Spätný preklad špecializovaných a pokročilých inštrukčných sád nástrojom RetDec

02

Autor: Juraj Holub (xholub40@stud.fit.vutbr.cz)
Vedúci: Ing. Zbyněk Křivka, Phd.

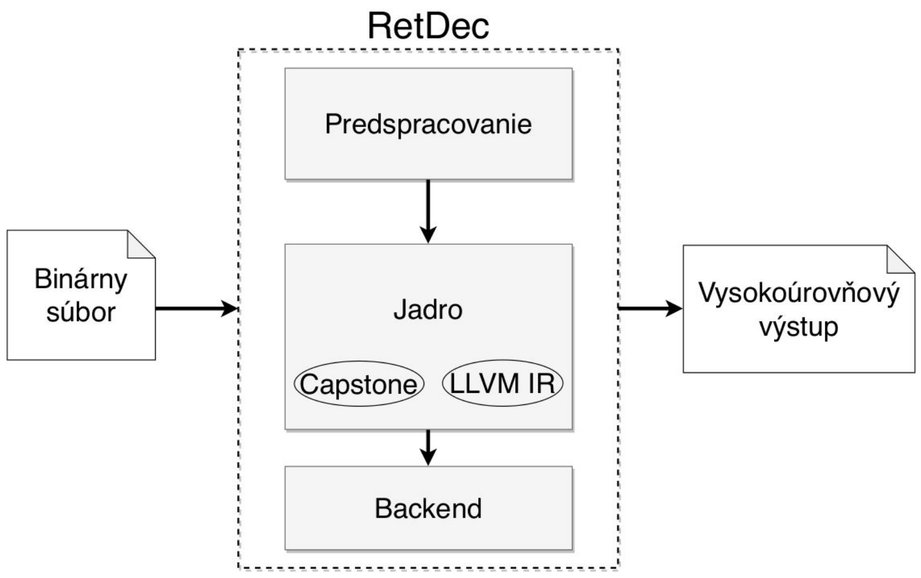
Motivácia

Kybernetická bezpečnosť

- **Malvér**: Analýza škodlivých binárnych súborov s cieľom zlepšenia ochrany.
- **Digitálny obsah:** Ochrana plateného SW pred pirátstvom a snaha o jej prelomenie.

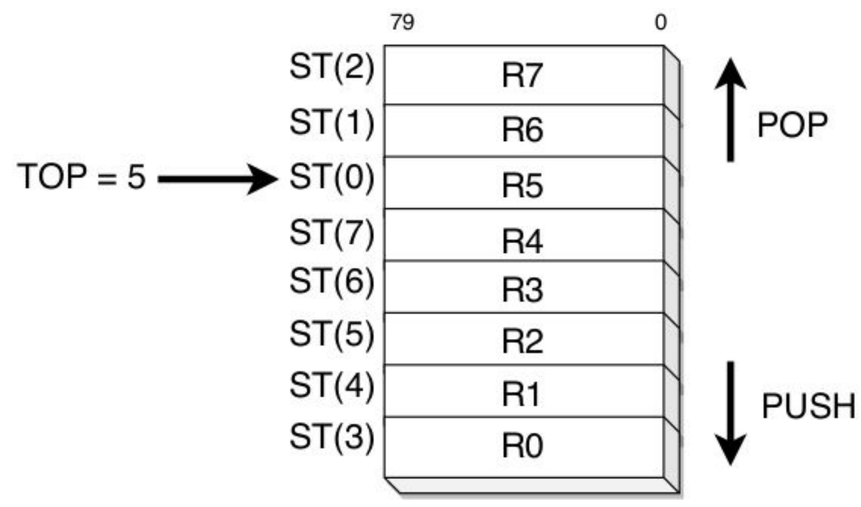
SW vývoj

- **Proprietárna SW dokumentácia**: Jednoduchá analýza nejasného chovania SW.
- **Konkurenčné súperenie**: Získavanie efektívnych riešení podčastí SW a algoritmov.



