
Detection of Heartbleed at CESNET Using Extended Flow Data

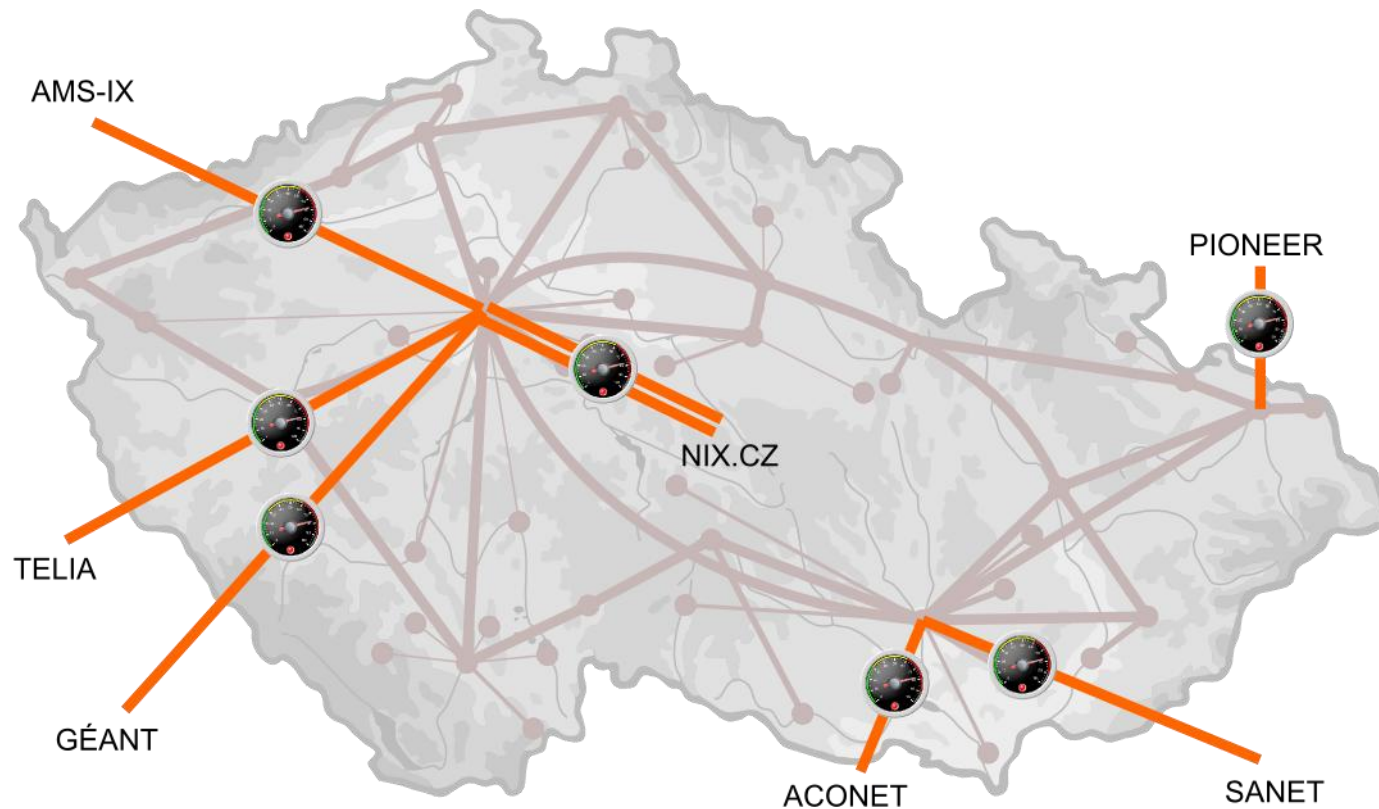
Václav Bartoš
bartos@cesnet.cz

TF-CSIRT Meeting, 30. 5. 2014



Monitoring at CESNET

- Flow monitoring using standalone probes
- All external links from/to CESNET2 (10 Gbps lines)



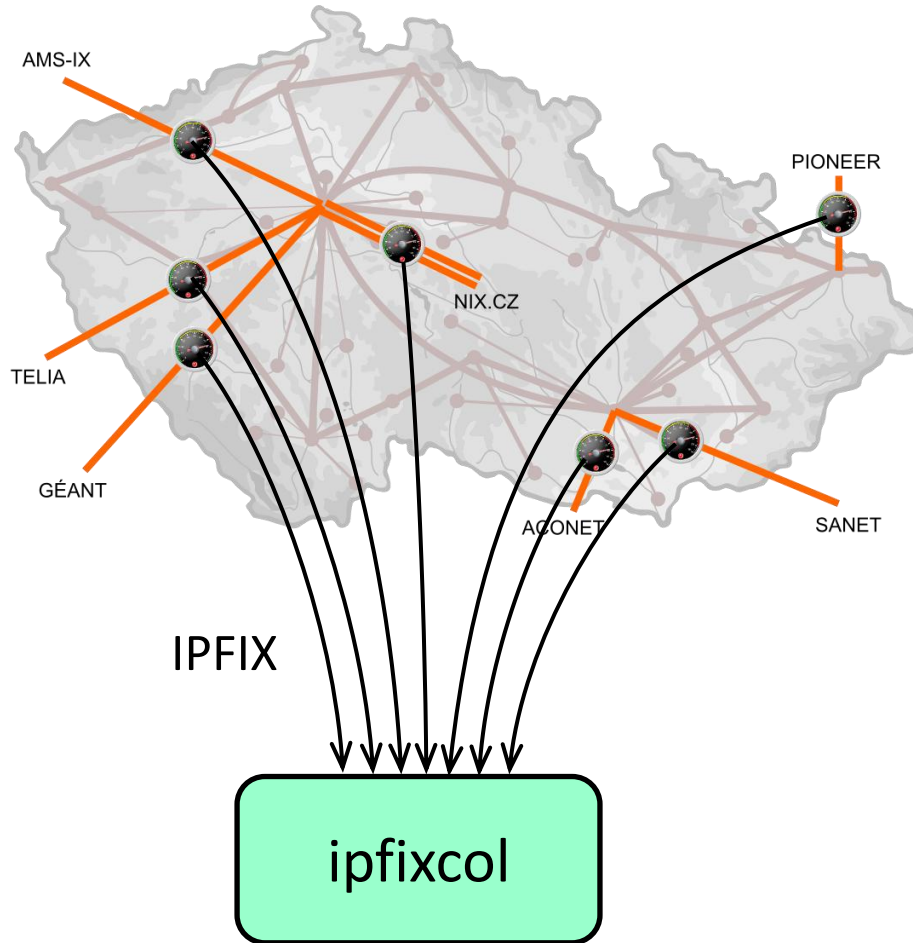
Probes

- Based on HW accelerated network cards
 - Full 10Gbps throughput (no sampling)

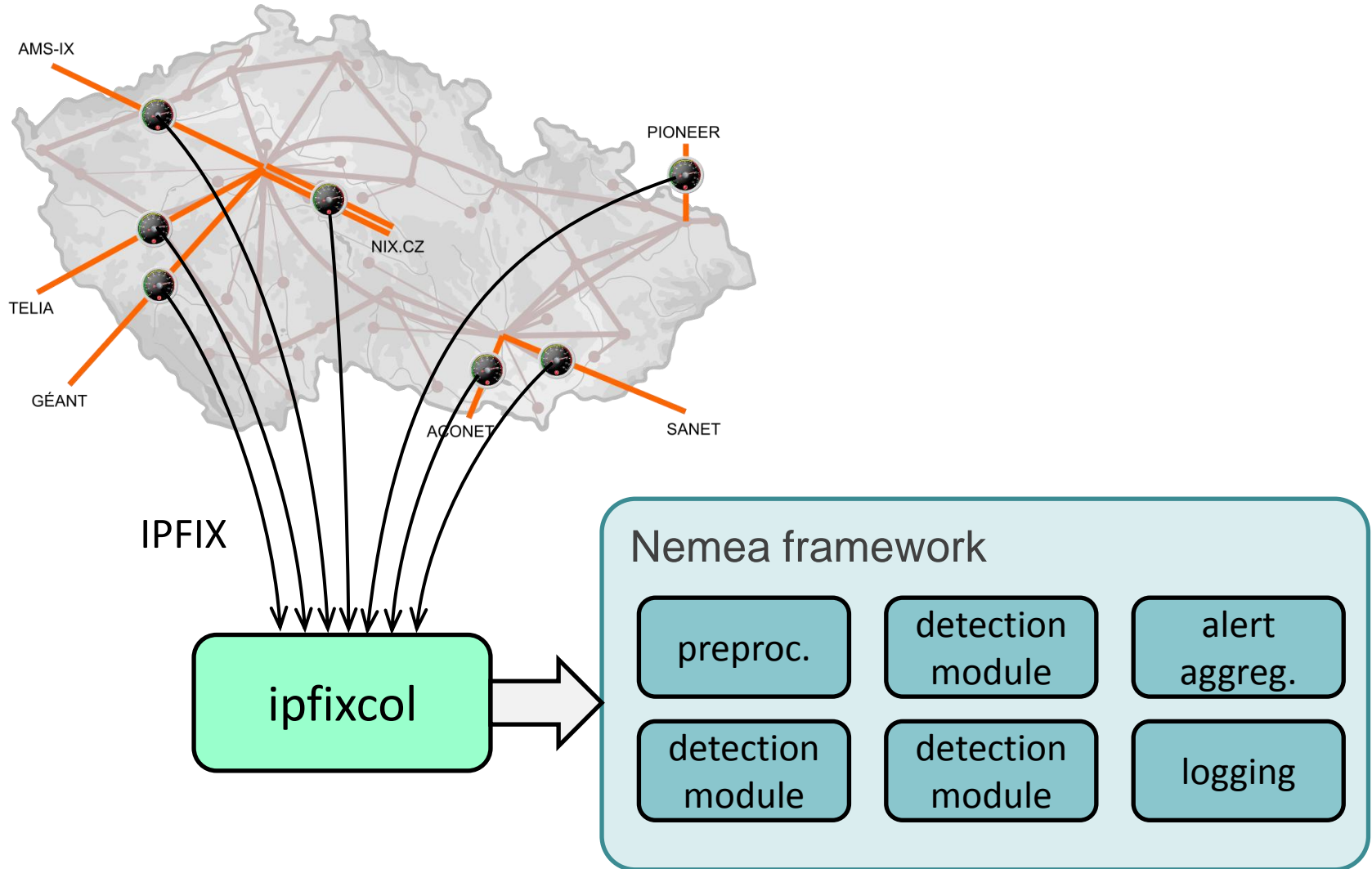


- FlowMon – software exporter
 - Plugin architecture
 - Possibility to **extract additional information** from **raw packets**
 - We experiment with parsing of DNS, HTTP and SMTP
 - Export via IPFIX

