Systém pre detekciu anomálnych tokov v IP sieťach

ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta riadenia a informatiky

Riešitelia: Bc. Juraj Hofer, Bc. Roman Helis
Vedúci práce: Ing. Ondrej Škvarek, PhD.
Konzultant: prof. Ing. Martin Klimo, PhD.

frame.time_relative	ip.src	ip.dst	tcp.srcport	tcp.dstport	frame.len	frame.cap_len	eth.type	frame.protocols	ipv6.nxt	ip.proto	kategorie
0.000000	109.200.199.21	192.168.100.2	NA	NA	246	246	2048	eth:ethertype:ip:udp:data	NA	17	5
0.005283	37.244.57.192	192.168.100.2	3724	51407	130	130	2048	eth:ethertype:ip:tcp:wow	NA	6	17
0.005332	192.168.100.2	37.244.57.192	51407	3724	54	54	2048	eth:ethertype:ip:tcp	NA	6	3
0.016566	109.200.199.21	192.168.100.2	NA	NA	234	234	2048	eth:ethertype:ip:udp:data	NA	17	32
0.039405	109.200.199.21	192.168.100.2	NA	NA	240	240	2048	eth:ethertype:ip:udp:data	NA	17	10

Motivácia

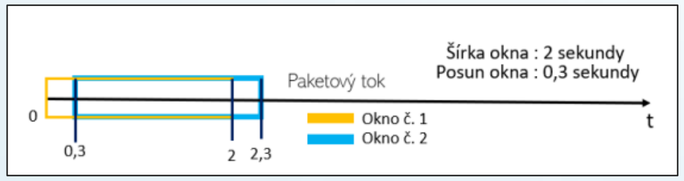
Pomocou zaznamenanej sieťovej prevádzky sa snažíme detegovať anomálie, ktoré nám pomáhajú pri odhaľovaní a predchádzaniu sieťových útokov.

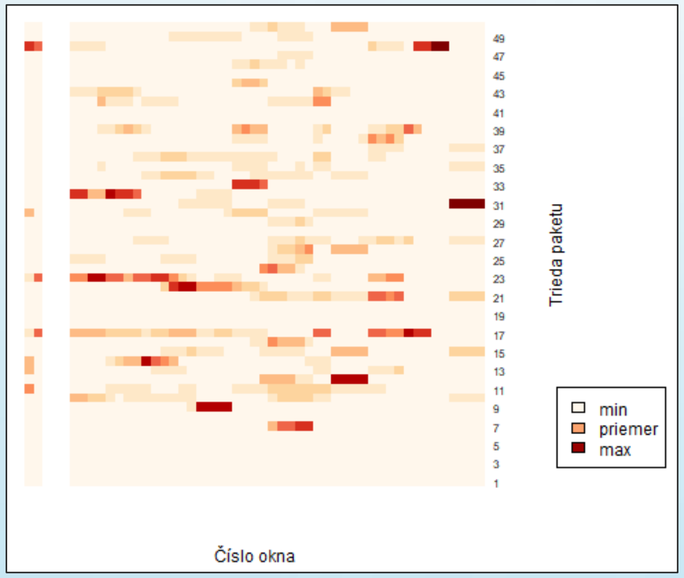
Cieľ

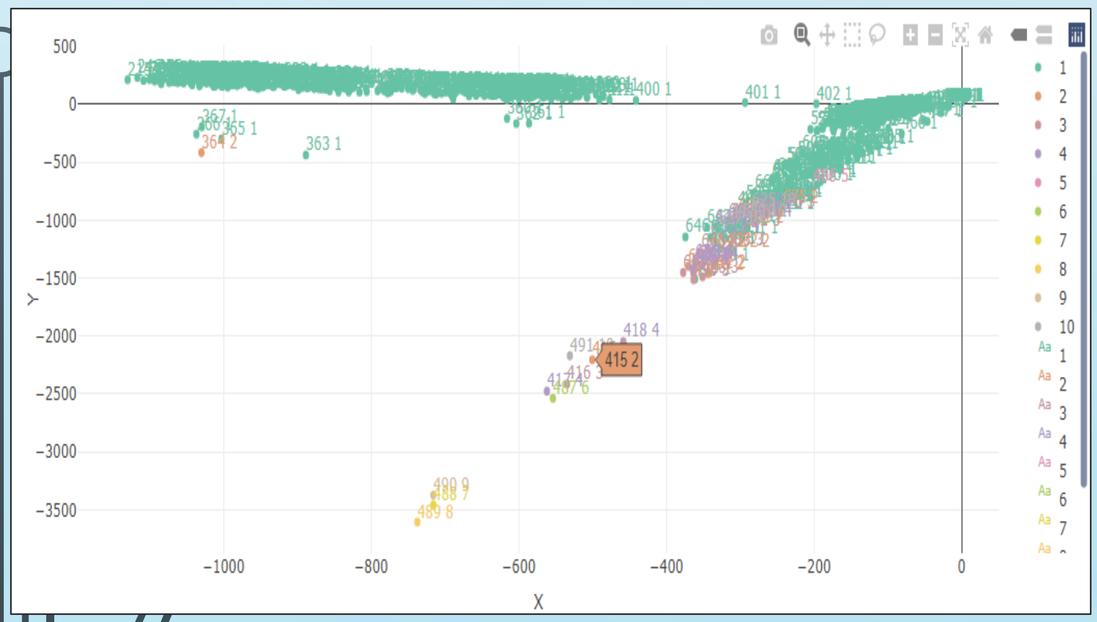
Vytvorenie komplexného systému, ktorý zo zaznamenanej sieťovej prevádzky vytvorí trénovaciu množinu, pomocou ktorej následne môžeme porovnávať a vyhodnocovať zaznamenávanú sieťovú prevádzku v reálnom čase a odhaliť anomálne toky.

Trénovanie

1. Zaznamenanie sieťovej prevádzky pomocou Wireshark-u/načítanie dát z PCAP súboru
2. Výber sledovaných polí pre dáta, podľa ktorých sa budú ďalej vyhodnocovať (napr. ip.src, ip.dst, frame.len...)
3. Kategorizácia dát podľa Shannon-Fanovho kódovania
4. Vytvorenie prekrývajúcich sa časových okien
5. Vytvorenie teplotných máp
6. Použitie hierarchického prístupu zhlukovania s výpočtom vzdialeností podľa Euklida, kde body patriace mimo polomeru sú vyhlásené za anomálne







Testovanie

Načítajú sa parametre z trénovacej množiny, spustí sa zachytávanie sieťovej prevádzky v reálnom čase.

Údaje sú po krátkych časových intervaloch ukladané do PCAP súborov, z ktorých sú načítané, postupne roztriedené do vhodných kategórií a následne prebehne ich porovnanie s trénovacou množinou a ich vyhodnotenie.

Rozšírenie aplikácie

Využitím programu Syslog získame záznamy o udalostiach na medziľahlých sieťových zariadeniach, pomocou parsovacích funkcií vyfiltrujeme potrebné informácie a pripravíme ich do vhodného tvaru ako vstupné údaje do systému aplikácie na detekciu anomálií.