Retagetable Decompiler - RetDec

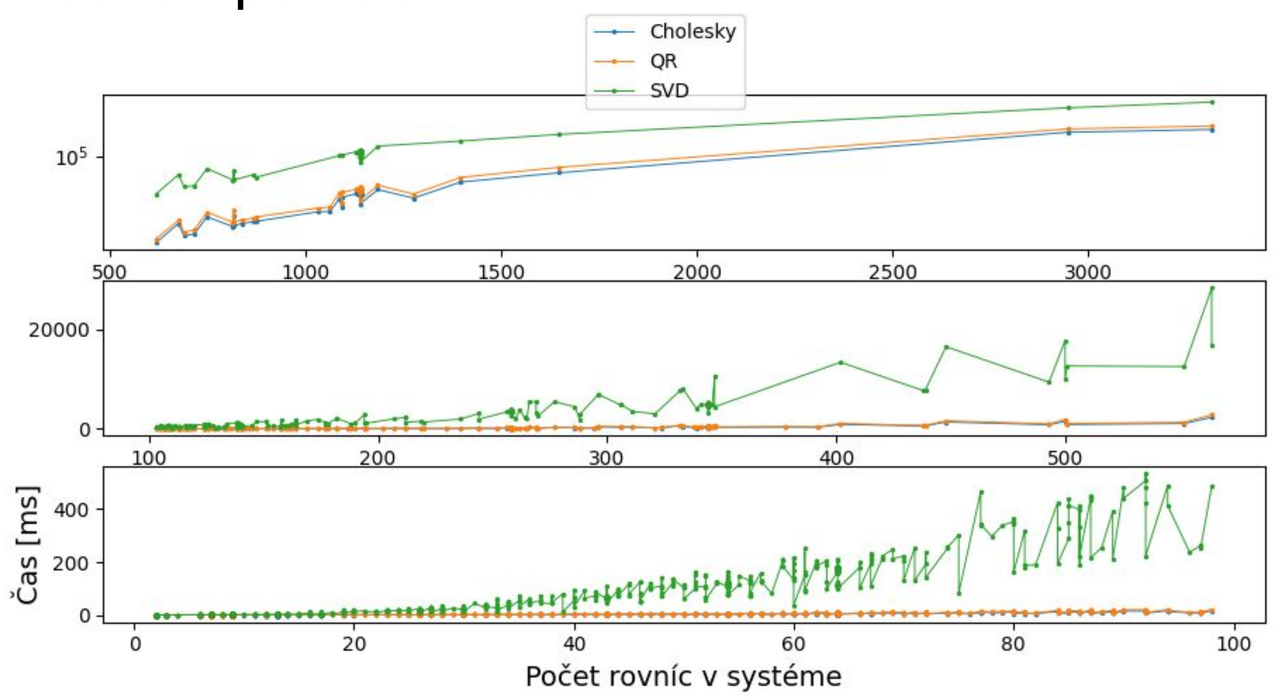
- Open-source spätný prekladač.
- Flexibilita: nezávislosť na formáte analyzovaných binárnych súborov.
- Jadro vytvára a optimalizuje IR (Intermediate Representation).



Navrhovaná optimalizácia

- **Intel x86**: **Zásobník** inštrukčnej sady **FPU.**
- **Problém**: Počas vykonávania programu sa SW označenie registru `STx` odkazuje na rôzne HW registre. Dekompilácia vyžaduje rekonštrukciu zásobníku.
- **Riešenie**: Sekvenčná analýza registrov v základnom bloku. Transformácia CFG na *preurčený* (*overdetermined*) lineárny systém rovníc. Riešenie pomocou aproximačných metód: *Cholesky*, *QR*, *SVD* dekompozícia.

```
1:    FADD  ST0 , ST1
2:    FLD1 //FPU push
3:    FADD  ST0 , ST1
```



Výsledky

- **Experimentálne meranie** skutočných binárnych súboroch (822 súborov).
- Najefektívnejšie riešenie implementuje **QR dekompozícia**.
- Optimalizácia prebehla úspešne na celej testovacej sade.
- Potenciálne zlepšenie efektivity pre veľmi rozsiahle programy.

Excel@FIT 2020

RD Retargetable Decompiler

avast!