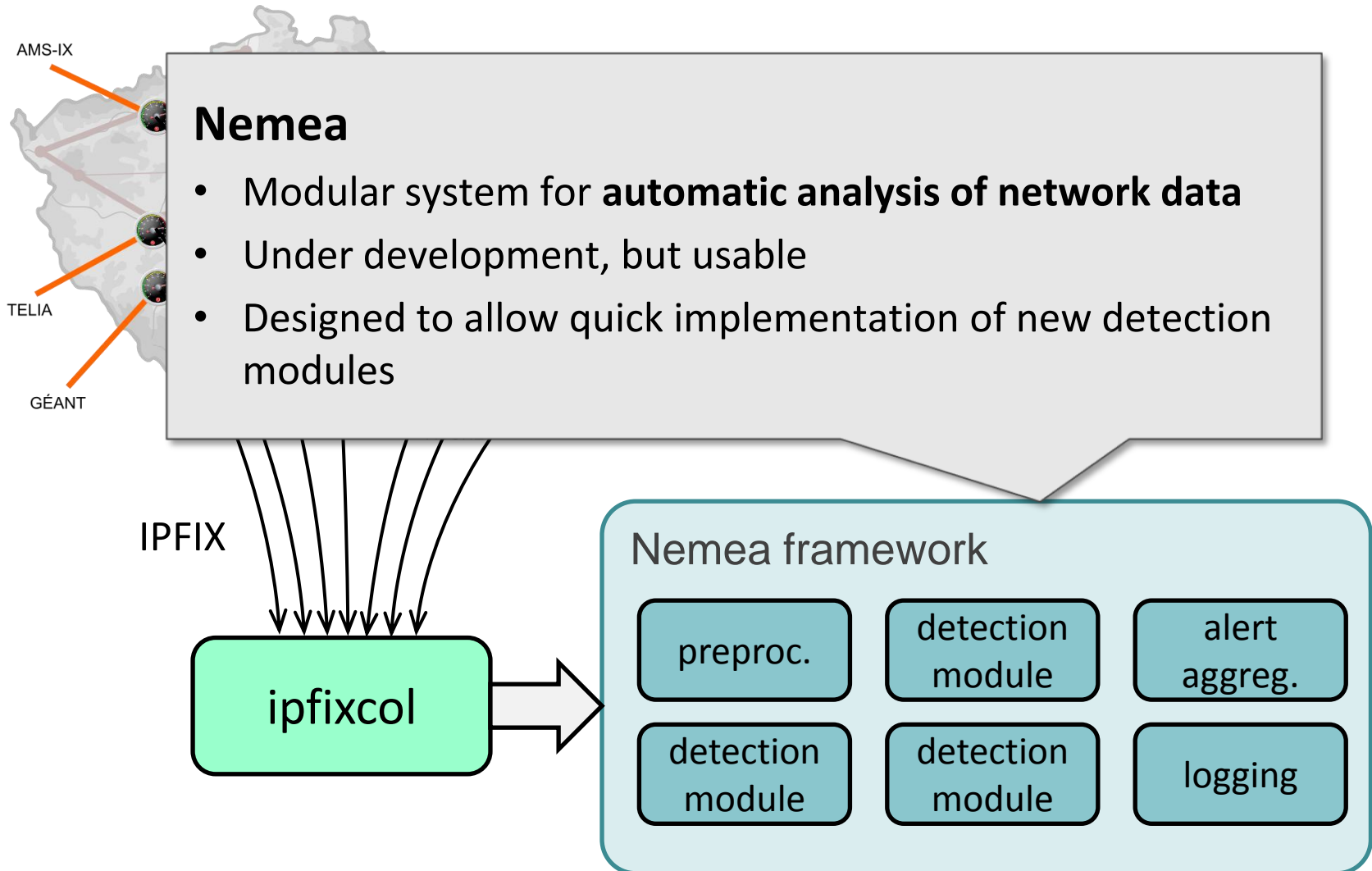
Monitoring infrastructure



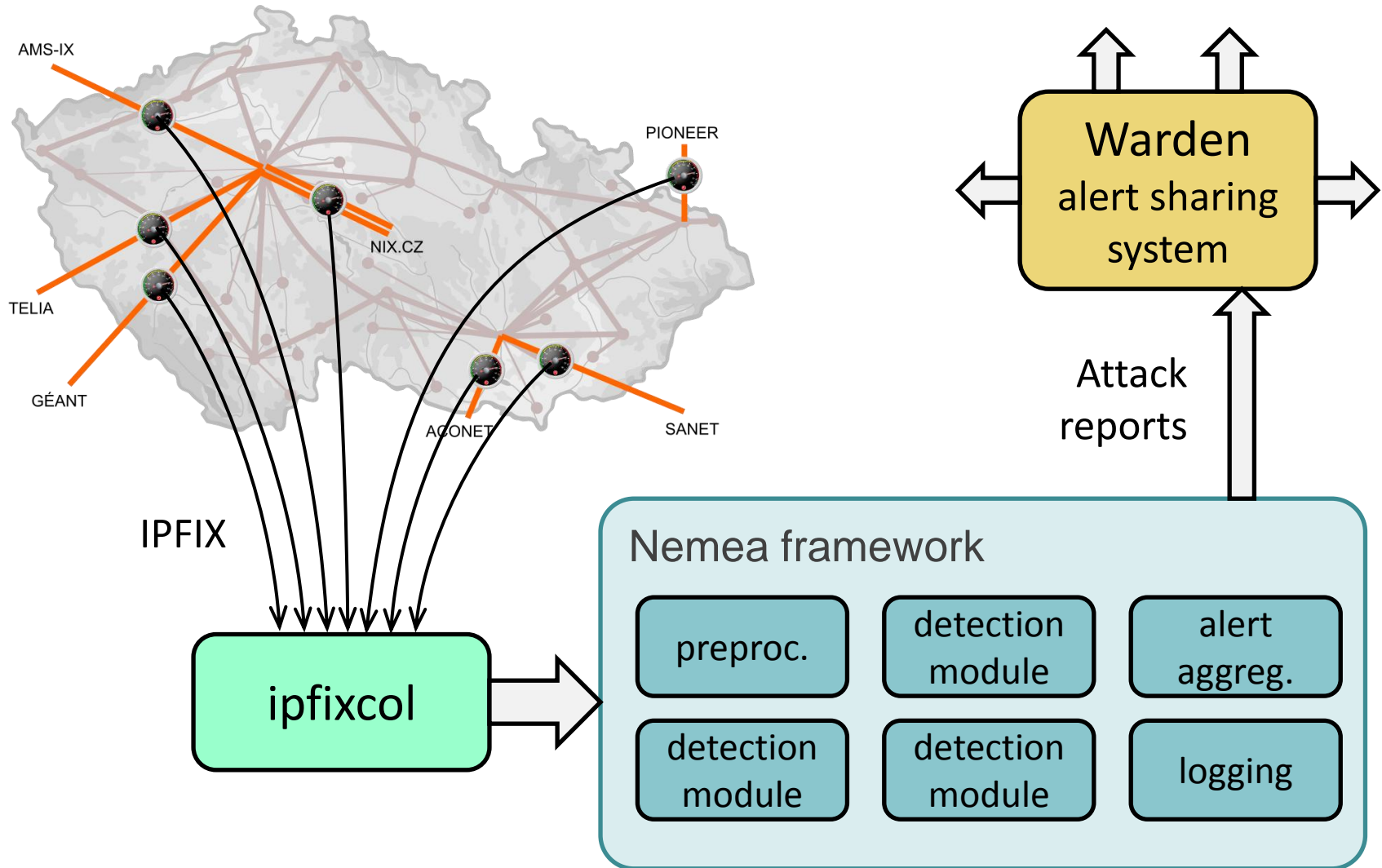
Monitoring infrastructure



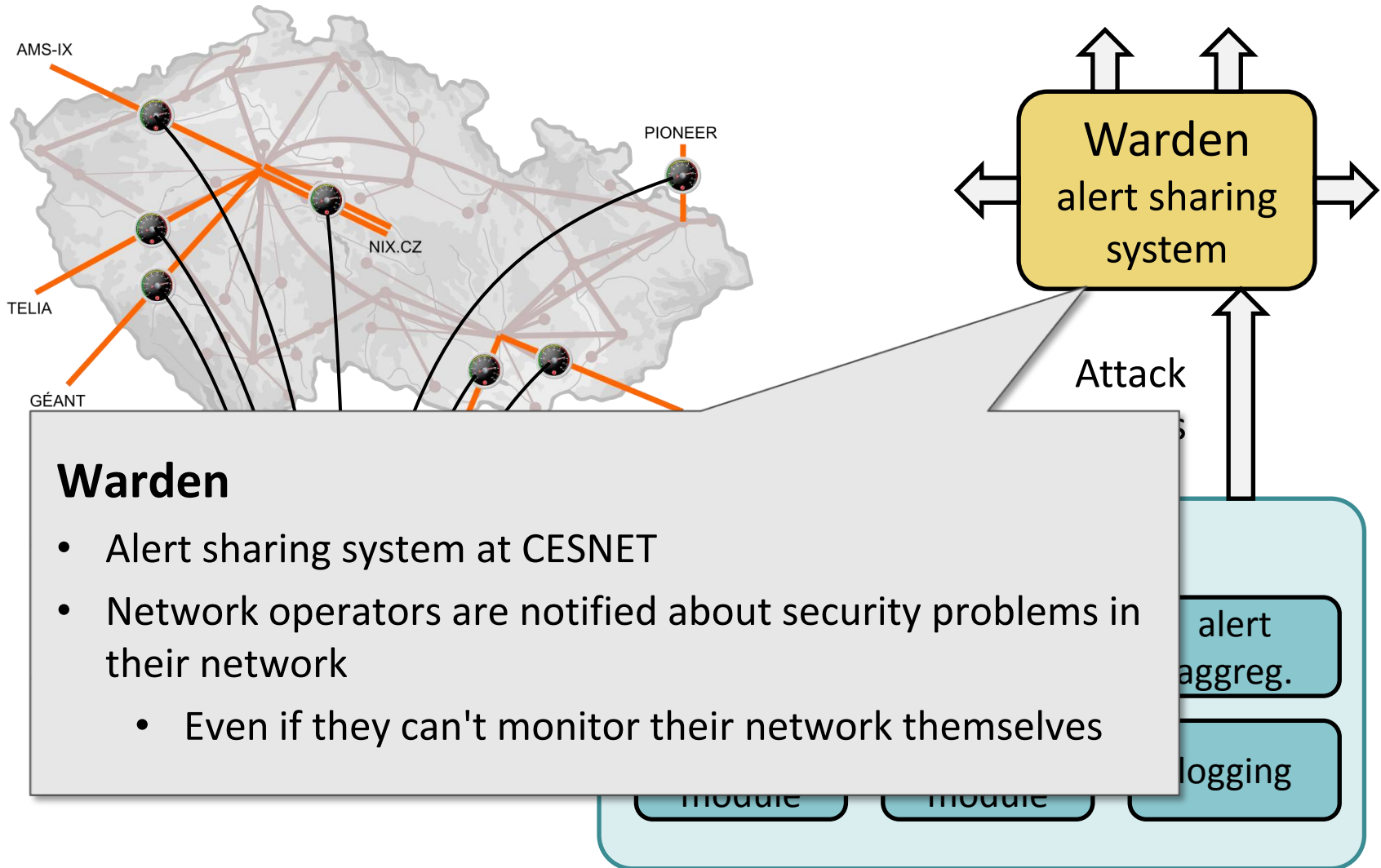
Monitoring infrastructure



Monitoring infrastructure



Monitoring infrastructure



Heartbleed attack

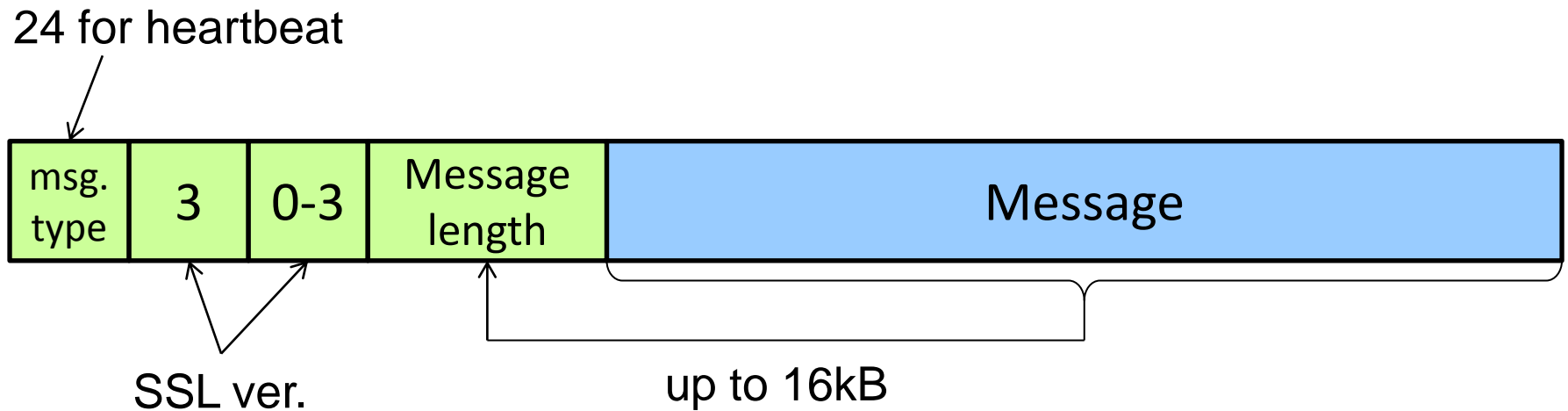


Heartbleed

- Heartbleed
 - Bug in OpenSSL allowing to read data from server's memory
 - Published on 7th April 2014
