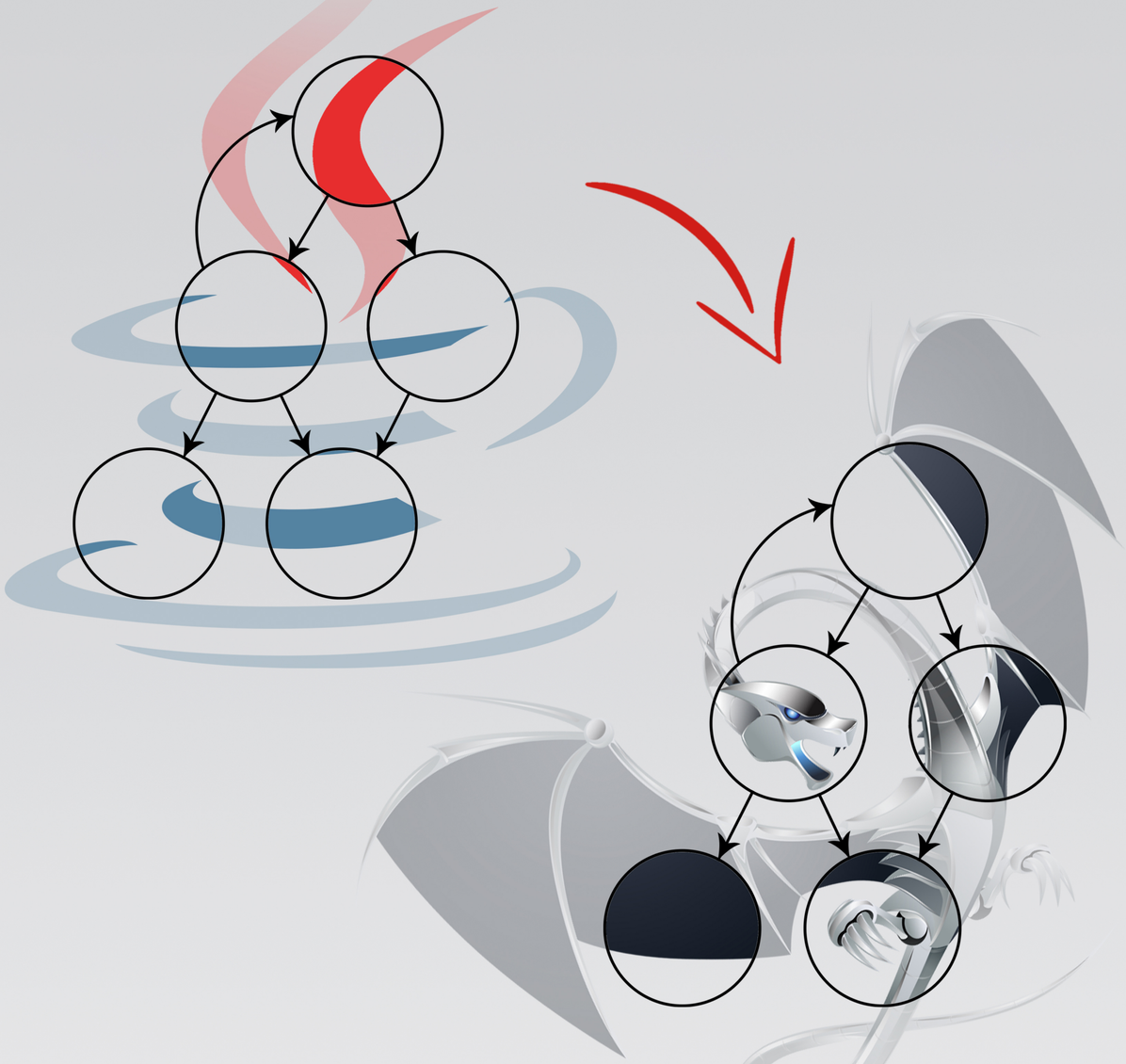
50 EXTRAKCE GRAFŮ TOKU ŘÍZENÍ Z BAJTKÓDU JAZYKA Java™

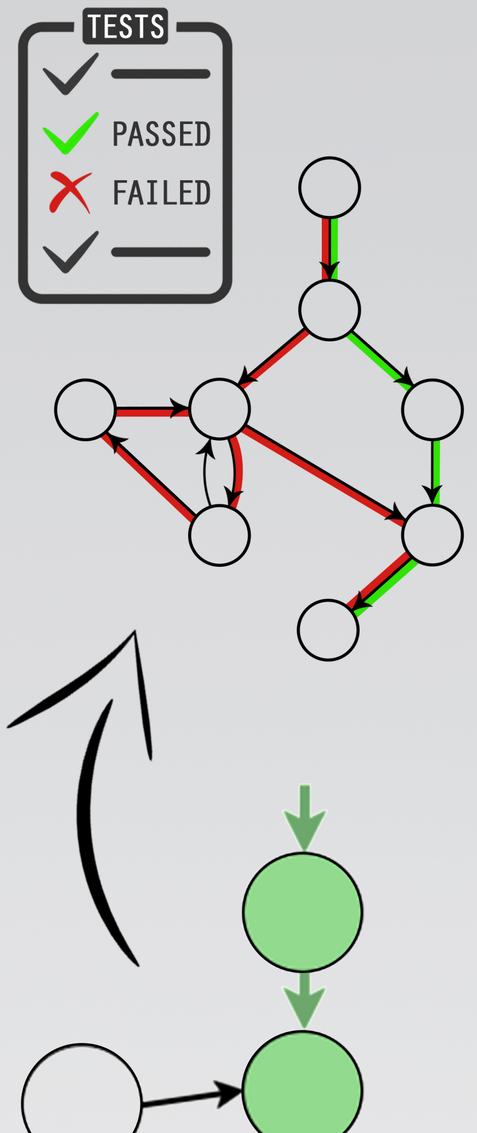
O CO JDE?

