

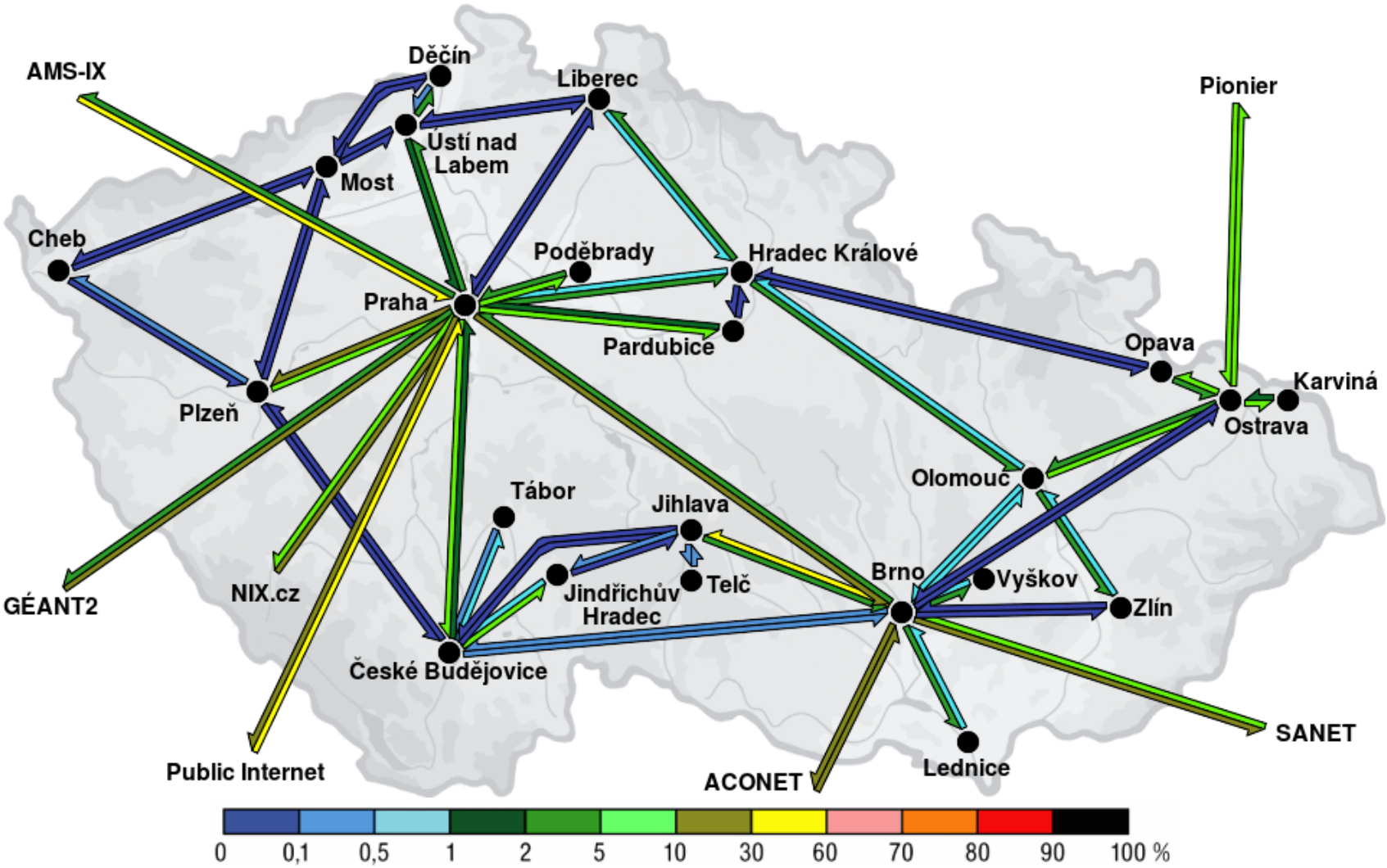

Tomáš Čejka
cejkat@cesnet.cz

Network Measurements Analysis (Nemea)

LinuxDays 2015

Počítačové sítě

Síť CESNET2



http://netreport.cesnet.cz/netreport/

Monitorování

Motivace:

- Provozní důvody
  - (Funguje infrastruktura jak má? Dostačují kapacity?)
- Účtování
  - (Uživatelé/zákazníci platí za přenesená data/využité zdroje)
- Bezpečnostní důvody
  - (Odhalení infikovaných zařízení, detekce útoků, ...)