 - Based on specially crafted heartbeat packet
- Heartbeat
 - Extension of TLS protocol providing keep-alive functionality
 - Request-reply, the same random payload
- Detection in flow data?
 - No special flow characteristics
 - We can parse packets in exporter and export additional information, but...
 - SSL/TLS = encryption ☹️
 - But look at it closer ...

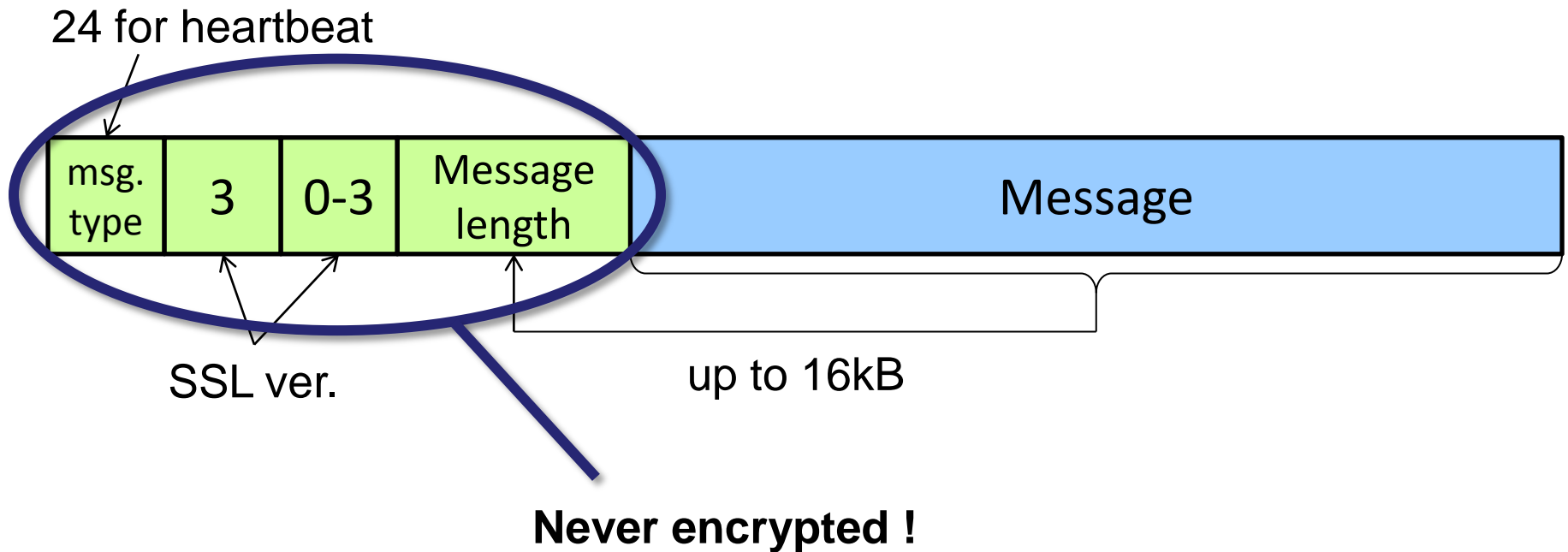
Heartbleed attack

- TLS record:



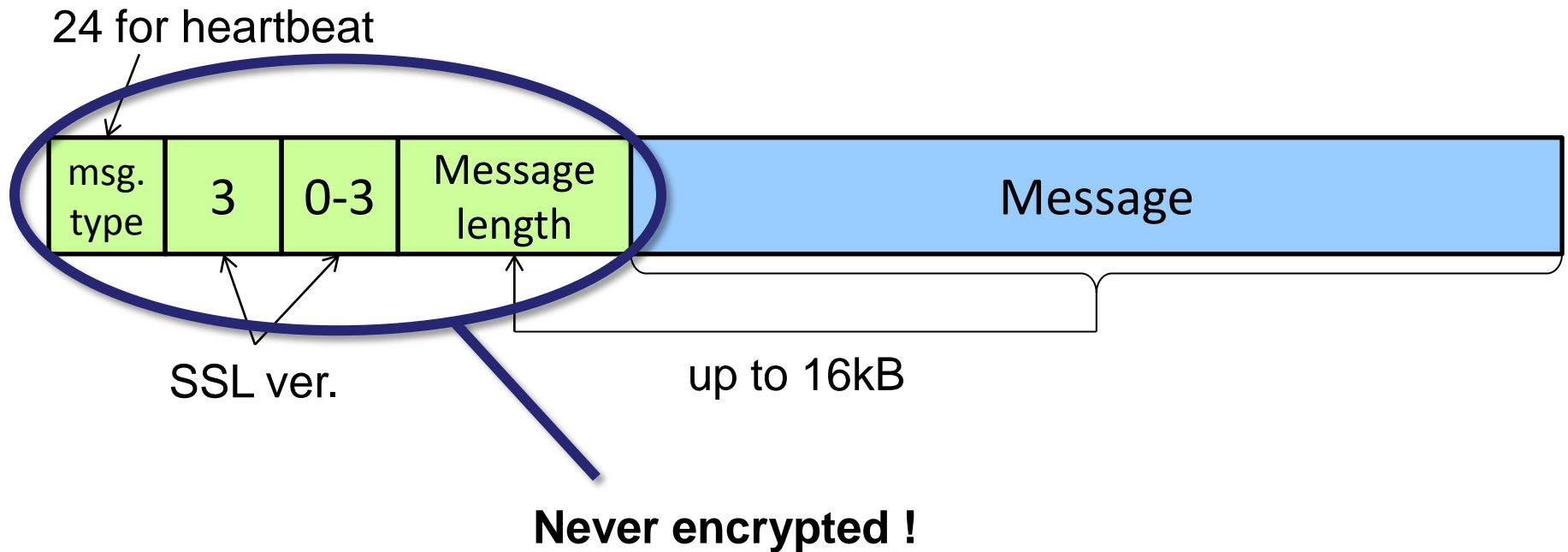
Heartbleed attack

- TLS record:



Heartbleed attack

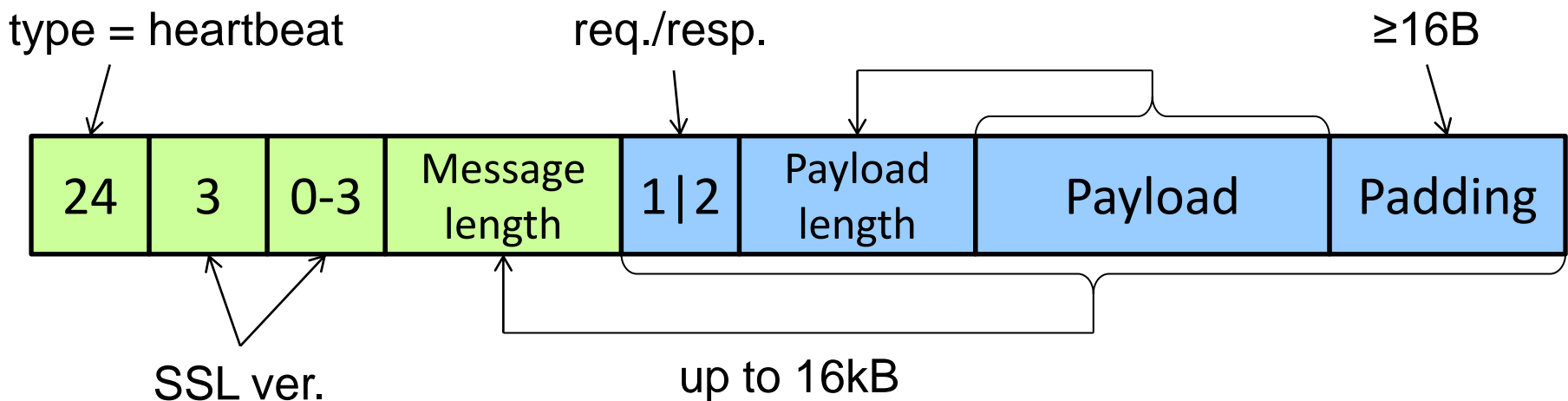
- TLS record:



Message **may be** encrypted. But usually isn't in case of Heartbleed.

Heartbleed attack

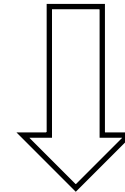
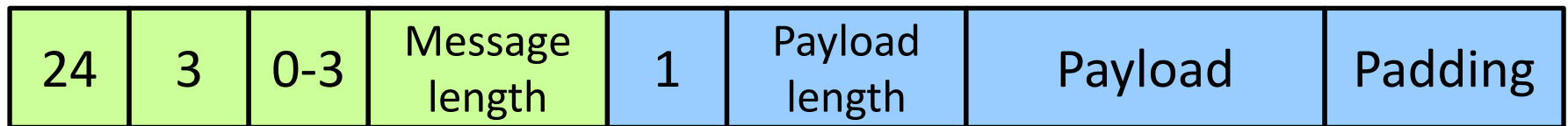
- Normal Heartbeat record:



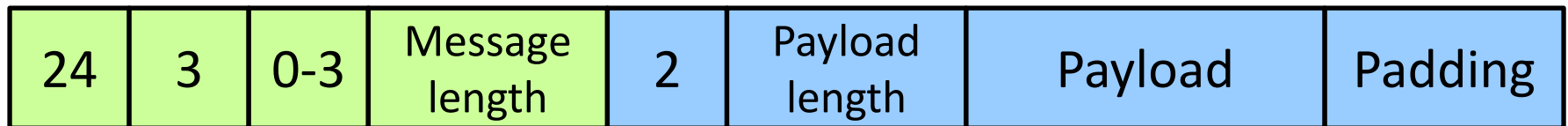
Heartbleed attack

- Reply to heartbeat carries the same payload

Request:



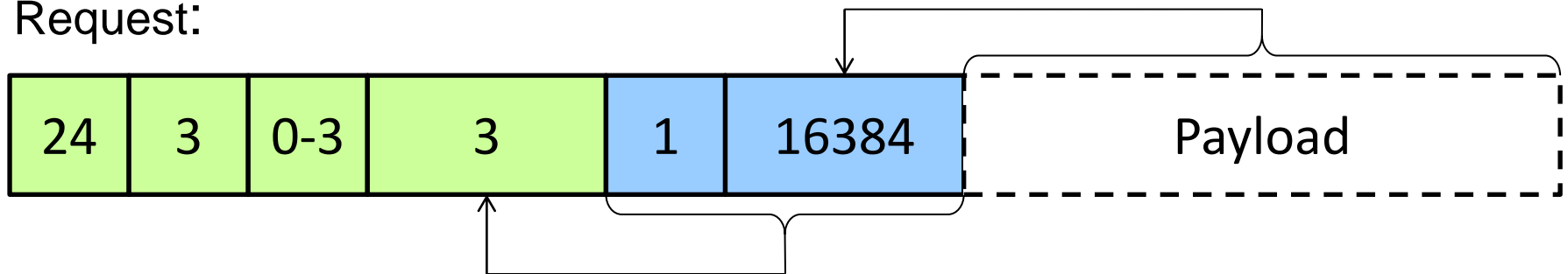
Reply:



Heartbleed attack

- Heartbleed packet:

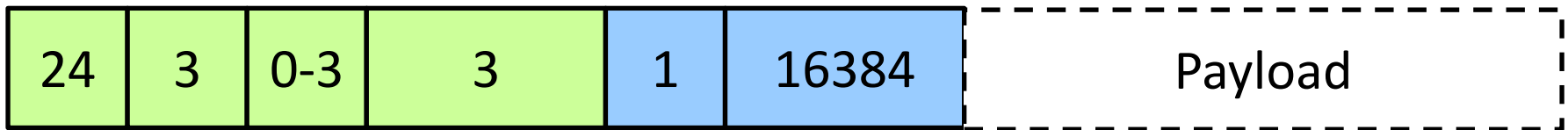
Request:



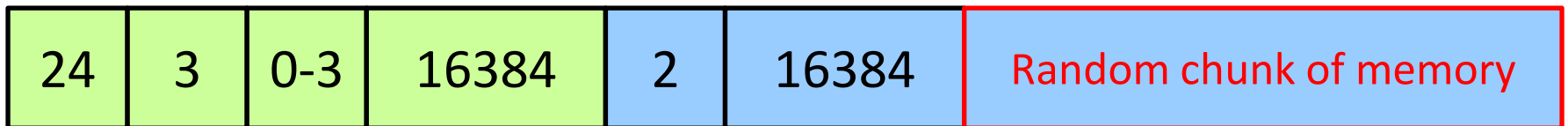
Heartbleed attack

- Heartbleed packet:

Request:

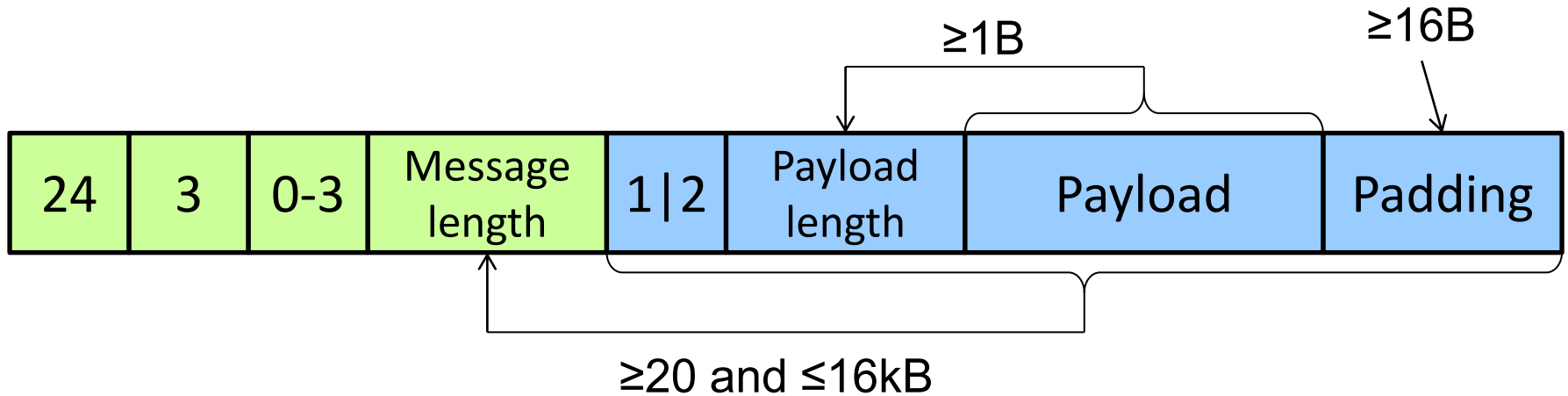


Reply (OpenSSL):



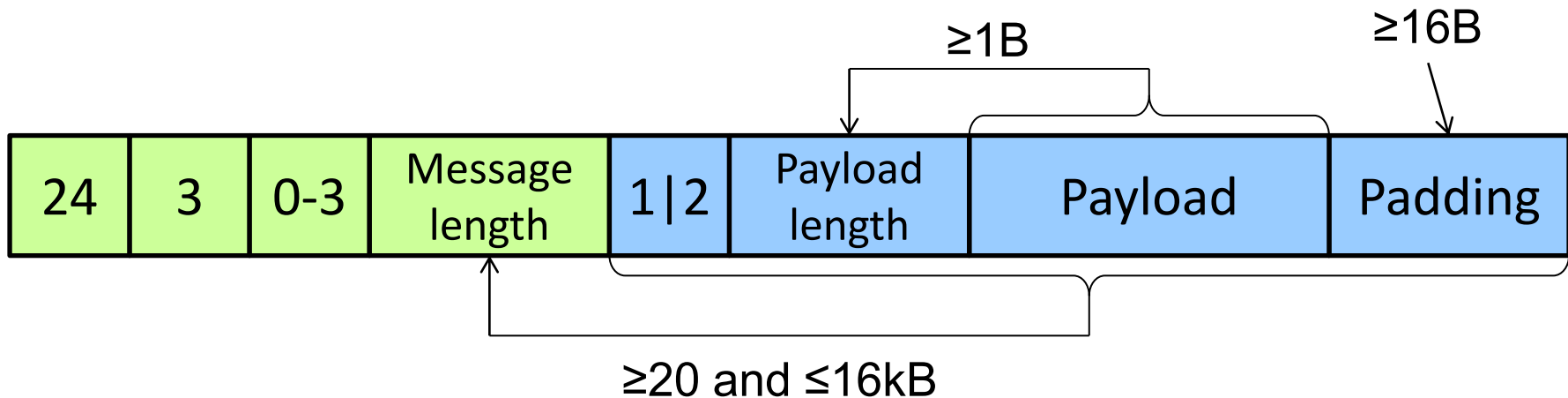
Heartbleed attack

- What is important for detection:



Heartbleed attack

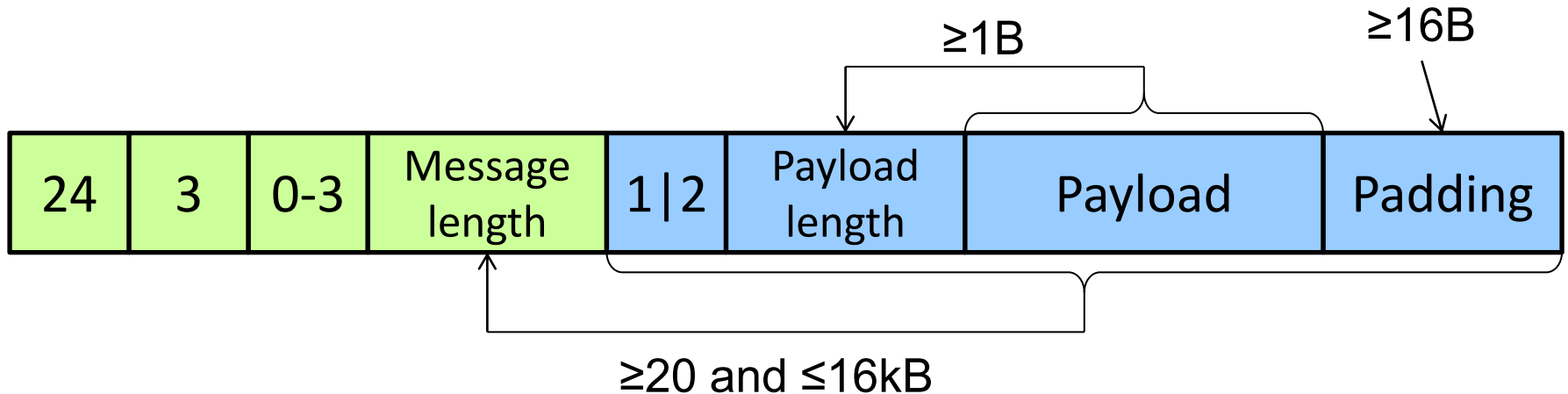
- What is important for detection:



$$message_length \geq 1 + 2 + payload_length + 16$$

Heartbleed attack

- What is important for detection:

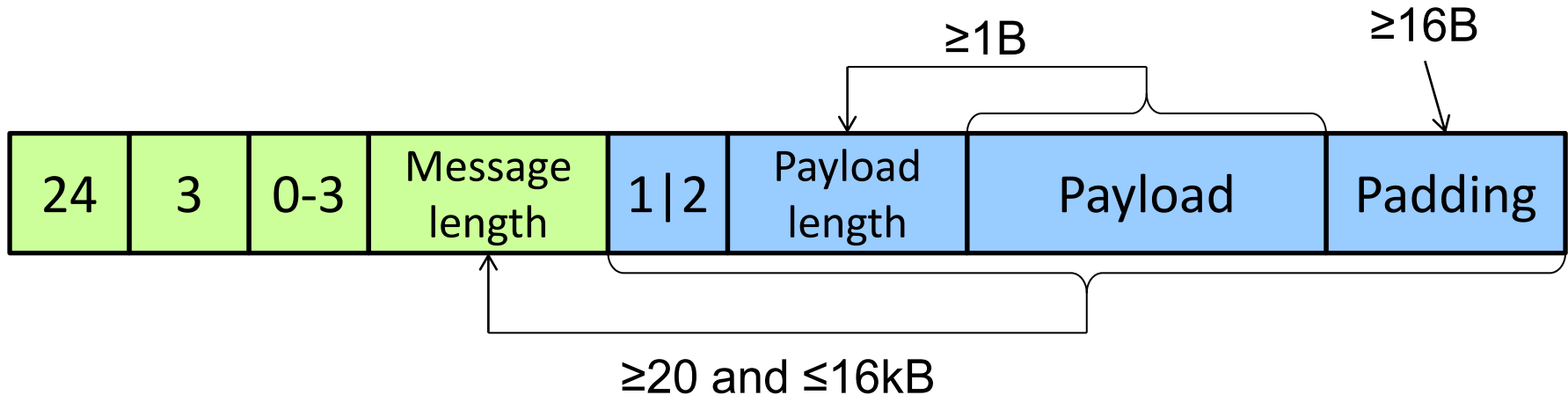


$$\text{message_length} \geq 1 + 2 + \text{payload_length} + 16$$

$$\text{message_length} \geq 20$$

Heartbleed attack

- What is important for detection:



$$\text{message_length} \geq 1 + 2 + \text{payload_length} + 16$$

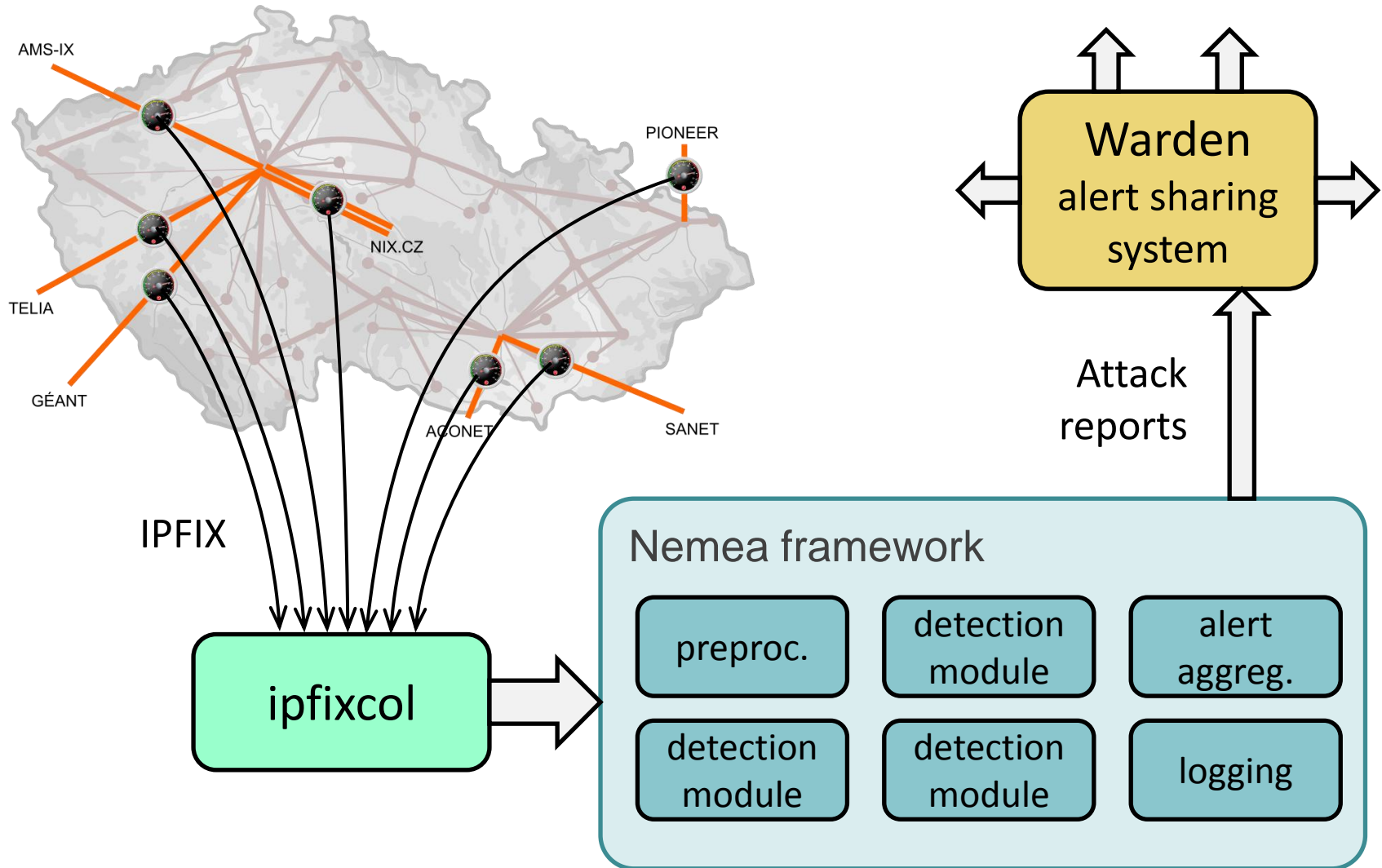
$$\text{message_length} \geq 20$$

$$\text{reply size} = \text{request size}$$

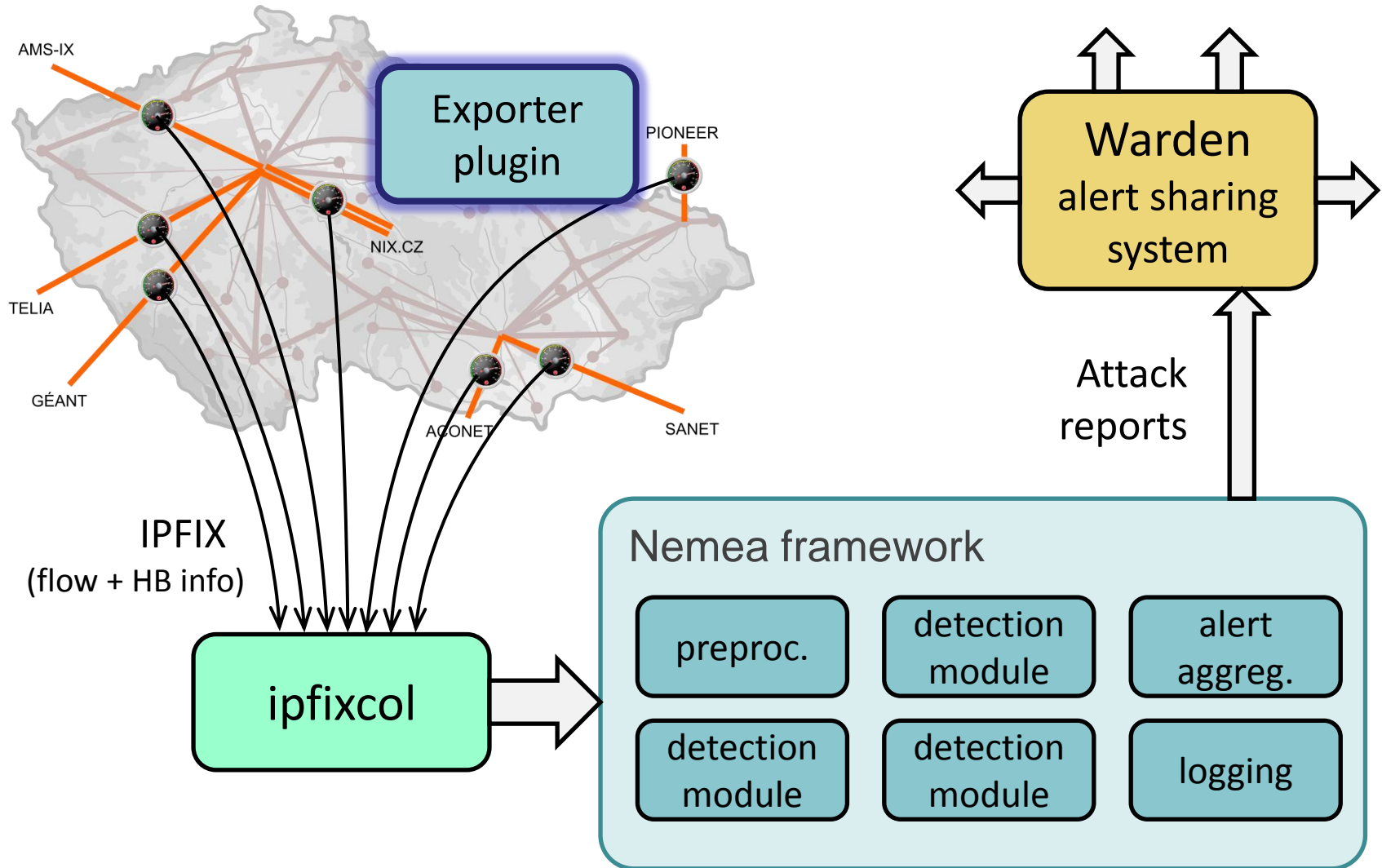
Heartbleed attack detection at CESNET



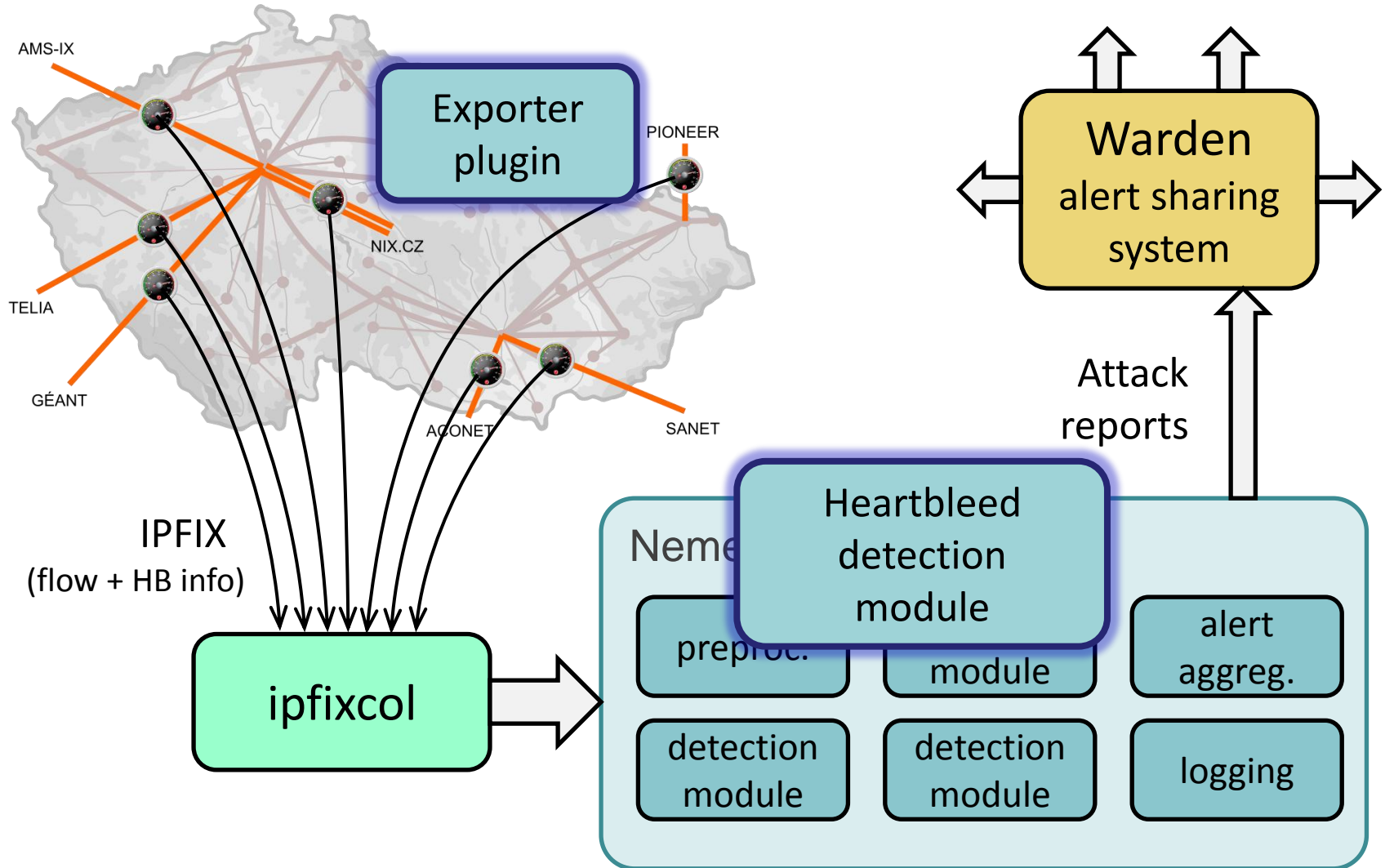
Monitoring infrastructure



Monitoring infrastructure



Monitoring infrastructure



Exporter plugin

- Plugin for INVEA-TECH's FlowMon exporter
- Recognizes heartbeat packets:
 - TCP port 443 HTTPS
 - tcp_payload[0] = 24 heartbeat message type
 - tcp_payload[1] = 3 major version
 - tcp_payload[2] = 0..3 minor version
 - tcp_payload[5] = 1 | 2 request / response
- Creates a flow record for each heartbeat packet
- Additional IPFIX fields:
 - Message size
 - Direction (request / response)
 - Payload size

Exporter plugin

- Possible problems:
 - TLS record might not begin at the beginning of TCP segment
 - Only possible solution – reconstruct TCP stream
 - impossible at 10Gbps
 - Many records are missed
 - Random data matches the filter
 - Probability: $1.86 \cdot 10^{-9}$
 - We see approx. $2.5 \cdot 10^7$ packets on port 443 per minute
 - -> One false match each 20 minutes on avg. (worst case)

