Detekcia zneužívania bezpečnostných zraniteľností v binárnych programoch

Jozef Brandys
Školiteľ: Mgr. Peter Košinár

10.5.2017

Motivácia

- Zlepšiť detekciu - ochrániť spoločnosť pred útočníkmi
- Zabezpečiť bezpečnosť u softvéru, ktorý už nie je udržiavaný alebo má zlú bezpečnostnú reputáciu
- Detegovať nové exploity, aby sme sa mohli voči nim chrániť
- Znížiť množstvo falošných alarmov
    - Jednoduchšie používanie
    - Šetrenie peňazí na falošné alarmy

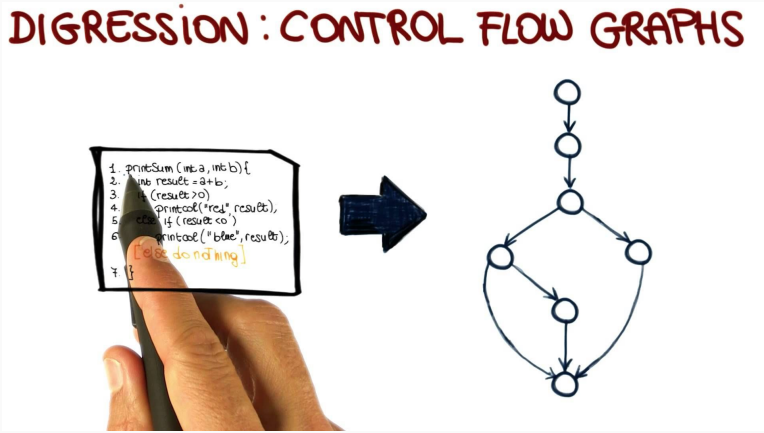
Cieľ práce

- Cieľ práce je zlepšiť metódy detekcie exploitácie, implementovať a vyhodnotiť efektívnosť navrhnutého riešenia
- Poskytnúť prehľad metód

