

Network security monitoring working group



Jan Vykopal
Masaryk University

40th TF-CSIRT meeting, London, UK

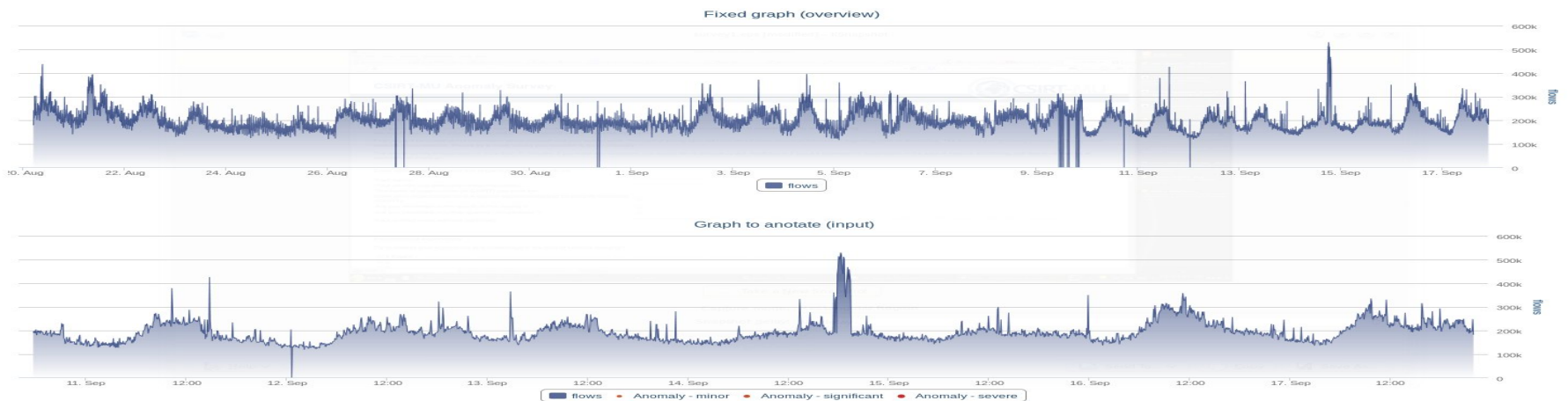
September 27, 2013

Agenda

1. Time series solver & anomaly survey
Jan Vykopal, CSIRT-MU
2. Czech Cyber Crime Centre of Excellence
Jan Vykopal, CSIRT-MU
3. BGP Ranking – update
Raphael Vinot, CIRCL
4. ???
Anyone else?

Time series solver & anomaly survey

Jan Vykopal
CSIRT-MU



Tools developed by CSIRT-MU

- NfSen plugins:
 - RDPMonitor – RDP brute-force attacks detection
 - SSHMonitor – SSH brute-force attacks detection
 - Honeyscan – honeynet monitoring plugin (feeds Team Cymru)
- Other tools:
 - NfPluggger – plugin template generator for NfSen
 - PhiGARo – for management and resolution of phishing incidents
 - NetFlow and IPFIX Geolocation Tools
 - Plugins for HTTP Monitoring
 - IPFIX Export Plugin
- Available at <http://www.muni.cz/ics/services/csirt/tools/> and <http://www.muni.cz/ics/920232/web/>

