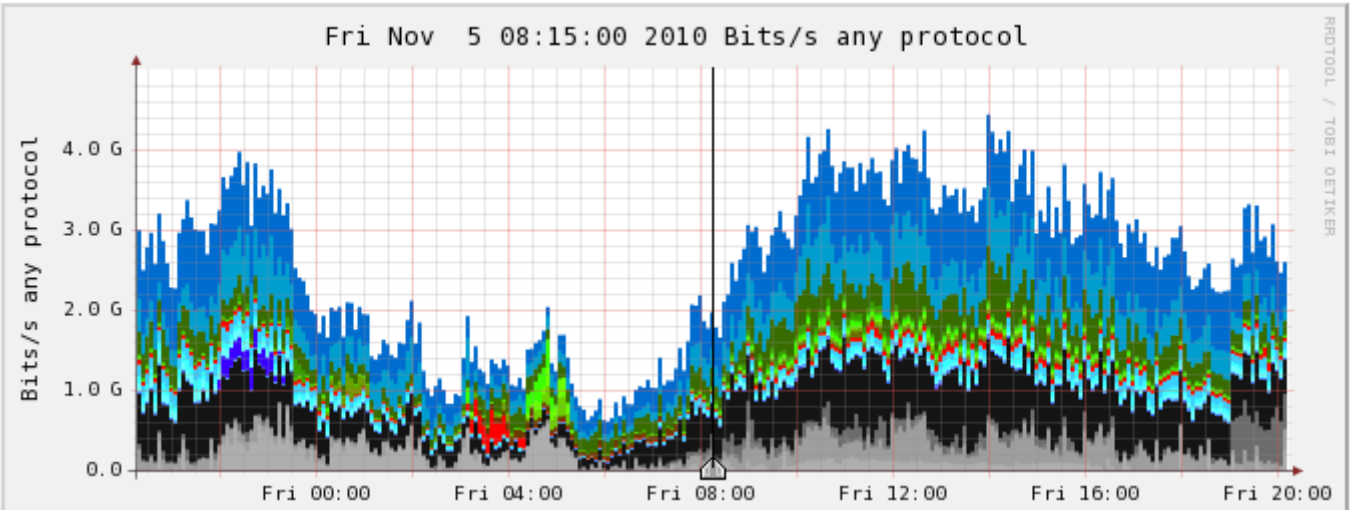
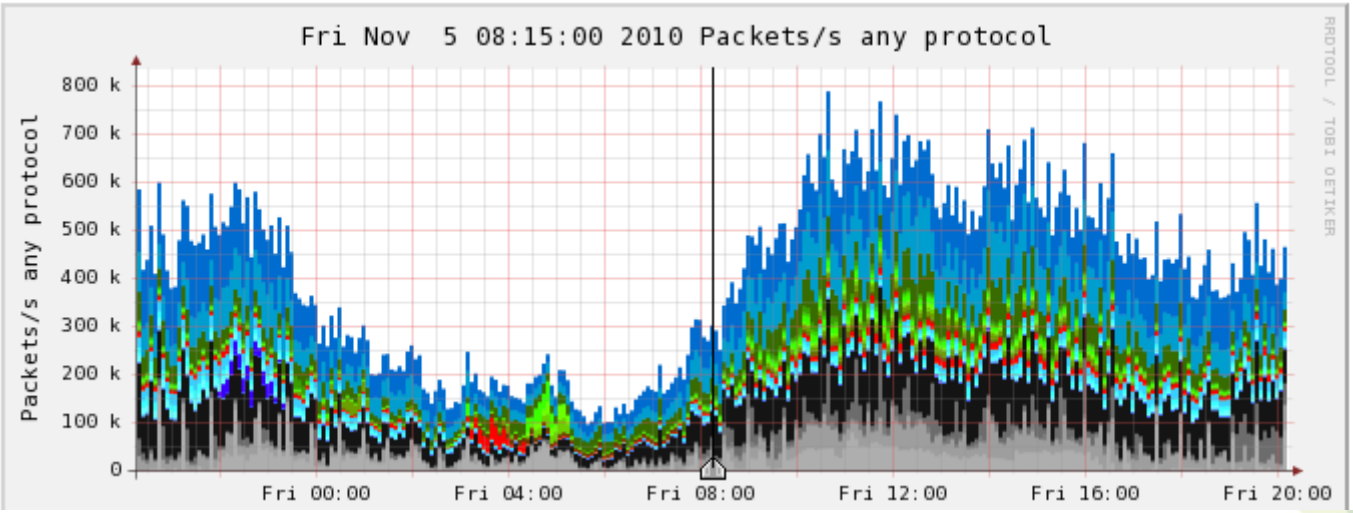
Network Security Hardening Framework