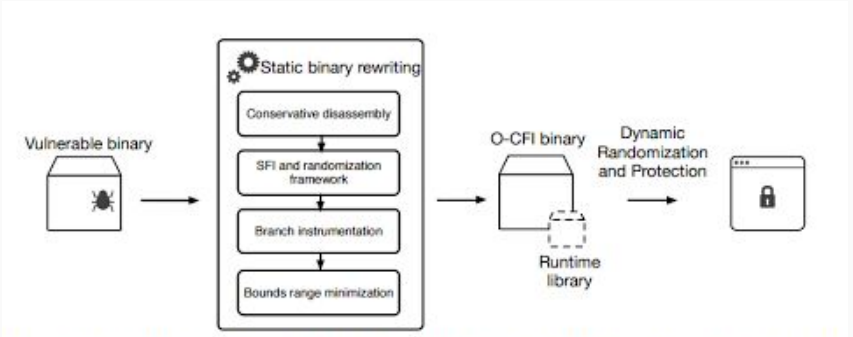
Detekcia v binárnych programoch

Detekcia v binárnych programoch

Kontrola toku programu

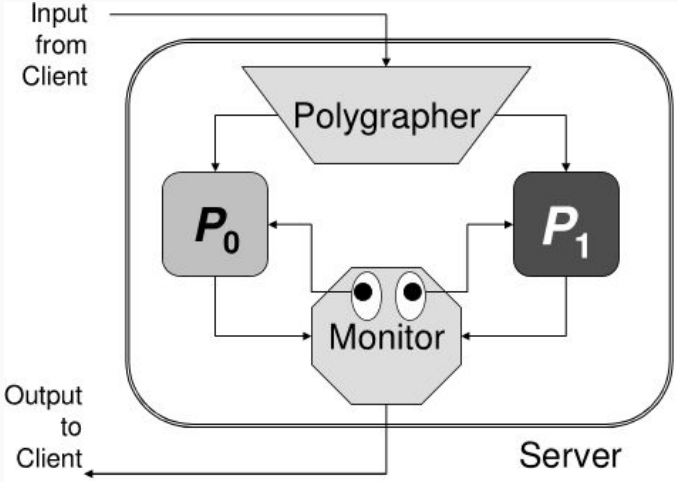


Znáhodnenie a kontrola behu

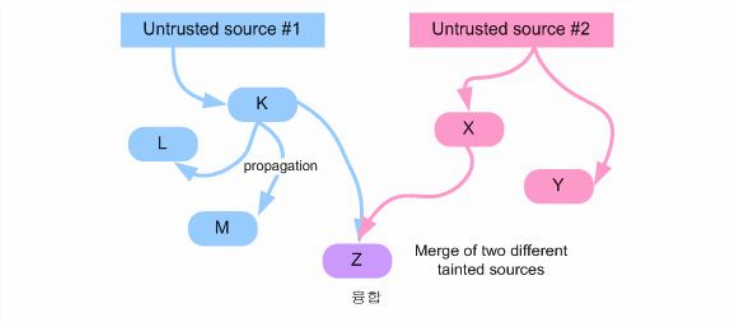


Detekcia v binárnych programoch

