Ohlédnutí se za výzkumem v oblasti bezpečnosti

Jan Kořenek a celé oddělení TMC

Začátky výzkumných aktivit

2001 – projekt sdružení CESNET „Směrovače na platformě PC"

2002 – Liberouter: součást projektu 6NET

2004 – první 10Gb SCAMPI adapter

2006 – FlowMon adaptér (GN2)
sběr Netflow statistik ze sítě
(Jiří Tobola)

2007 – spin-off společnost Invea-Tech, a.s.
akvizice společností Kemp v roce 2020

Vynikající výsledky v oblasti HW akcelerace

V roce 2007 Prezentace platformy NetCope na Xilinx Academic Fóru

Spolupráce na vývoji 10GE NetFPGA karet (Stanford, Cambridge)

- Obecná platforma pro výzkum v oblasti sítí
- Nick McKeown prezentoval nad kartami koncept OpenFlow

HW akcelerované sondy pro přesný sběr informací o síťových tocích

- Obohacení sběru dat o informace z aplikačních protokolů

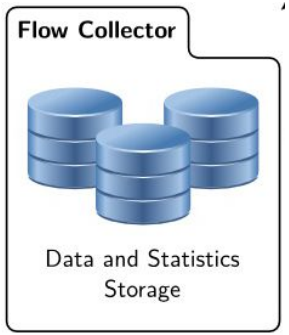
Nasazení sond na všech externích linkách sdružení CESNET (2010)

Posun k analýze síťového provozu

Zvýšení rychlosti zpracování dat na 100 Gb/s (DMON100)

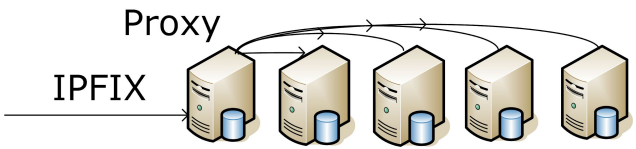
IPFIX kolektor pro ukládání dat z více sond

- Flexibilní záznam dat pro podporu aplikačních dat
- Optimalizace rychlosti ukládání a vyhledávání dat
- Podpora distribuované architektury (Security Cloud)



Systém NEMEA pro analýzu síťových dat

- framework pro proudové zpracování dat
- postupné rozšiřování sady detekčních metod

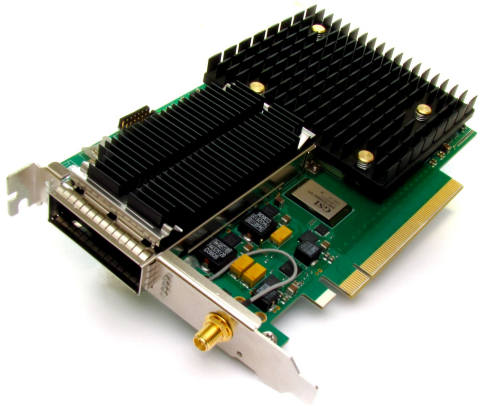


Úspěchy 100 GE technologie

Projekt DMON100 získal ocenění Nejlepší spolupráce roku

Karta COMBO-CG získala cenu *Česká hlava v kategorii Industrie*

- Komercializace společností Netcope Technologies



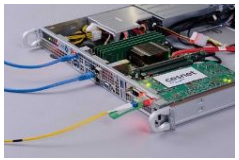
NERD a DDoS Mitigace

Reputace síťových entit (NERD)

- Výpočet FMP skóre na základě výsledků detekčních metod
- První využití technik strojového učení

DDoS Mitigace

- Reakce na nárůst DDoS útoků na připojené organizace
- Využití zkušeností s rychlým zpracování paketů pomocí akceleračních karet
- Primární zaměření na amplifikačních útoky (ochrana infrastruktury)
- Za necelý rok vytvořeno a nasazeno první řešení



Flexibilita & P4 Programovatelnost

Kompilátor jazyka P4

- Od roku 2015 návrh a vývoj vlastního kompilátoru pro technologii FPGA
- Komercializace společností Netcope Technologies
- Nyní primární kompilátor pro čipy technologie Intel

NETCOPE TECHNOLOGIES

```
table routing {
  key = { ipv4.dstAddr : lpm; }
  actions = { drop; route; }
  size : 2048;
}
control ingress() {
  apply {
    routing.apply();
}
```

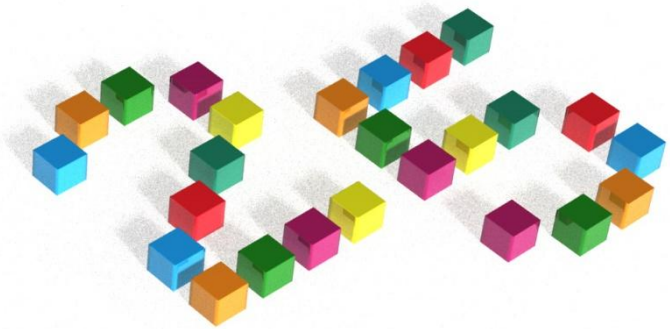
Aktuální témata

Monitorování linek na rychlosti 400 Gb/s

Analýza šifrovaného síťového provozu pomocí strojového učení

Odvozování dat z detekovaných událostí a logů

Mitigace DDoS útoků



Děkuji za pozornost!