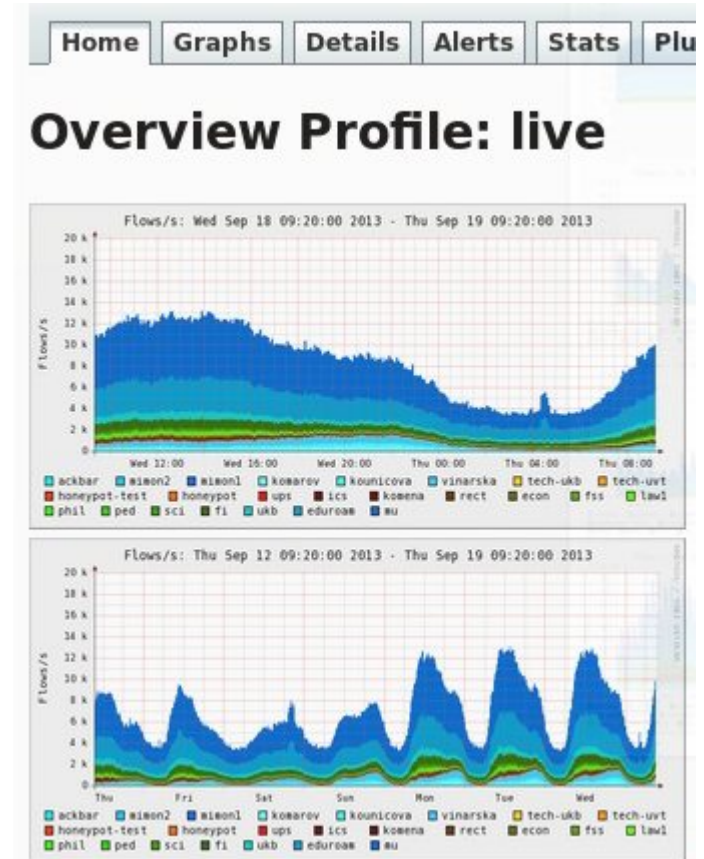


Time series analysis

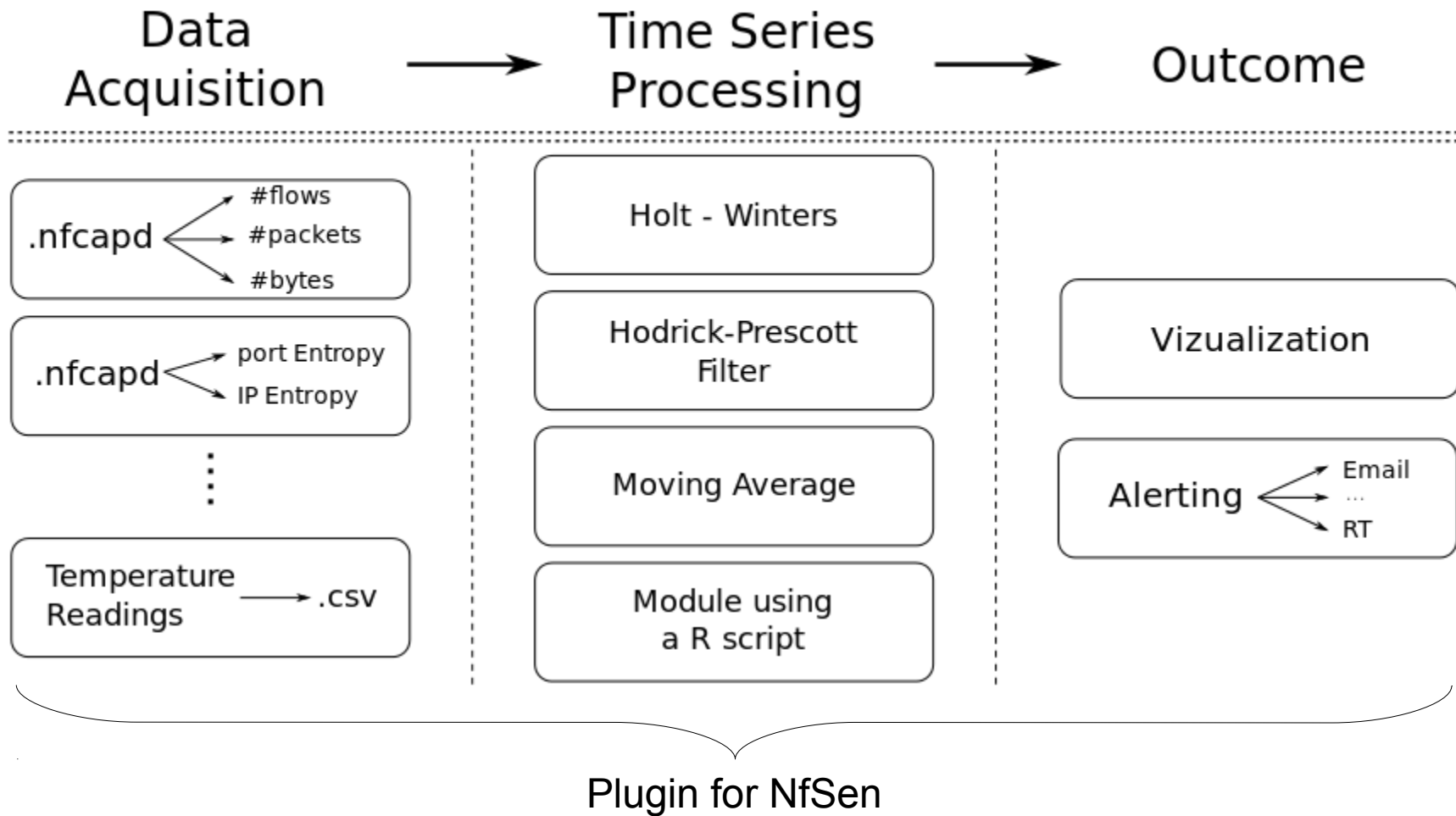
Motivation

Requirements:

- Automatic anomaly detection
- Automatic parameter settings
- Extensibility
- No suitable tools for time series analysis available
- Is Holt-Winters dead?



Time series solver (TSS) Architecture