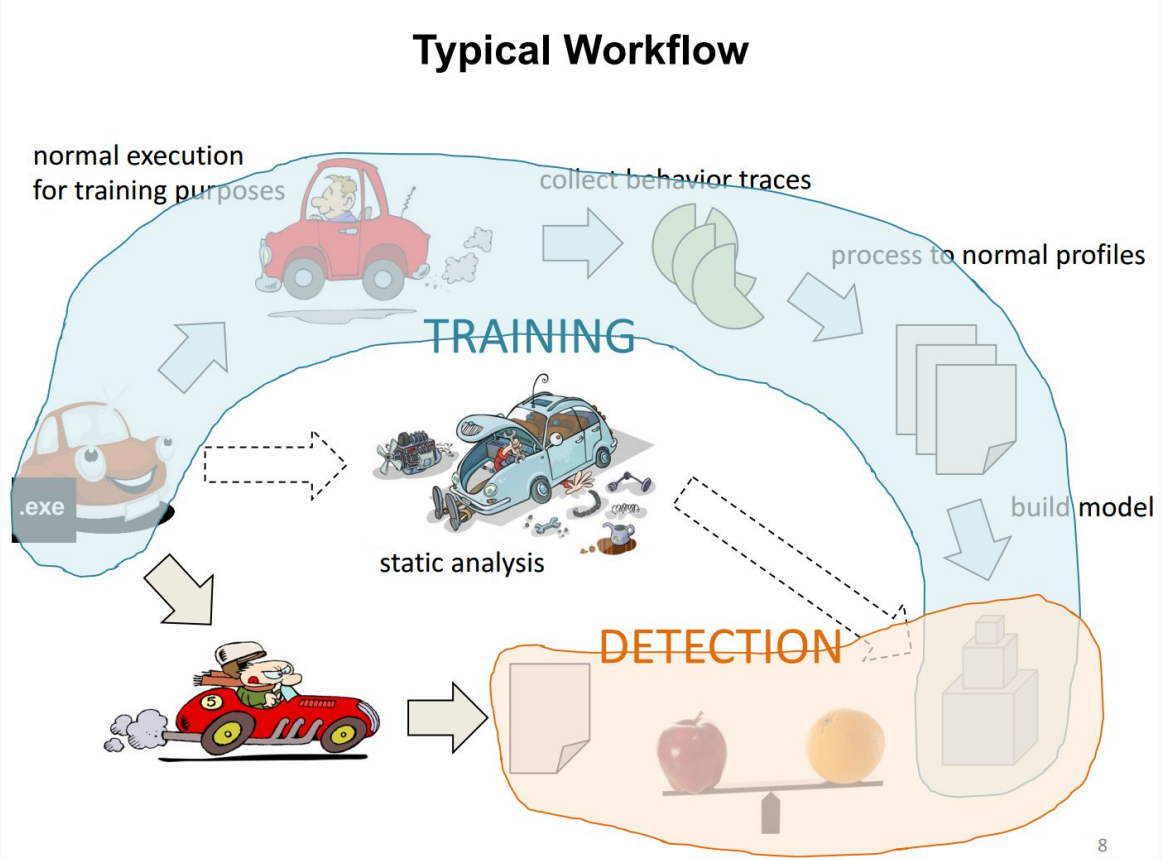
Detekcia pomocou diverzity



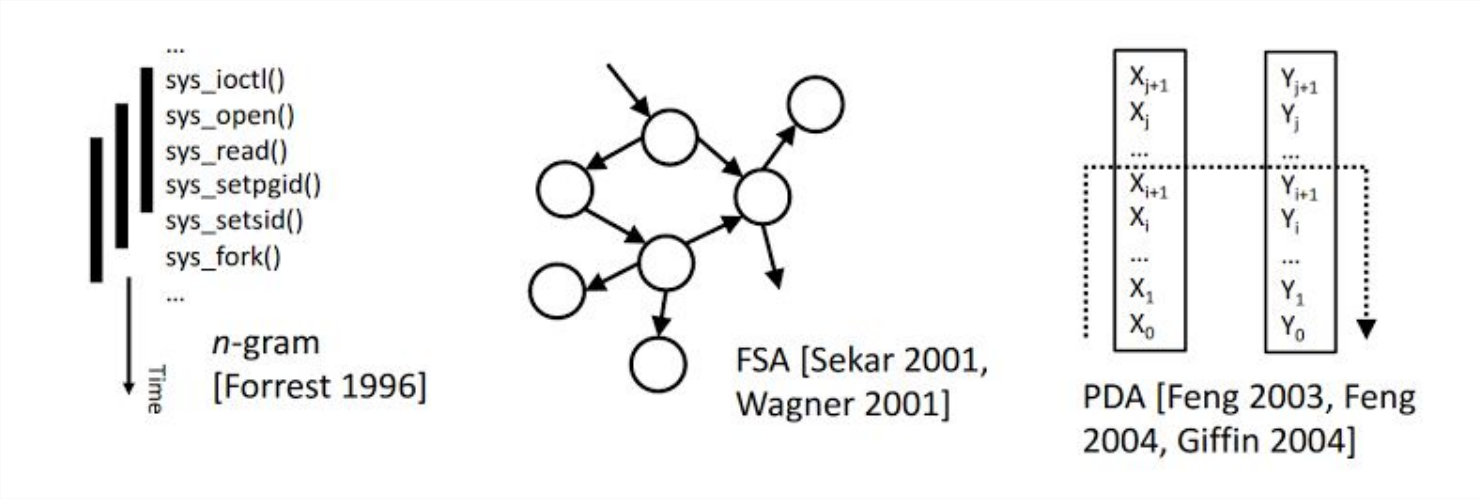
Analýza toku škodlivého vstupu



Hľadanie anomálií



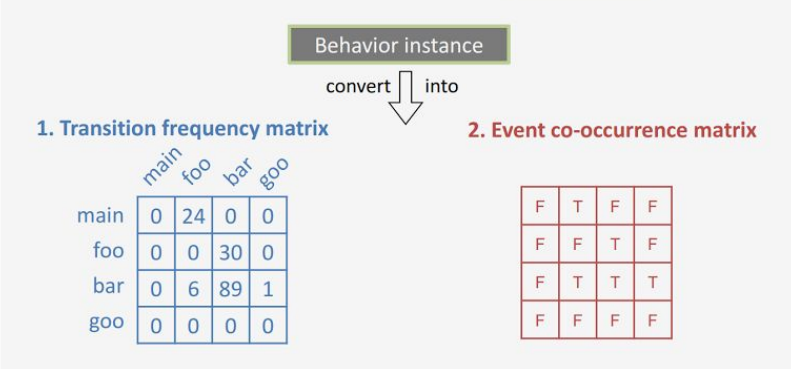
Hľadanie anomálií - N-gramy, FSA, PDA, HMM,...