Martin Drašar
drasar@ics.muni.cz

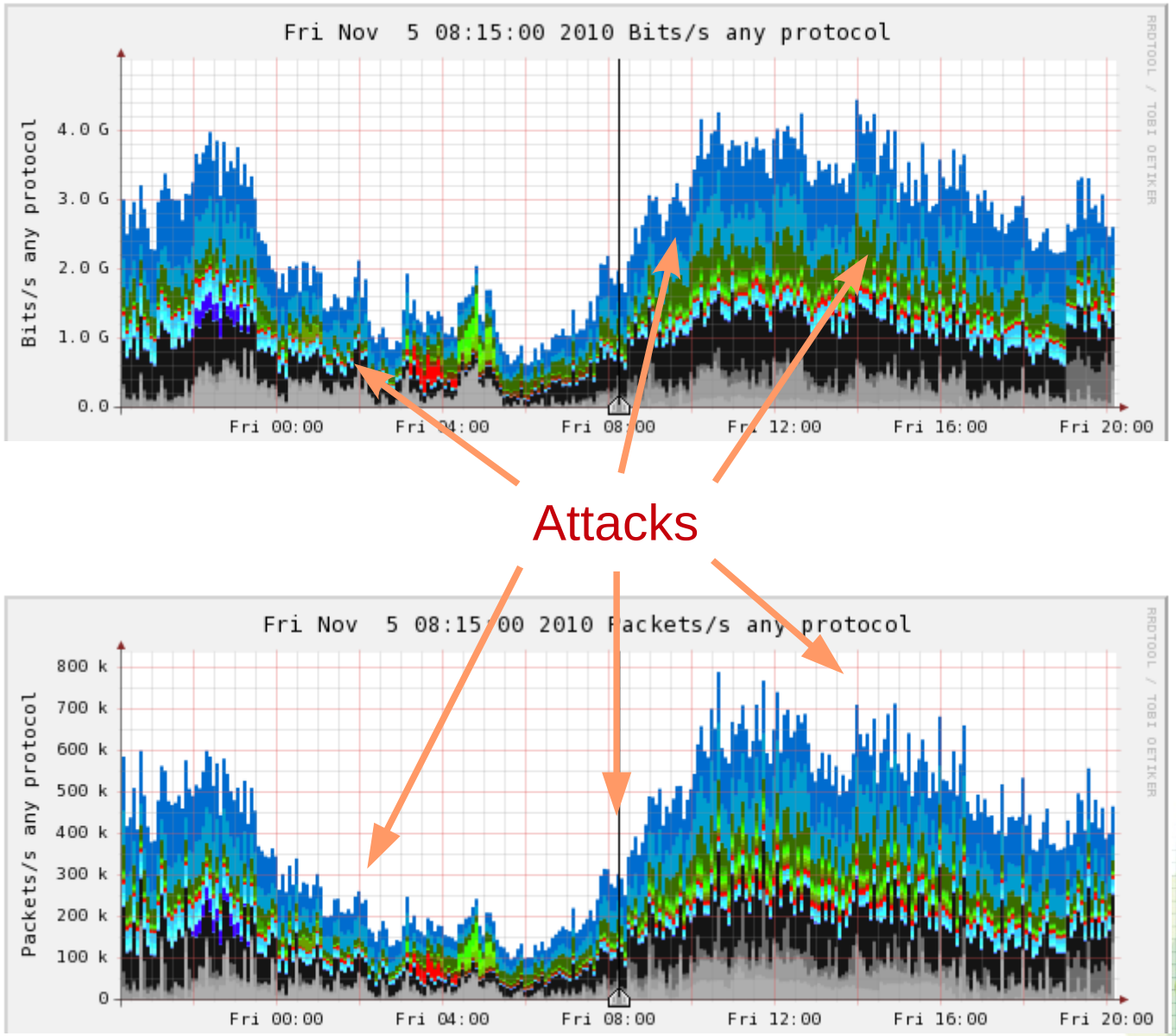
9. 11. 2010

Problem...