Time series solver (TSS)

Detection methods

- Main idea:
 - 1) Predict the network behavior
 - 2) If prediction differs "*significantly*", mark as anomaly
- Detection methods
 - Moving average
 - Holt – Winters exponential smoothing
 - Hodrick - Prescott filter

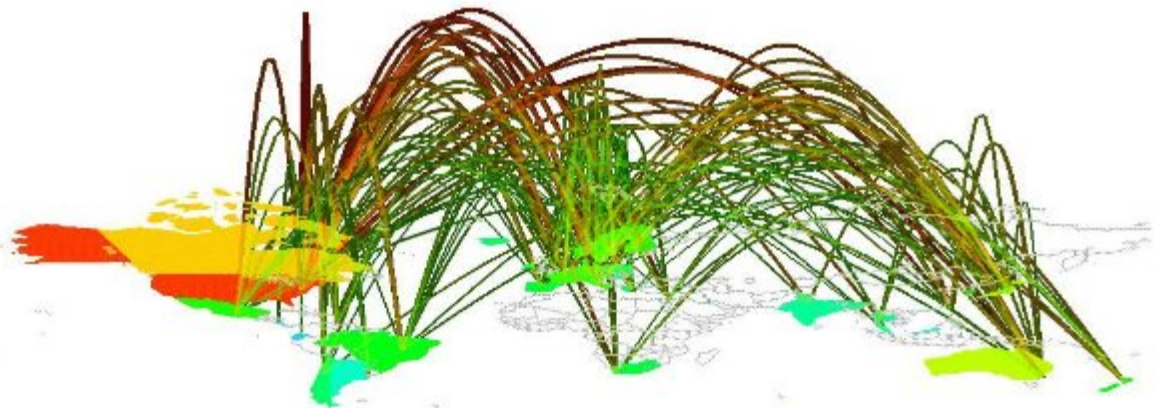
Time series solver (TSS)