Niektoré existujúce prístupy

Detekcia pomocou klasterizácie behov

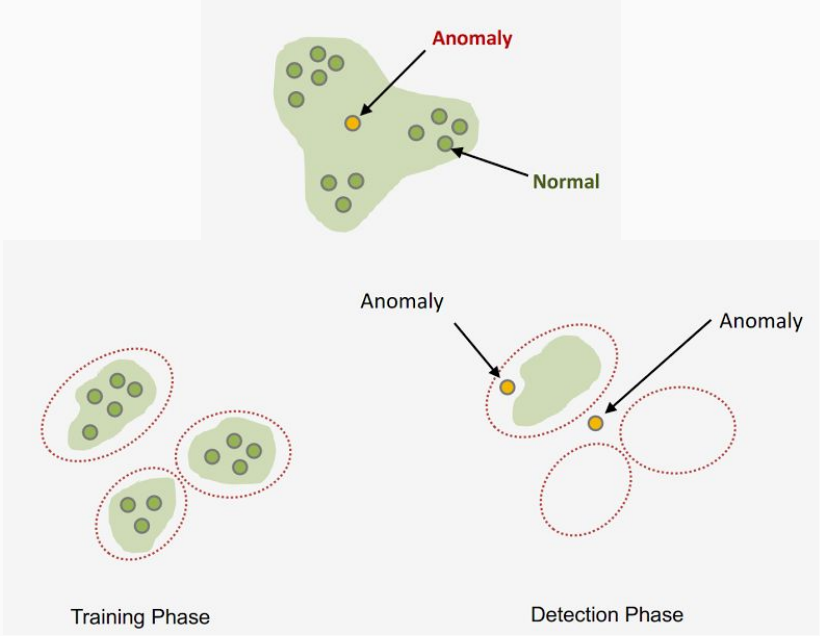
Trénovacie dáta



	main	foo	bar	goo
main	0	24	0	0
foo	0	0	30	0
bar	0	6	89	1
goo	0	0	0	0

F	T	F	F
F	F	T	F
F	T	T	T
F	F	F	F

Klasterizácia dát

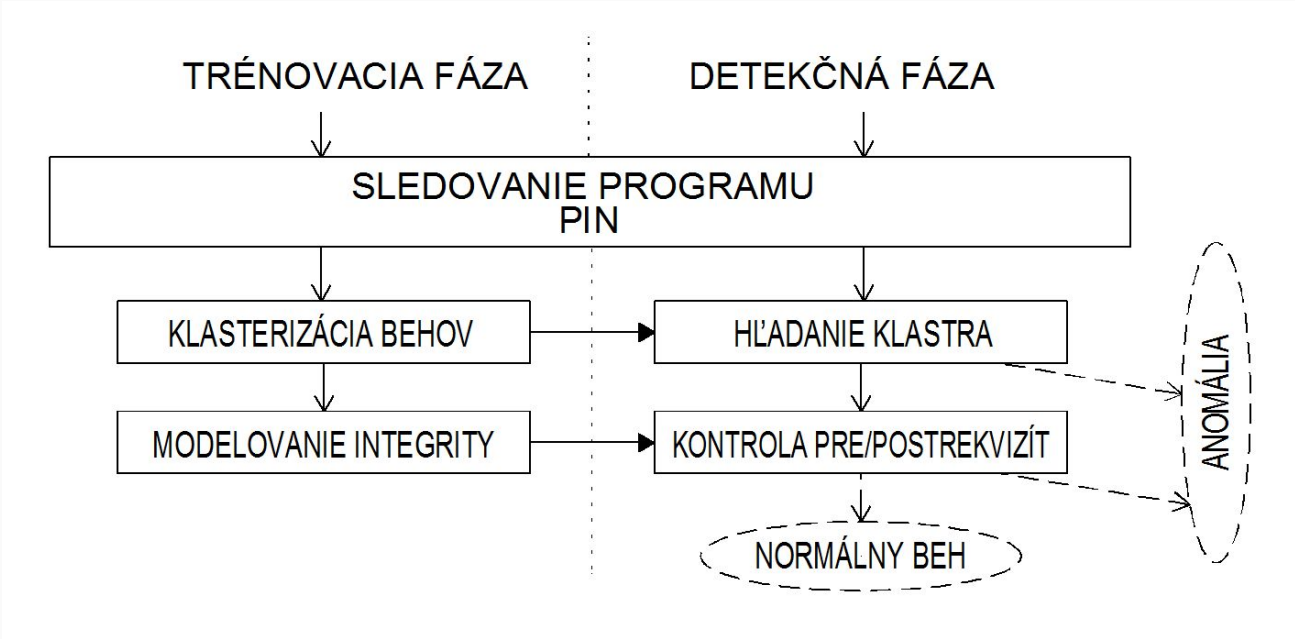


Naša práca

Zrýchlenie zberu dát

- Udalostiam sa priradia náhodné čísla
- Následne výskyt hrany zapisujeme do pamäte ako (A xor B) mod veľkosť
- Výhody
  - Malé spomalenie
  - Veľkosť pamäte lineárna od počtu rozličných hrán
- Nevýhody
  - Možné kolízie