Fri Nov 5 08:15:00 2010 Bits/s any protocol
Bits/s any protocol
4.0 G
3.0 G
2.0 G
1.0 G
0.0
Fri 00:00
Fri 04:00
Fri 08:00
Fri 12:00
Fri 16:00
Fri 20:00
RRDTOOL / TOBI OETIKER

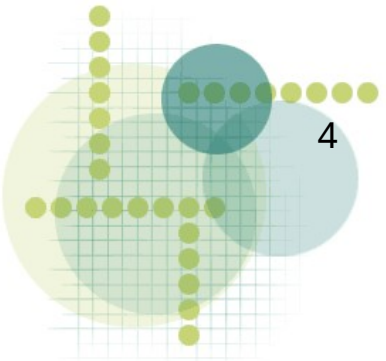

Fri Nov 5 08:15:00 2010 Packets/s any protocol
Packets/s any protocol
800 k
700 k
600 k
500 k
400 k
300 k
200 k
100 k
0
Fri 00:00
Fri 04:00
Fri 08:00
Fri 12:00
Fri 16:00
Fri 20:00
RRDTOOL / TOBI OETIKER

Problem...


Fri Nov 5 08:15:00 2010 Bits/s any protocol
Bits/s any protocol
4.0 G
3.0 G
2.0 G
1.0 G
0.0
Fri 00:00
Fri 04:00
Fri 08:00
Fri 12:00
Fri 16:00
Fri 20:00
RRDTOOL / TOBI OETIKER
Attacks
Fri Nov 5 08:15:00 2010 Packets/s any protocol
Packets/s any protocol
800 k
700 k
600 k
500 k
400 k
300 k
200 k
100 k
0
Fri 00:00
Fri 04:00
Fri 08:00
Fri 12:00
Fri 16:00
Fri 20:00
RRDTOOL / TOBI OETIKER

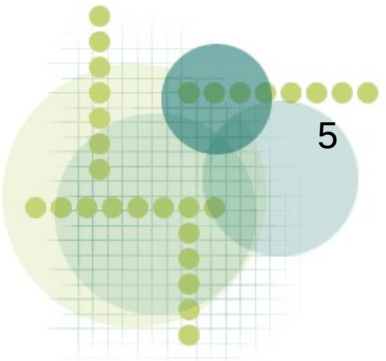
Presenation Outline

- Current detection methods
- The aspect-based detection
- WitchdOCtoR – the distributed bruteforcer
- Goals of thesis



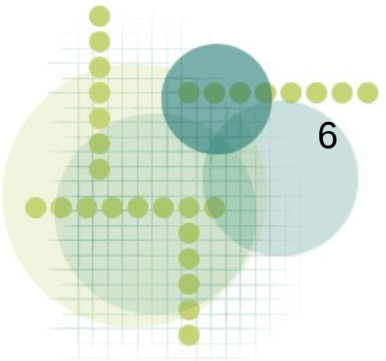
Deep Packet Inspection

- Analysis of individual packets
- Signature-based method
- Very good at detecting known attacks
- Cannot detect anything new
- Does not scale well – unsuitable for multigigabit networks