Reporting

- Anomaly needs to be
 - reported with context
 - visualized



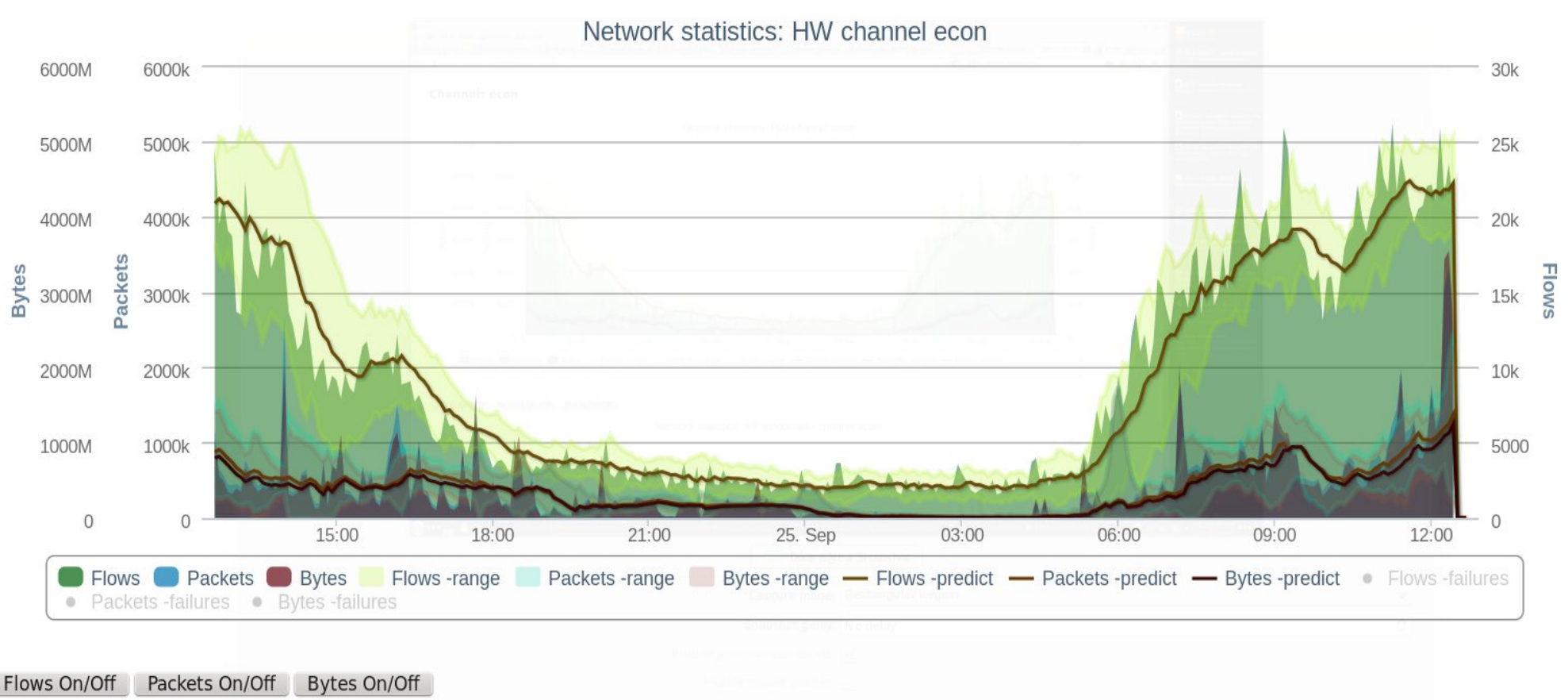
- Reporting via
 - e-mail
 - ticket system
 - early warning/data sharing system (Warden)



Time series solver (TSS)