Zpracování informací o provozu

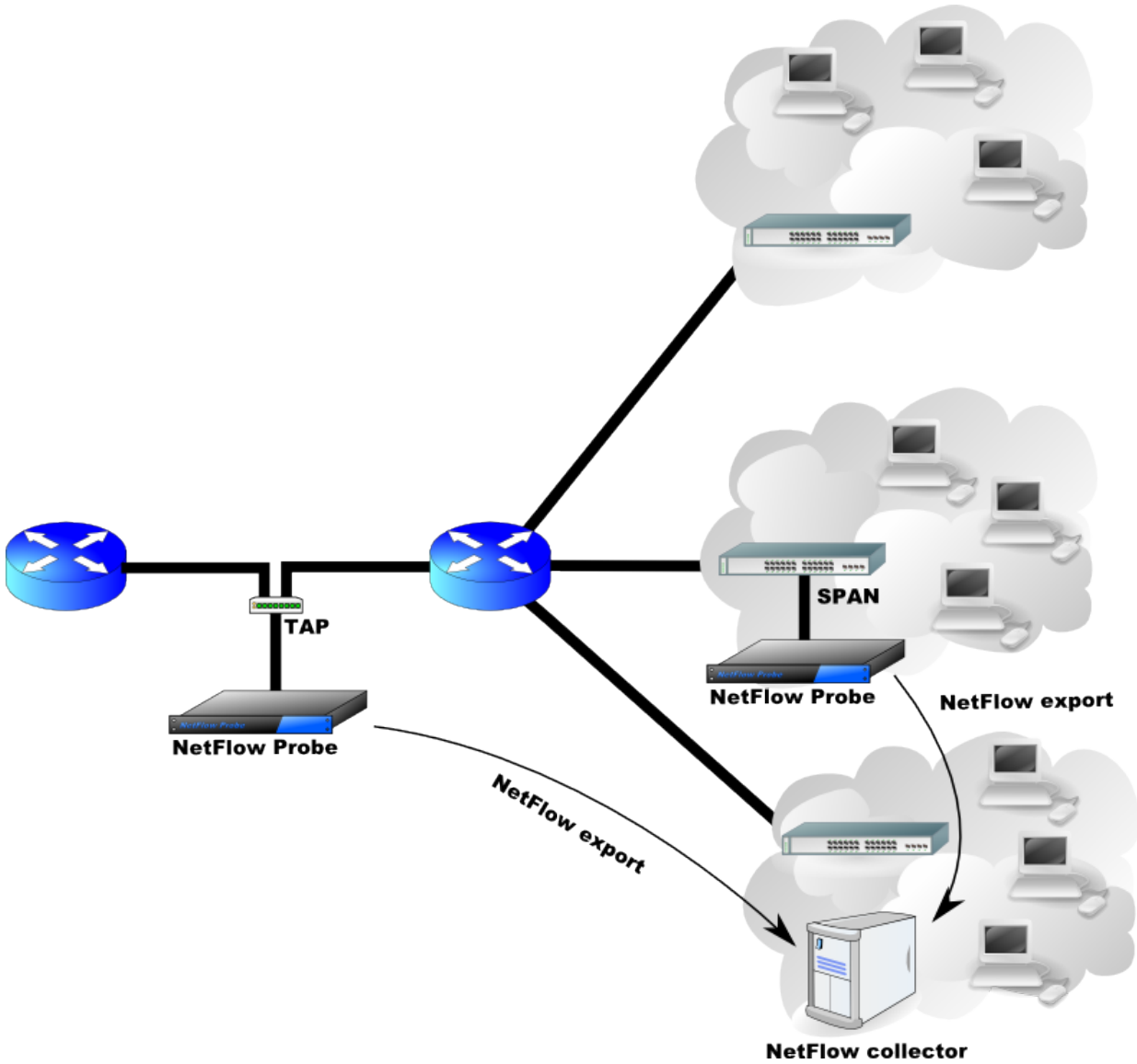
Co můžeme sledovat?

- čítače (např. SNMP)
- pakety (zachytávání celé komunikace např. tcpdump/wireshark)
- toky (agregace informací o provozu do tzv. záznamů o tocích — *flow records*)

Dnes se používá převážně flow-based monitoring.