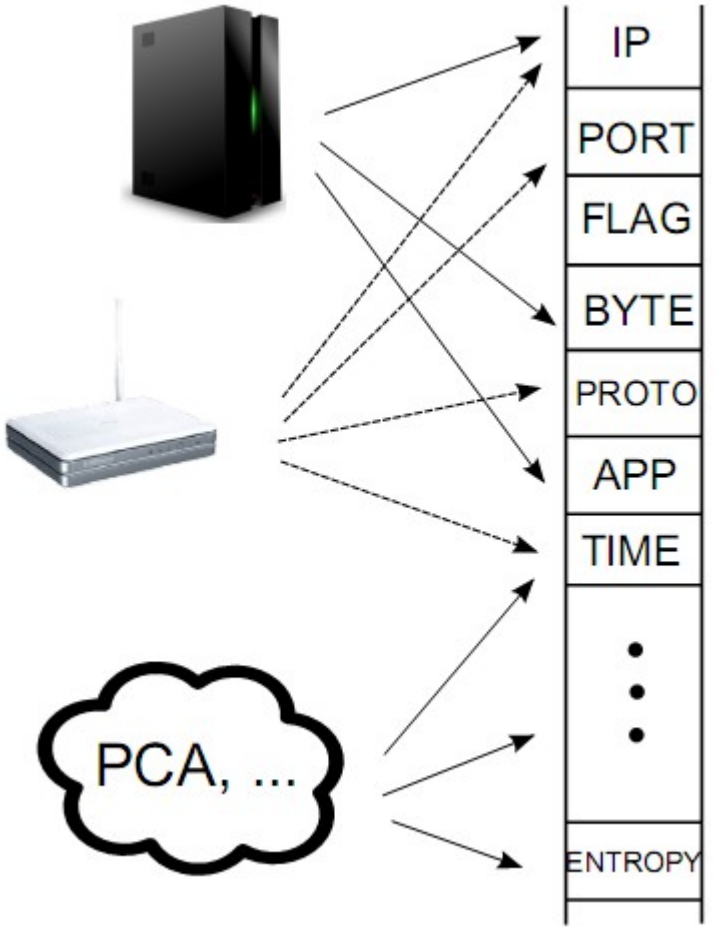
Behavioral Analysis

- Analysis of aggregated data
- Looking for abnormalities in network traffic
- Statistical methods
  - Time series
  - Principal component analysis
- In theory – can detect unknown attacks, can reasonably detect known attacks and scales well
- In real life – scales well



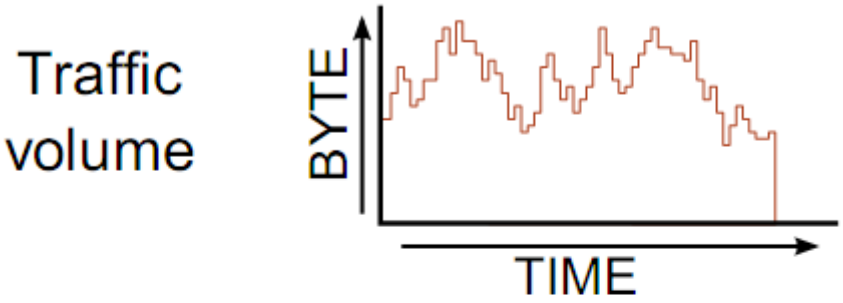
The Aspect-based Detection I.

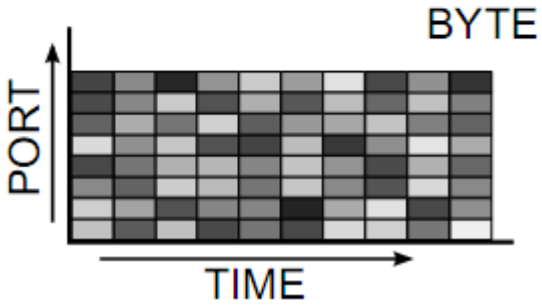
- Takes various traffic descriptors as an input
  - addresses, ports, protocols, entropy, …
- Sources
  - Switches
  - Routers
  - Probes
  - Other methods



The Aspect-based Detection II.

- Aspect – subset of available traffic descriptors
- Feature of traffic
- n-dimensional array



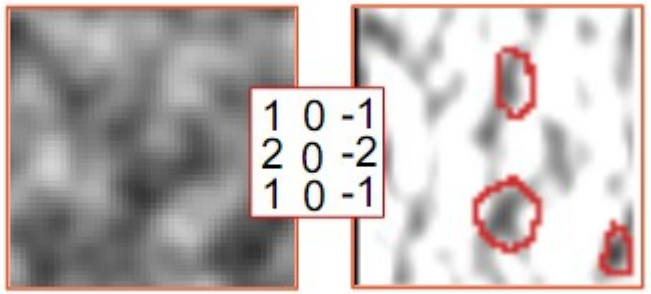


Service usage

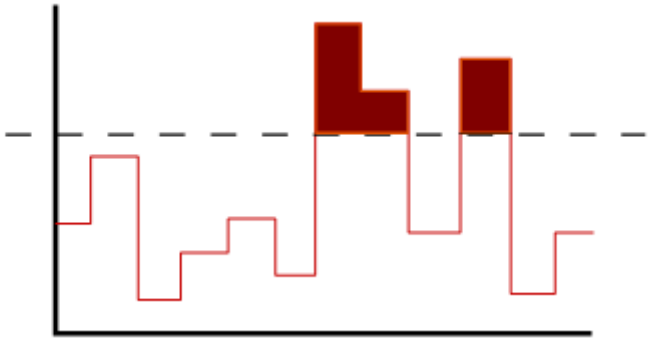
The Aspect-based Detection III.