Screenshots

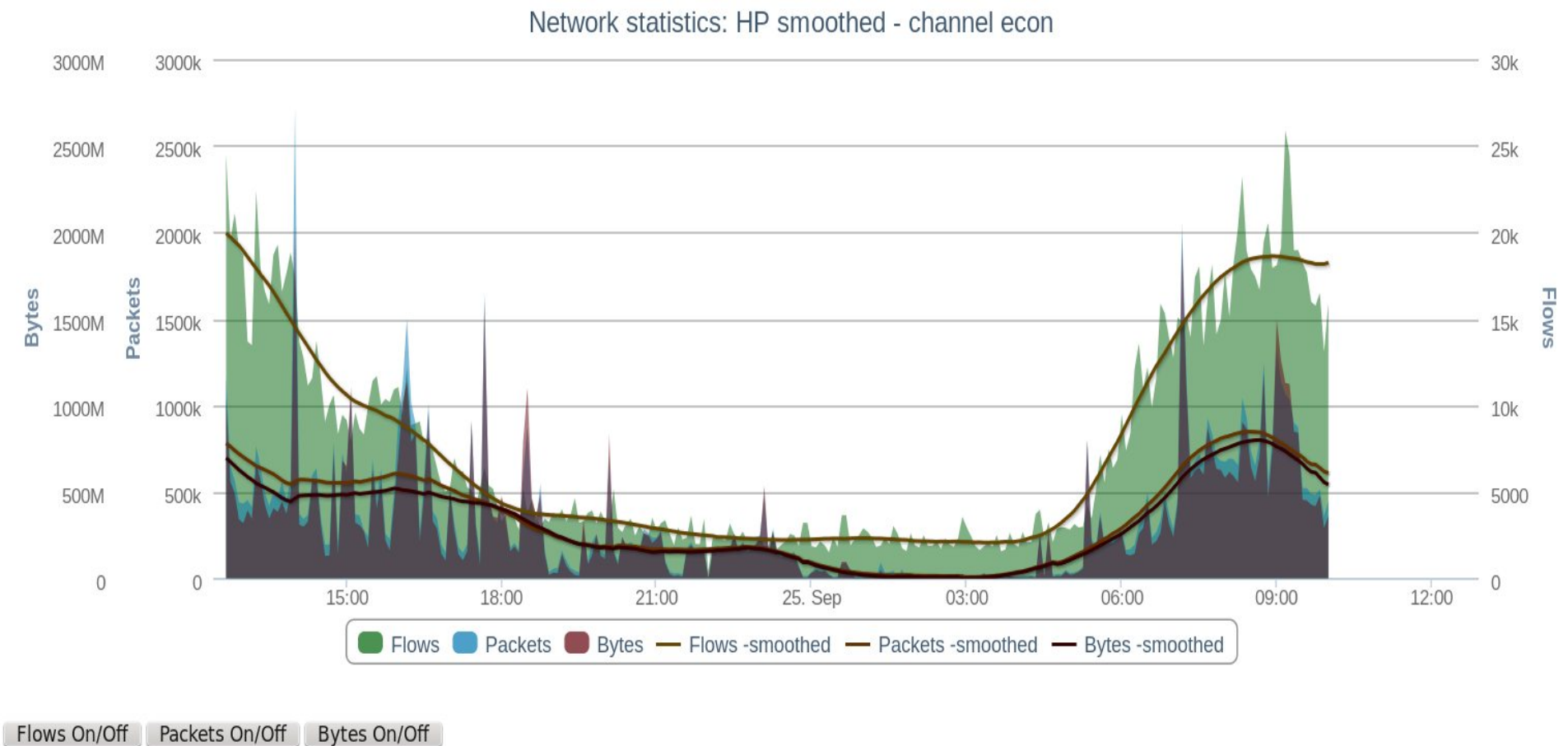
Holt-Winters method



Time series solver (TSS)

Screenshots

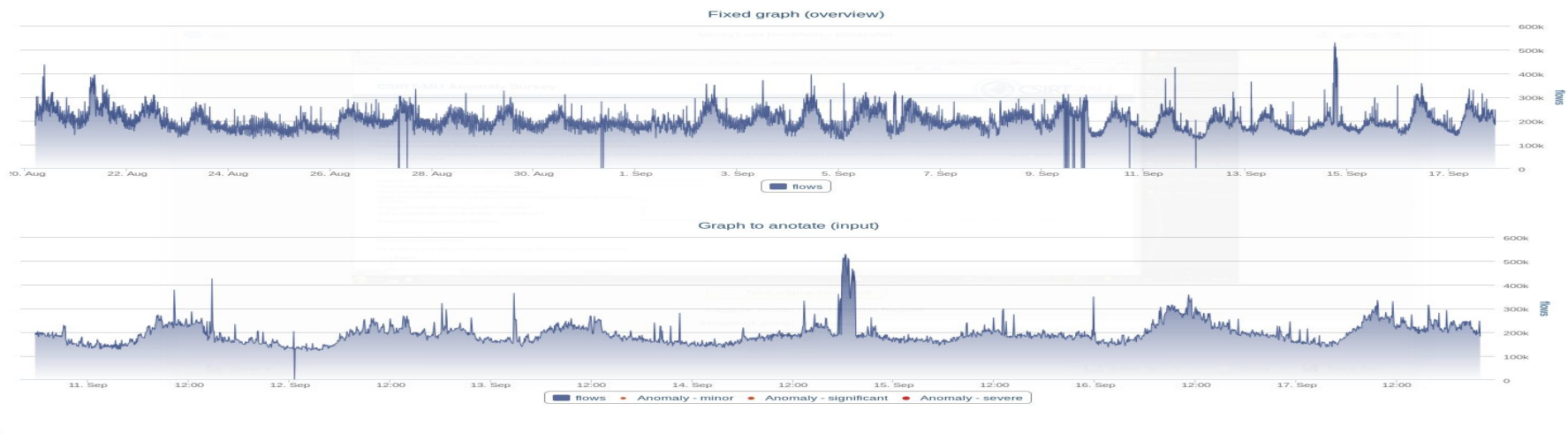
Hodrick – Prescott filter



Anomaly Survey

See https://security.ics.muni.cz/anomaly_survey/

The survey is open for anyone interested until
November 30, 2013.



Network security monitoring working group



<http://muni.cz/csirt>

Jan Vykopal

vykopal@ics.muni.cz