Záznam o toku obsahuje:
adresy (L3), protokol (L4), porty (L4), objem dat, čas

Architektura netflow (flow-based monitoring)



https://en.wikipedia.org/wiki/NetFlow

Existující řešení

- Monitorovací sondy (exporter)
  např. nfdump, FlowMon, HW karta viz stánek CESNET
- Kolektor (collector)
  např. ipfixcol
- Vizualizace
  např. nfsen

Existuje spoustu komerčních i nekomerčních řešení.

Na CESNETu je „oddělení nástrojů pro monitorování a konfiguraci“, které se zabývá vývojem a výzkumem.

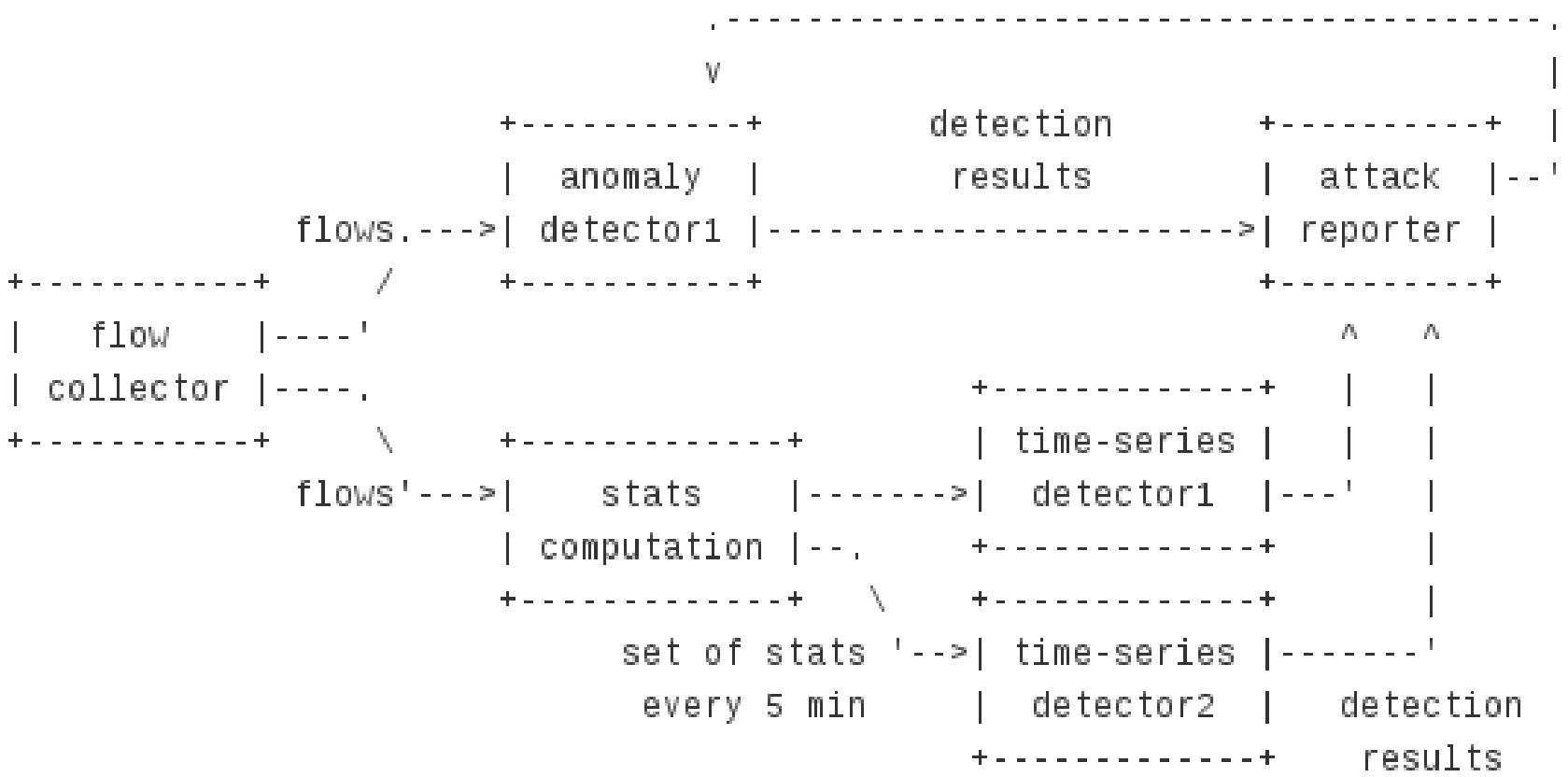
Nemea

Network Measurements Analysis

Proč Nemea?