Náš prístup - prehľad



Naše prístupy

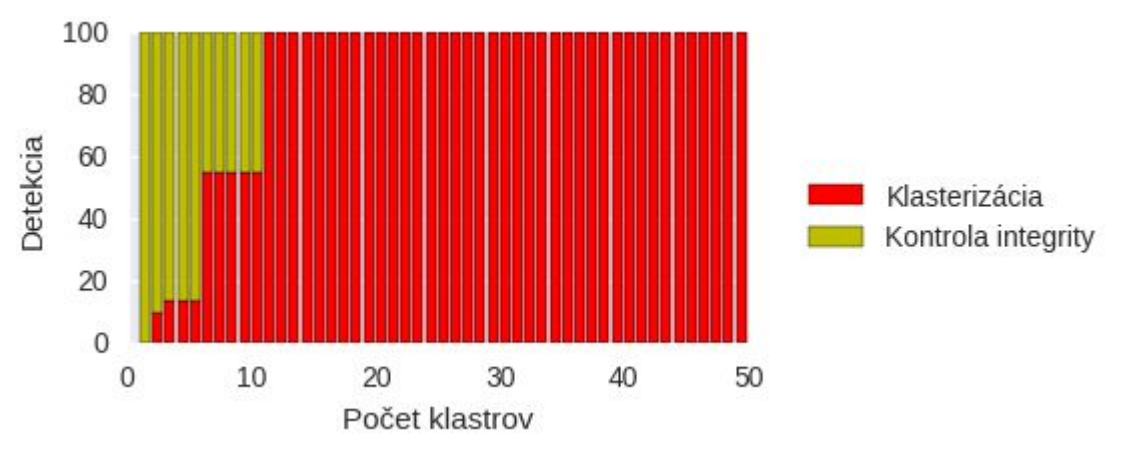
- Používame klasterizáciu na rozdelenie behov do skupín
- Vytvárame sadu podmienok - udalosti, ktoré majú nastať pred/po prvým/posledným výskytom udalosti
  - Ťažšie vytvorenie mimicry útoku
  - Zvýšenie citlivosti a dokáže detegovať potencionálne ďalšie útoky
- Pre každý klaster máme “dolný” aj “horný” obal možných udalostí

Experimentálne testovanie

- Zberanie dát pomocou
  - **Pin - A Dynamic Binary Instrumentation Tool**
- Vyhodnocovanie a trénovanie v C++

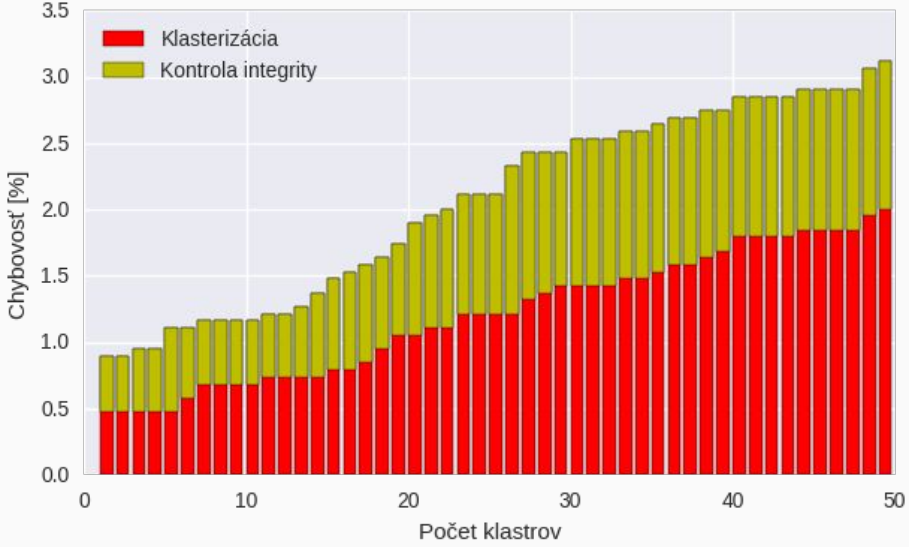
Výsledky

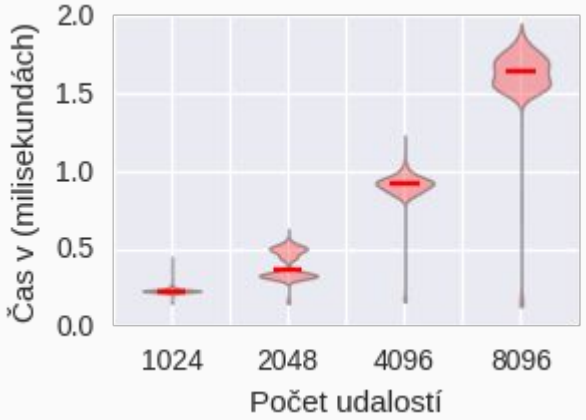
- Otestovali sme prístup na 2 zraniteľnostiach
  - Linksys
  - SSH



Detekcia pri testovaní zraniteľnosti v Linksys

Výsledky


Klasterizácia
Kontrola integrity
Chybovosť [%]
Počet klastrov
0.0
0.5
1.0
1.5
2.0
2.5
3.0
3.5
0
10
20
30
40
50


Čas v (milisekundách)
Počet udalostí
0.0
0.5
1.0
1.5
2.0
1024
2048
4096
8096

Ďakujem za pozornosť

Detekčná schopnosť od veľkosti tabuľky udalostí pre SSHD