Detection module

- Receives record with heartbeat data
 - Uses 4 heuristics to detect Heartbleed attack:
 1. message length $<$ payload length + 19
 - Bad payload length
 2. message length $<$ 20
 - Request is smaller than minimum
 3. size of request packet \neq size of reply packet
 - Request and reply have different size
 4. message length \geq 8kB
 - Unusually large replies
- } work even if encryption is enabled
- Scoring mechanism
 - Each heuristic adds some points to $\langle \text{src_ip}, \text{dst_ip} \rangle$ pair
 - Everything is logged
 - Successful attacks with high score are reported

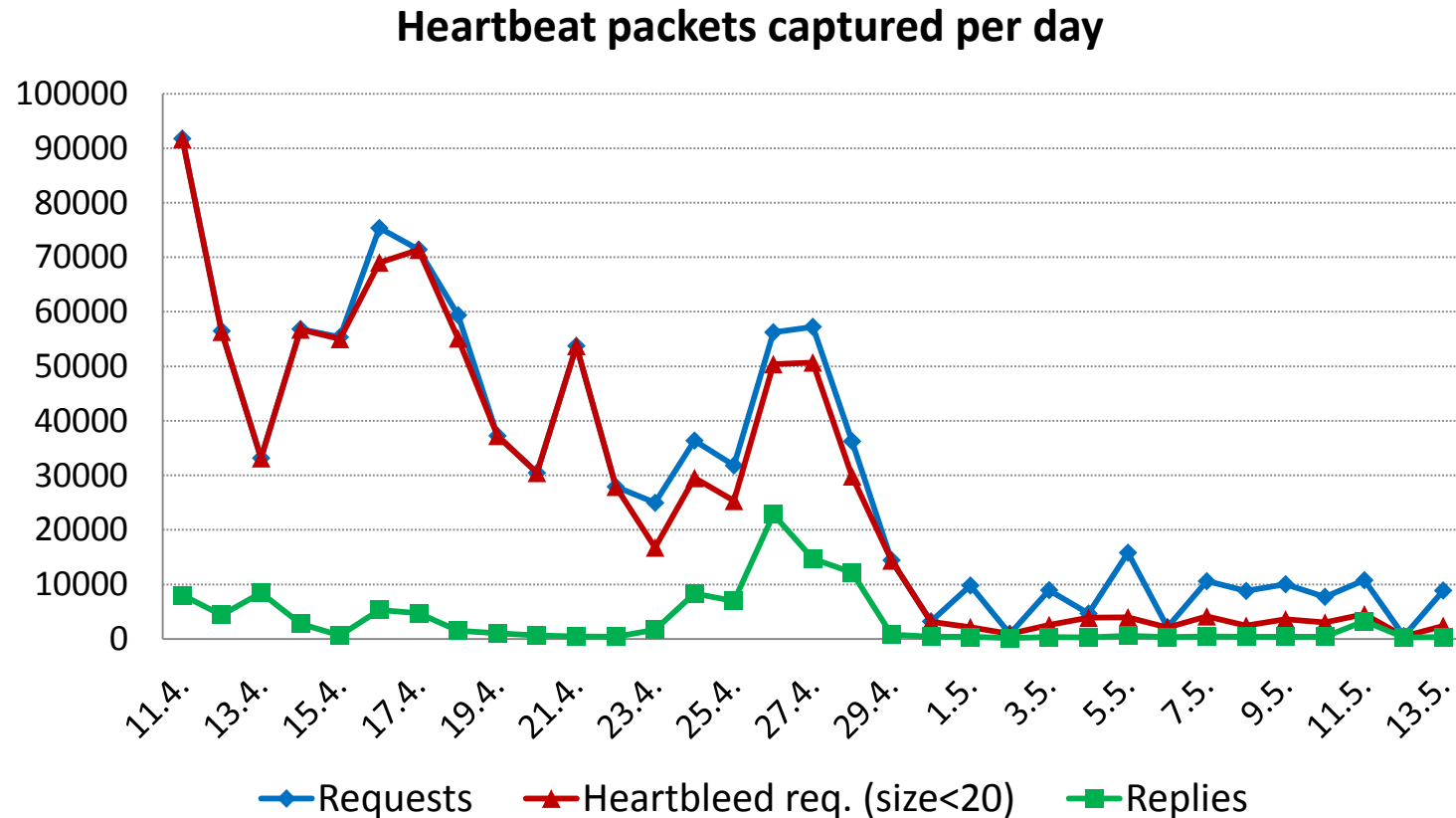
Timeline

- April 7 (Monday) – Heartbleed bug becomes publicly known
- April 10 (Thursday)
 - We started to work on its detection
 - Packet capture on all probes (all heartbeat packets)
- April 11 (Friday)
 - Exporter plugin done
- April 14 (Monday)
 - First version of the detection module done
 - First results reported manually by email
 - Automated reporting to Warden since April 25

Results

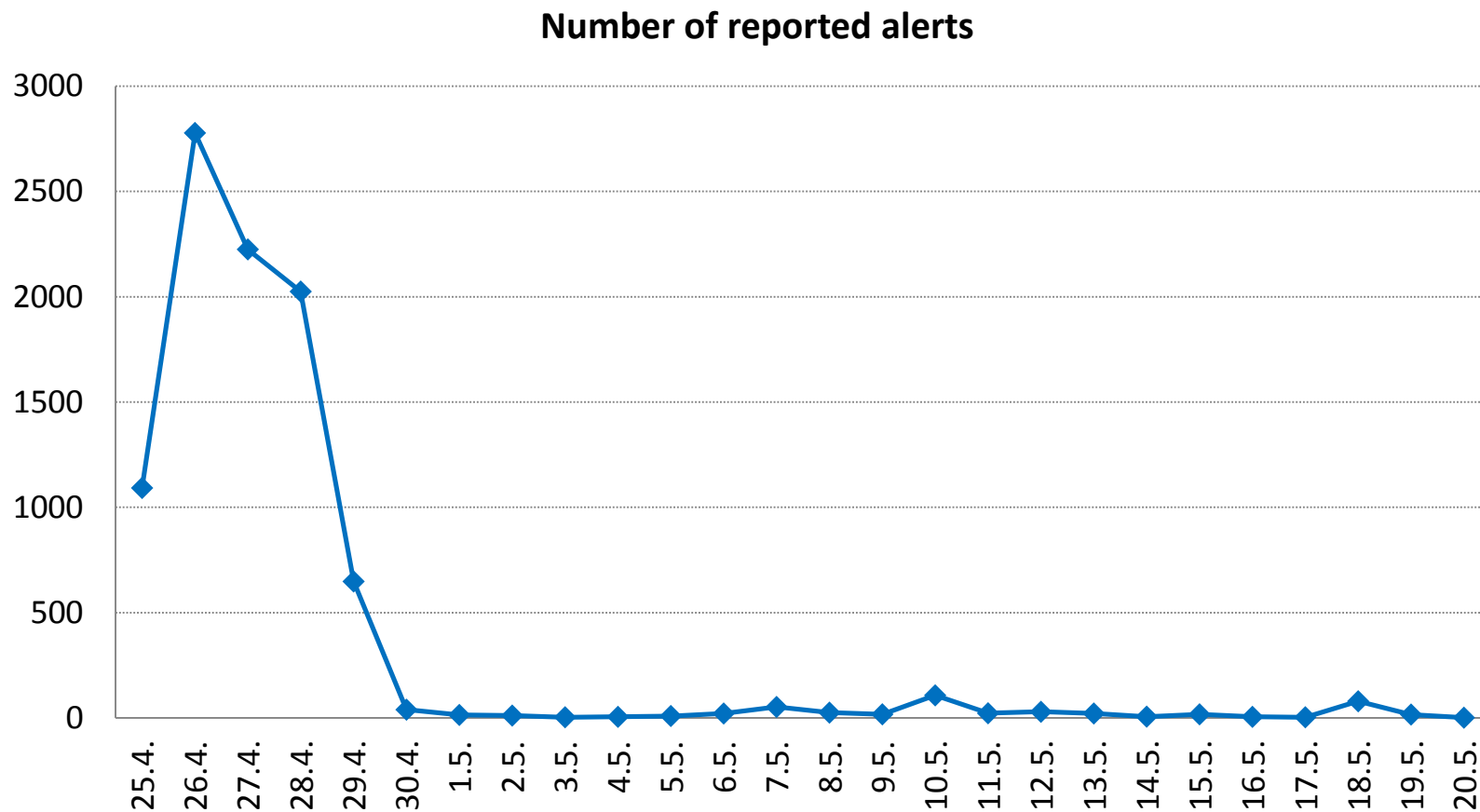


Heartbeat packets



- There are almost no regular heartbeat packets
- Most of attacks are unsuccessful

