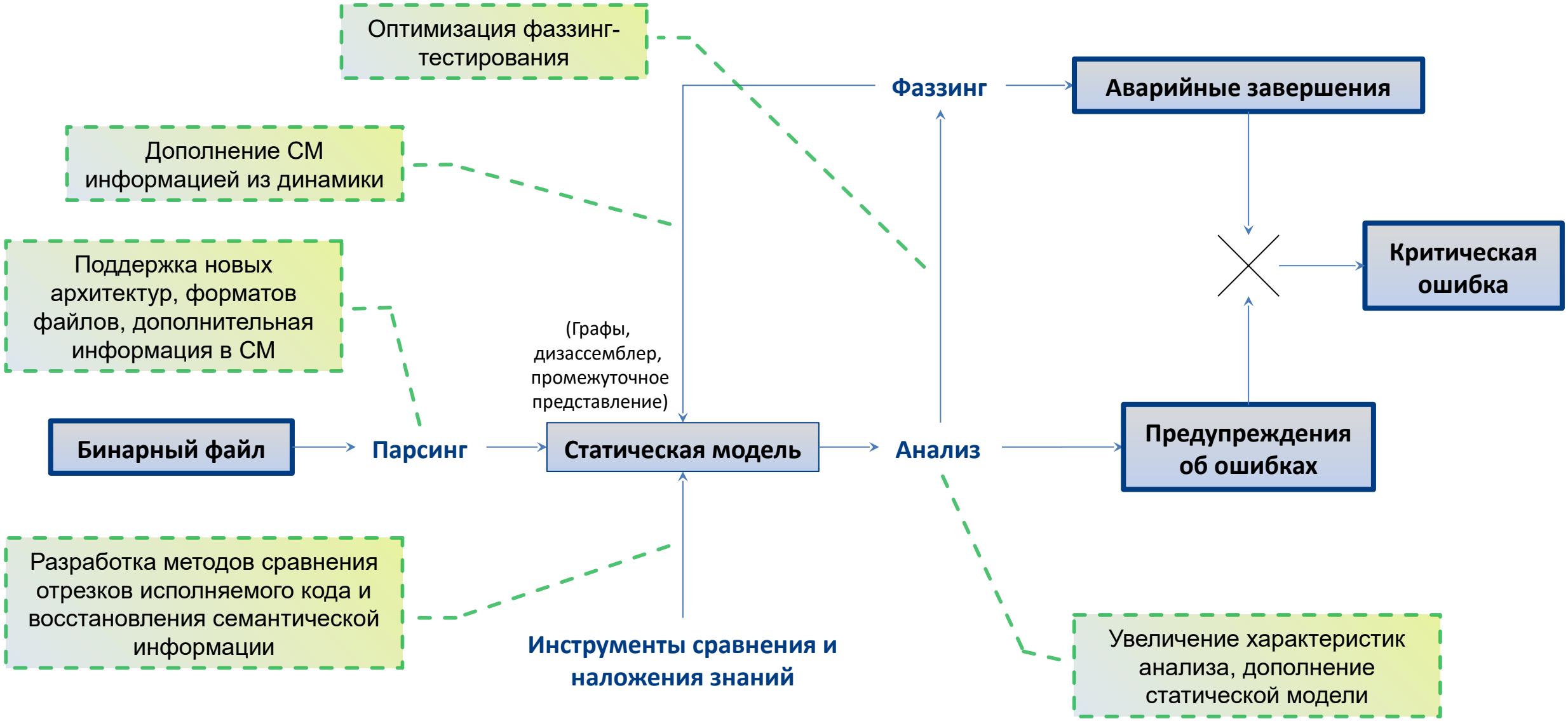
Другие результаты:

- ✔ Дополненная статическая модель
- ✔ Увеличение покрытия фаззинга
- ✔ Факт заимствования кода



✓ ЗАДАЧИ

ИСП РАН



✓ТЕМЫ ДЛЯ КУРСОВЫХ

ИСП РАН

ТЕМЫ:

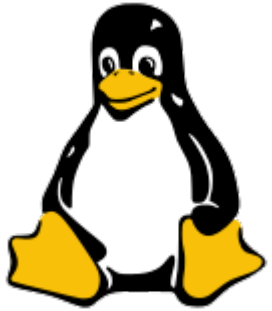
- ✔ Оптимизация промежуточного представления для облегчения статического анализа
- ✔ Разработка детекторов ошибок для анализа бинарного кода
- ✔ Уточнение статической модели информацией из динамического анализа
- ✔ Автоматизированная генерация трансляторов промежуточного представления REIL
- ✔ Разработка методов восстановления карты динамической памяти

Инициативные темы приветствуются!

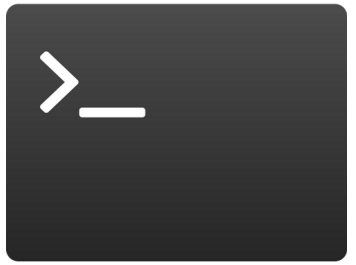
✓С ЧЕМ БУДЕМ РАБОТАТЬ

ИСП РАН

- ✔ Си/C++
- ✔ Ассемблер
- ✔ Операционные системы
- ✔ Компиляторы
- ✔ Linux-окружение
- ✔ Скриптовые языки: Bash, Python
- ✔ Фаззеры
- ✔ Статические анализаторы
- ✔ Символьные решатели



BASH



ИСП РАН

Спасибо!

Приходите!

Курмангалеев Шамиль - kursh@ispras.ru
Иванов Григорий - gregory@ispras.ru