- vyvíjeno pro velké a rychlé sítě
- **modulární rozšiřitelný** systém
- **automatická analýza** flow dat → detekce škodlivé komunikace/síťových útoků
- podpora flow dat rozšířených o informace **aplikačních vrstev**
- **proudové zpracování** → snažíme se neukládat na disk
- **kontinuální** zpracování bez fixních intervalů
- **open-source**, fungující na GNU/Linuxu

Nemea systém — ukázka



Jak to funguje

- Veřejně dostupný „Nemea framework“ → použití pro vývoj
- Nad frameworkem vznikly „Nemea moduly“ tvořící „Nemea systém“ → nasazení pro analýzu provozu

Nemea Framework řeší:

- **komunikaci** mezi moduly
- **formát zpráv** předávaných mezi moduly
- implementaci společných **datových struktur** a **algoritmů**

Co to umí?

Nemea systém jsme využili/využíváme mimo jiné pro:

- detekce zneužití **HeartBleed** (v roce 2014)
- **detekce** škodlivého provozu:
  - skenování
  - (D)DoS útoky
  - zneužití SIP ústředen
- **detekce** nežádoucího provozu:
  - komunikační tunely zneužívající DNS
- **počítání statistik** o provozu

Funkcionalitu je možné **libovolně rozšířit** přidáním nových modulů...

Jak Nemeu získám?

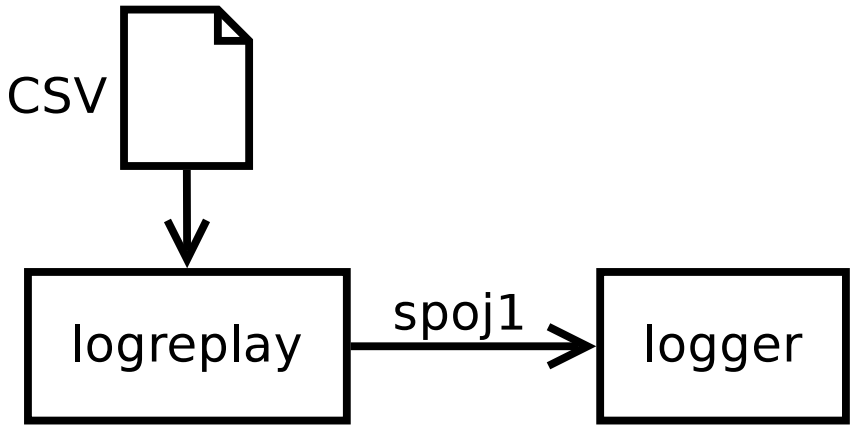
Krok 1 naklonování repozitáře:
`git clone --recursive https://github.com/CESNET/Nemea`

Dále mohu postupovat podle README ve **vagrant/**

nebo si mohu projekt zkompilovat:
`./bootstrap.sh&&./configure -q&&make -j10`

Jak začít?

Po zkompilování balíku Nemea jsou dispozici funkční ukázkové skripty v use-cases/.
Nejjednodušší ukázka propojení dvou modulů je logger-repeater.sh:



Skript `logger-repeater.sh` obsahuje:

```
../modules/logreplay/logreplay -i "u:spoj1" -f "$file"&

../modules/logger/logger -i "u:spoj1" -t
```

Skript očekává argument: CSV soubor nebo `generate`

```
use-cases$ ./logger-repeater.sh generate
ipaddr DST_IP,ipaddr SRC_IP,uint16 DST_PORT,uint16 SRC_
PORT
192.168.0.2,192.168.0.1,1234,80
1.2.3.4,8.8.8.8,53,6853
```

Chcete se zapojit do vývoje?

Rádi přivítáme další vývojáře :-)

Zpráva pro studenty:

- Baví vás programování?
- Zajímají vás počítačové sítě?
- Rádi byste pracovali na zajímavém projektu?
- Potřebujete téma závěrečné práce?

Pokud ano, napište: cejkat@cesnet.cz nebo cejkato2@fit.cvut.cz

CESNET stánek

Jste srdečně zváni na stánek CESNETu!

Čeká vás:

1. HW karta pro monitorování 100 Gb/s sítí,
2. k vidění prvky optických sítí
   (vlákna, transceivery i diagnostické nástroje, jako červený laser či měřič optického výkonu),
3. registrace na návštěvu výzkumné optické laboratoře a multimediální laboratoře SAGElab,
4. po vyplnění krátkého kvízu možnost vyhrát ceny.

Dotazy?