- Aspects analyzed for deviations
- Arbitrary methods for detection
- Best suited for non-linear filters
  - detect static deviations
- and linear filters
  - detect deviations in trends

LINEAR

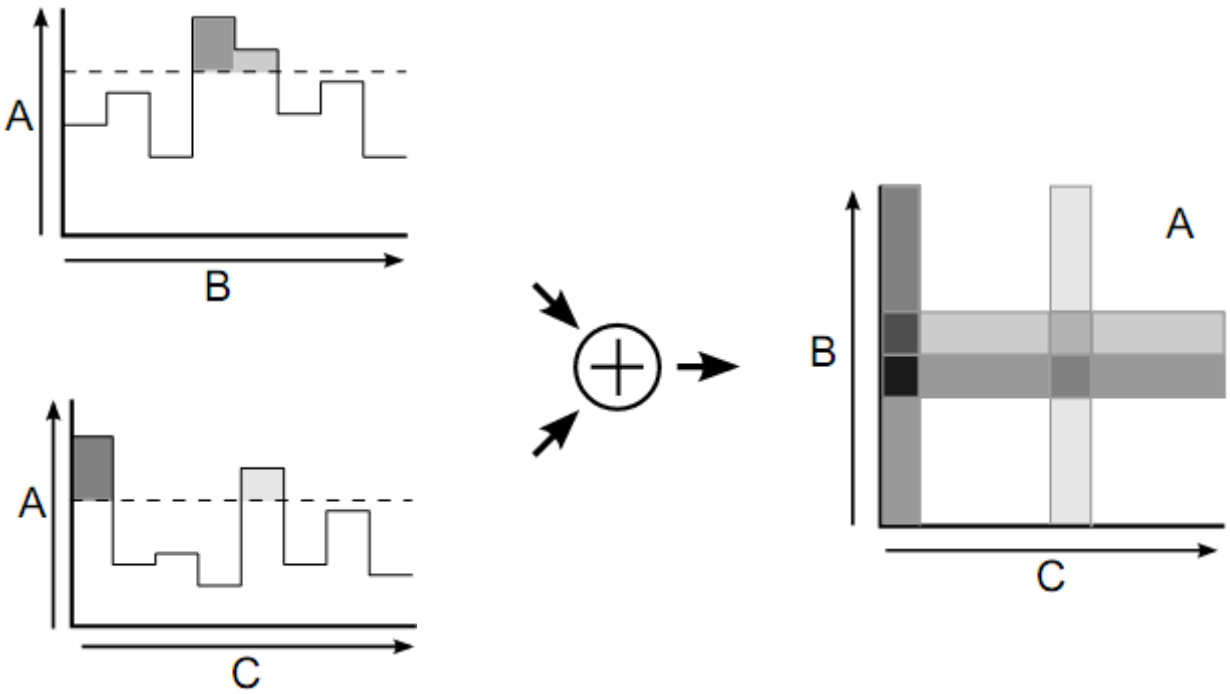


NON-LINEAR



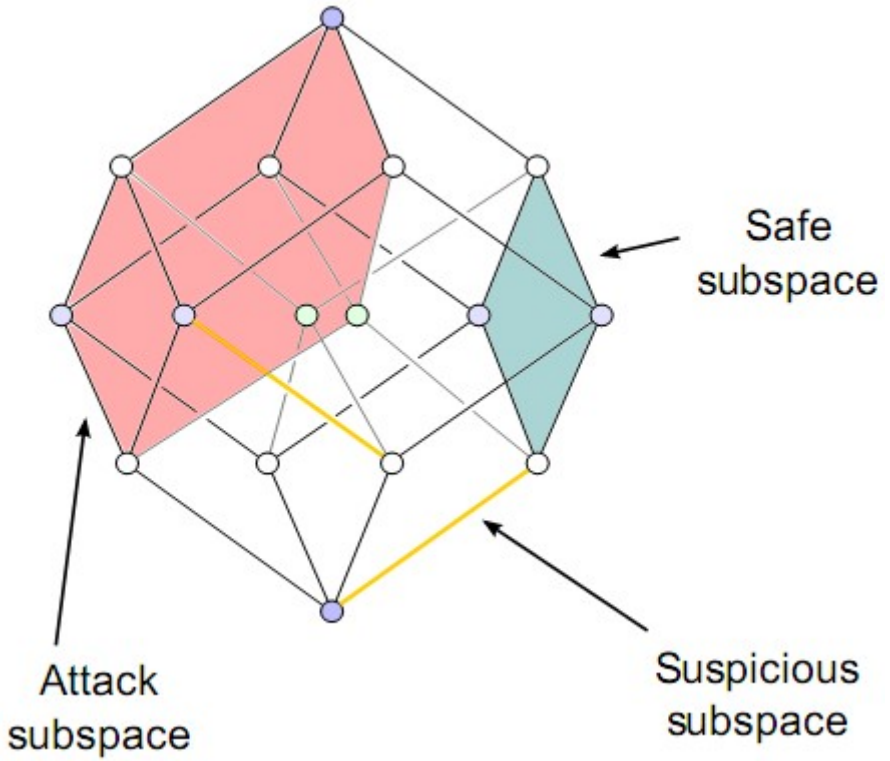
The Aspect-based Detection IV.

- Recomposition of analyzed aspects
- Correlation of findings in each aspect
- Deviations are composed and influence each other



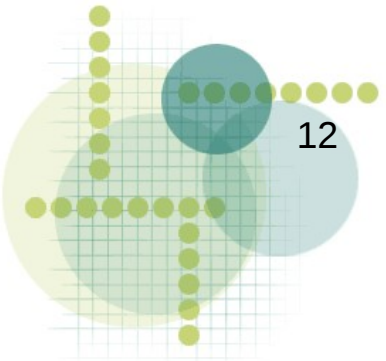
The Aspect-based Detection V.

- Composed deviations form vector space that has areas with significantly higher values
- Three types of areas:
  - Safe
  - Suspicious
  - Attack
- Attack identification
  - Automatic
  - Manual
  - Heuristic



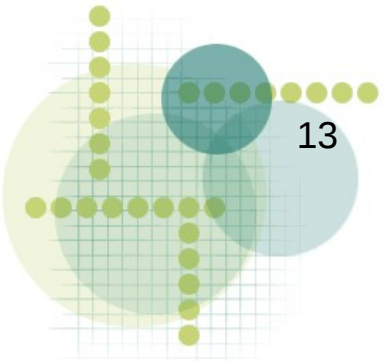
The Aspect-based Detection – Conclusion

- Novel method for attack detection
- Highly parallel
- Fast
- Extensible
- Can incorporate other detection methods
- Scaling well



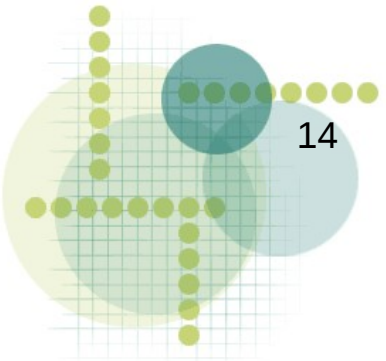
WitchdOCtoR I.

- There is a need to test and verify the security of a network
- Current tools have several downsides with regards to large networks
- Usually not suitable for:
  - parallel bruteforcing
  - adaptive bruteforcing
  - distributed attacks
  - DDoS simulation
- And if so – not in one package



WitchdOCtoR II.

- Main features
  - Cooperative
  - Scalable
  - Platform independent
  - Easy on resources
  - Extensible
  - Secure



Goals of the Thesis

- The implementation and the evaluation of the aspect-based detection framework
- Preparation of a distributed deployment of the WitchdOCtoR
- Research of new types of silent and adaptive bruteforce methods
- Research of metrics allowing to identify attacks based on their proximity to an attack subspace