Cílem práce je vytvoření nástroje pro **extrakci grafů toku řízení** z programů v **jazyce Java**. Na základě analýzy výsledných grafů mají být **generovány testovací případy** pro daný kód. Aby bylo možné tuto analýzu provádět co nejobecněji, jsou jednotlivé instrukce bajtkódu Javy obsažené v grafech **překládány do** obecné instrukční sady **LLVM IR**.



EXTRAKCE GRAFU

Vzniklý nástroj prochází bajtkód předaného programu a **vyhledává** v něm **skokové instrukce** a cíle těchto skoků, které ohraničují sekvence instrukcí patřících do jednotlivých základních bloků. **Každá metoda** původního programu je takto **zpracována na jeden graf**, který uchovává informace o uspořádání nalezených bloků, sekvence instrukcí **i původní programové lokace**.

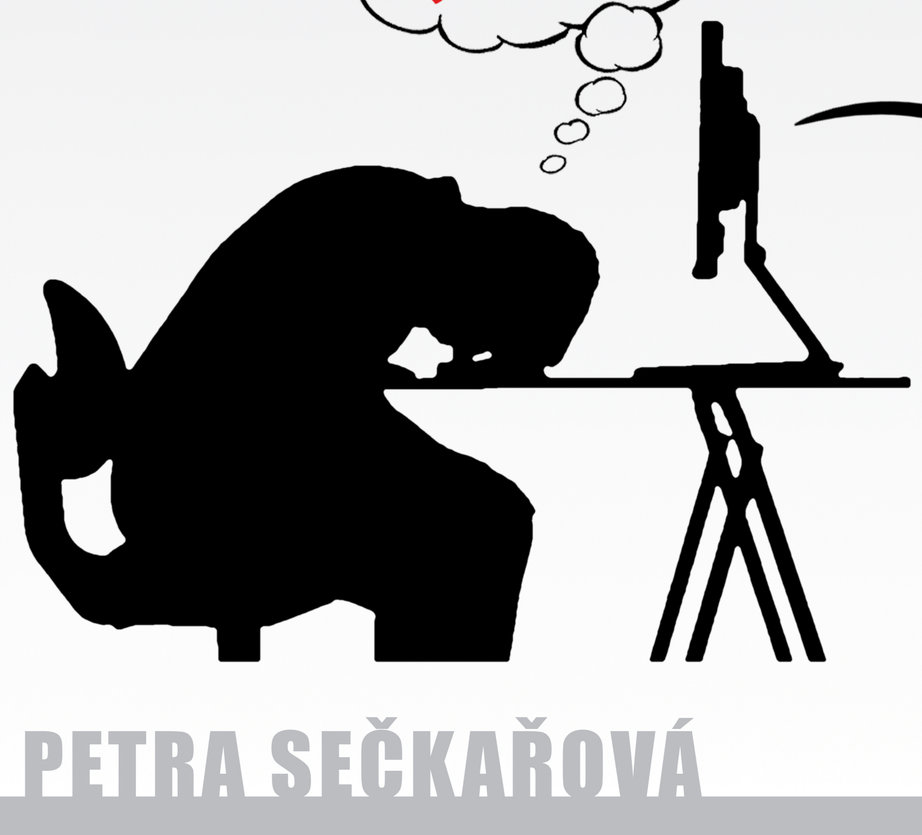


CFG CRAWLER

```
public static int foo(int, int);
  descriptor: (II)I
  Code:
     0: iload_0
     1: iconst_5
     2: if_icmple     10
     5: iload_0
     6: istore_2
     7: goto          12
    10: iload_1
    11: istore_2
    12: iload_2
    13: ireturn
  LineNumberTable:
    line 8: 0
    line 9: 5
    line 11: 10
    line 12: 12
```

PŘEKLAD DO LLVM IR

Překlad sekvencí instrukcí uvnitř nalezených základních bloků z bajtkódu Javy do instrukční sady LLVM IR je **netriviální**, protože obě **platformy jsou** velmi **odlišné**. Výsledek tohoto překladu však musí být co nejspolehlivější, aby mělo cenu přeložené instrukce dále analyzovat. Vytvořený nástroj dokáže vhodně přeložit **většinu** instrukčních **sekvencí**.



Java™ CFG

PETRA SEČKAŘOVÁ
xsecka02@stud.fit.vutbr.cz

TESTOS

Excel @FIT 2017