Detekce síťových anomálií

Petr Dvořák

Obsah prezentace

- Vymezení problému
- Klasifikace síťových anomálií
- Existující metody detekce
- Cíl práce

Co je anomálie

- def.: odchylka od normálního tvaru/stavu
- Co je normální?
- Co je normální v síťovém provozu?

Klasifikace síť. anomálií

- síťové útoky
  - různé DoS, port-scan, mail-bomb, ...
- problém v síti
  - špatná konfigurace/funkce síťového prvku
  - přetížení sítě

Metody detekce

- lze dělit na dvě základní skupiny
- hledání konkrétních typů anomálií
  - využívají Pattern Matching
  - máme databázi vzorků různých útoků
  - vysoká úspěšnost
- obecné hledání všech anomálií
  - nevíme, co hledáme (viz definici)
  - menší úspěšnost, více planých poplachů

Metody pro obecnou detekci

- statistické
  - hlavní komponenta, ...
- signálové
  - (Fourierova), waveletová transformace
- umělá inteligence
  - expertní systémy (fuzzy cognitive maps, ...)

Cíl práce

- najít lepší metodu :-)
- řádně otestovat nad reálnými daty
  - ,,verifikace``
- implementovat real-time detektor anomálií využívající vybranou metodu
- použitelnost na rychlých linkách – 10 Gb/s
  - možnost paralelního zpracování
    - cluster / GPU

Současný stav

- zkoumání a testování existujících metod
- spolupráce s CIVem (reálná data, ...)
- zakoupena grafická karta ;-)
- TODO: sepsat práci k SDZ