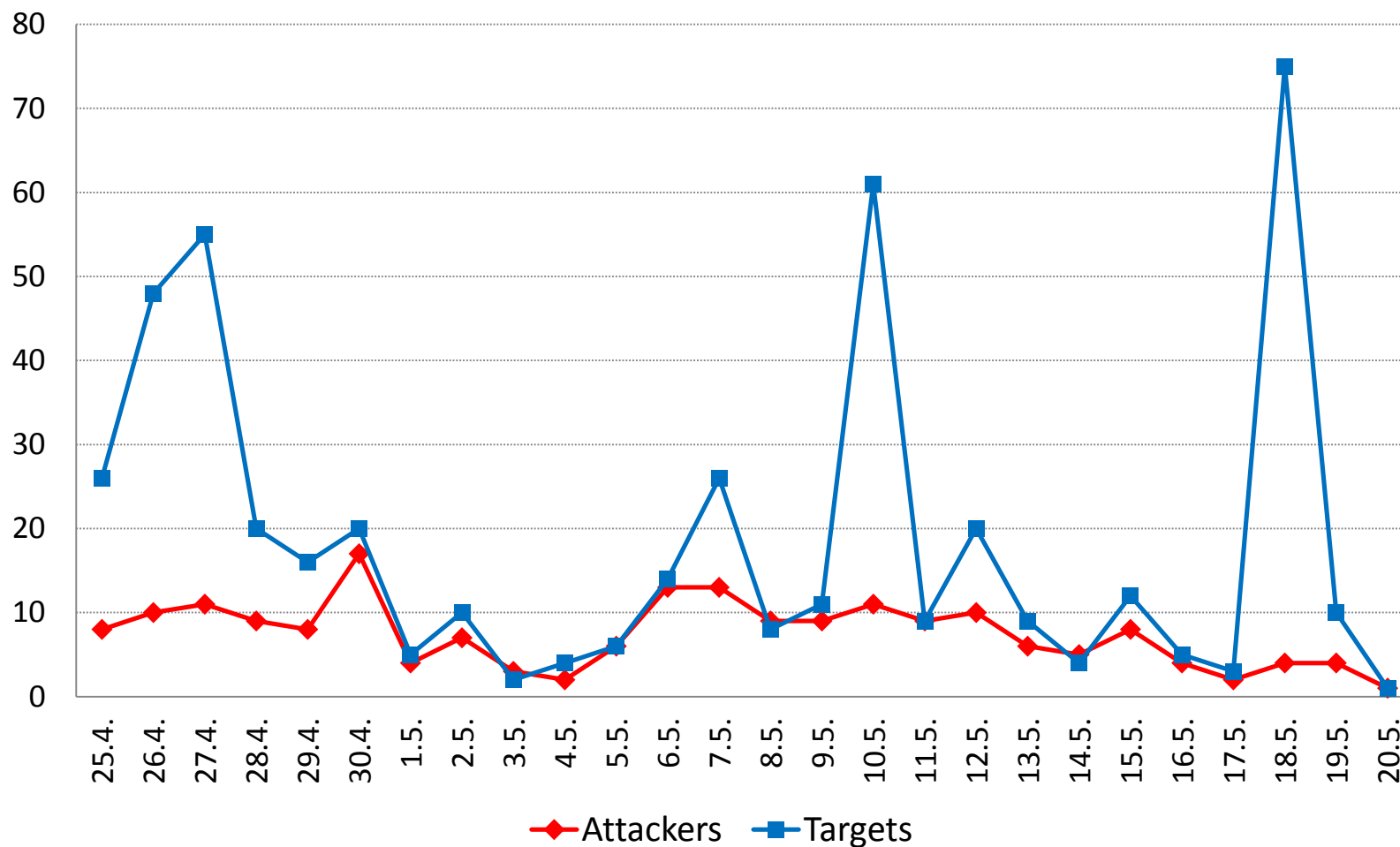
Reported alerts



5min aggregation – long attacks reported many times

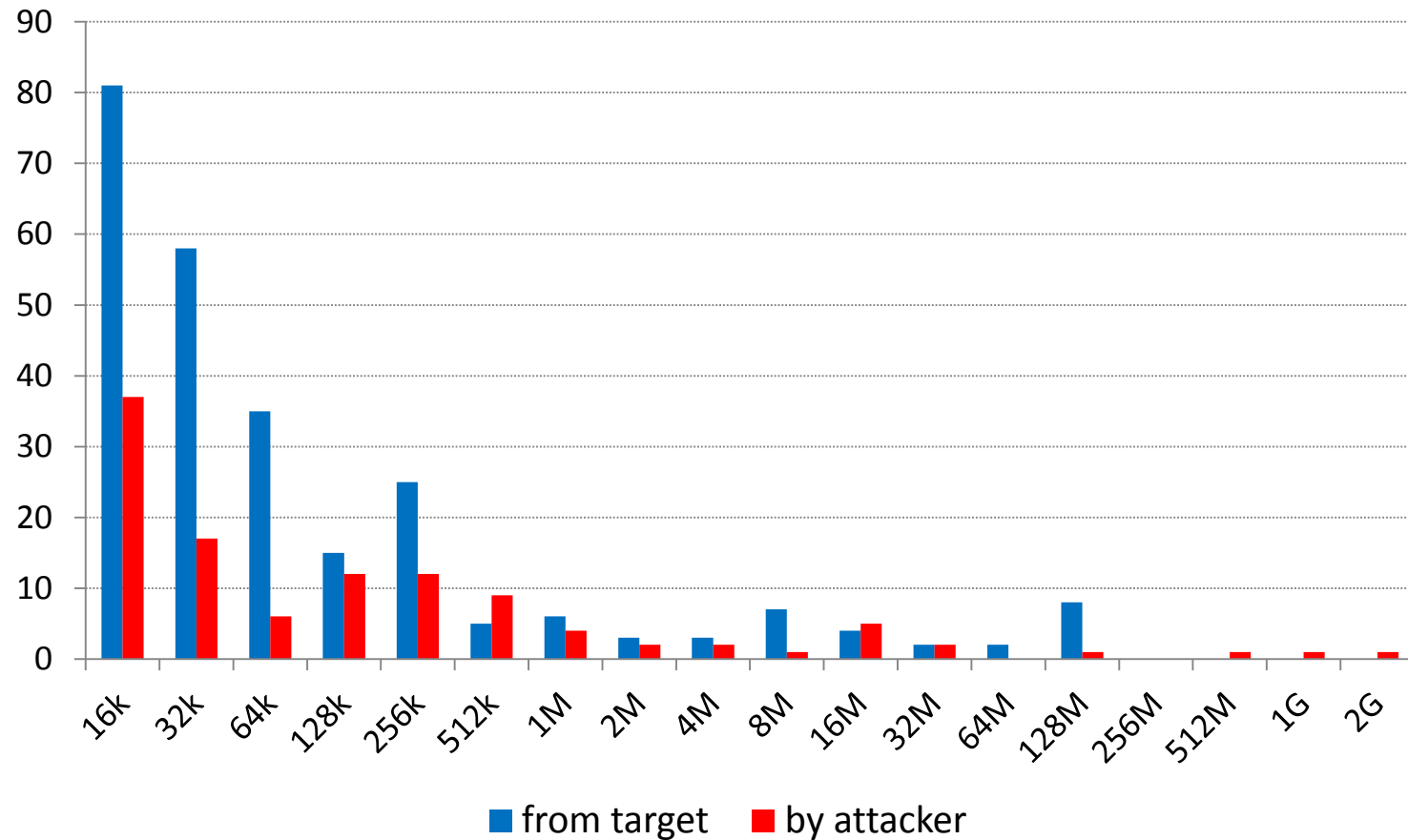
Reported alerts

Number of unique attackers and targets



Bytes read from server

Bytes read from target / by attacker



Summary

- Method:
 - Passive monitoring
 - Whole CESNET network
 - Flow + DPI
- 10000s Heartbleed attacks per day
 - Most of them unsuccessful, servers were patched very quickly
- Many vulnerable machines found and reported
 - >300 via Warden (since April 25)
 - Many more manually earlier
- Feedback
 - Some servers didn't need HTTPS
 - We found some old forgotten servers

Thank you for your attention.

Questions?

