No More DDoS

Anti-DDoS-Coalitie

DDoS Clearing House Update

Thu Dec 17, 2020

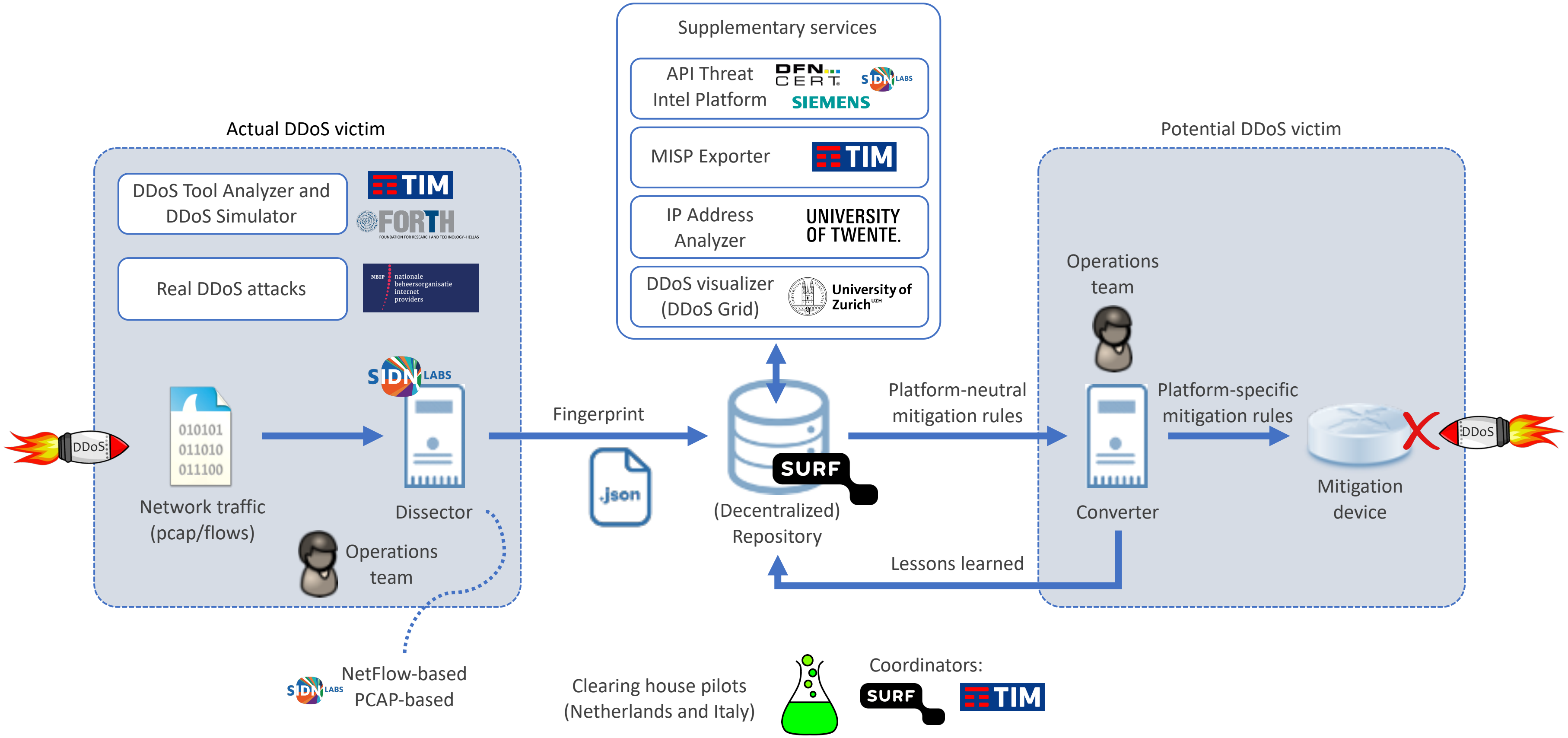
João Ceron en Cristian Hesselman

(SIDN Labs)

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

Components and data flow (CONCORDIA)



Supplementary services

API Threat Intel Platform

MISP Exporter

IP Address Analyzer

DDoS visualizer (DDoS Grid)

Actual DDoS victim

DDoS Tool Analyzer and DDoS Simulator

Real DDoS attacks

Network traffic (pcap/flows)

Dissector

Operations team

Fingerprint

(Decentralized) Repository

Platform-neutral mitigation rules

Potential DDoS victim

Operations team

Converter

Platform-specific mitigation rules

Mitigation device

Lessons learned

NetFlow-based
PCAP-based

Clearing house pilots (Netherlands and Italy)

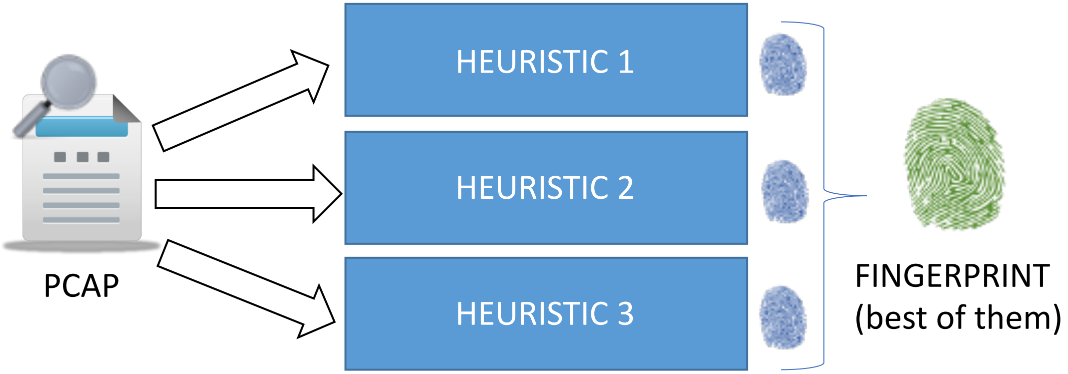
Coordinators:

No More DDoS Anti-DDoS-Coalitie

CONCORDIA

Technical update

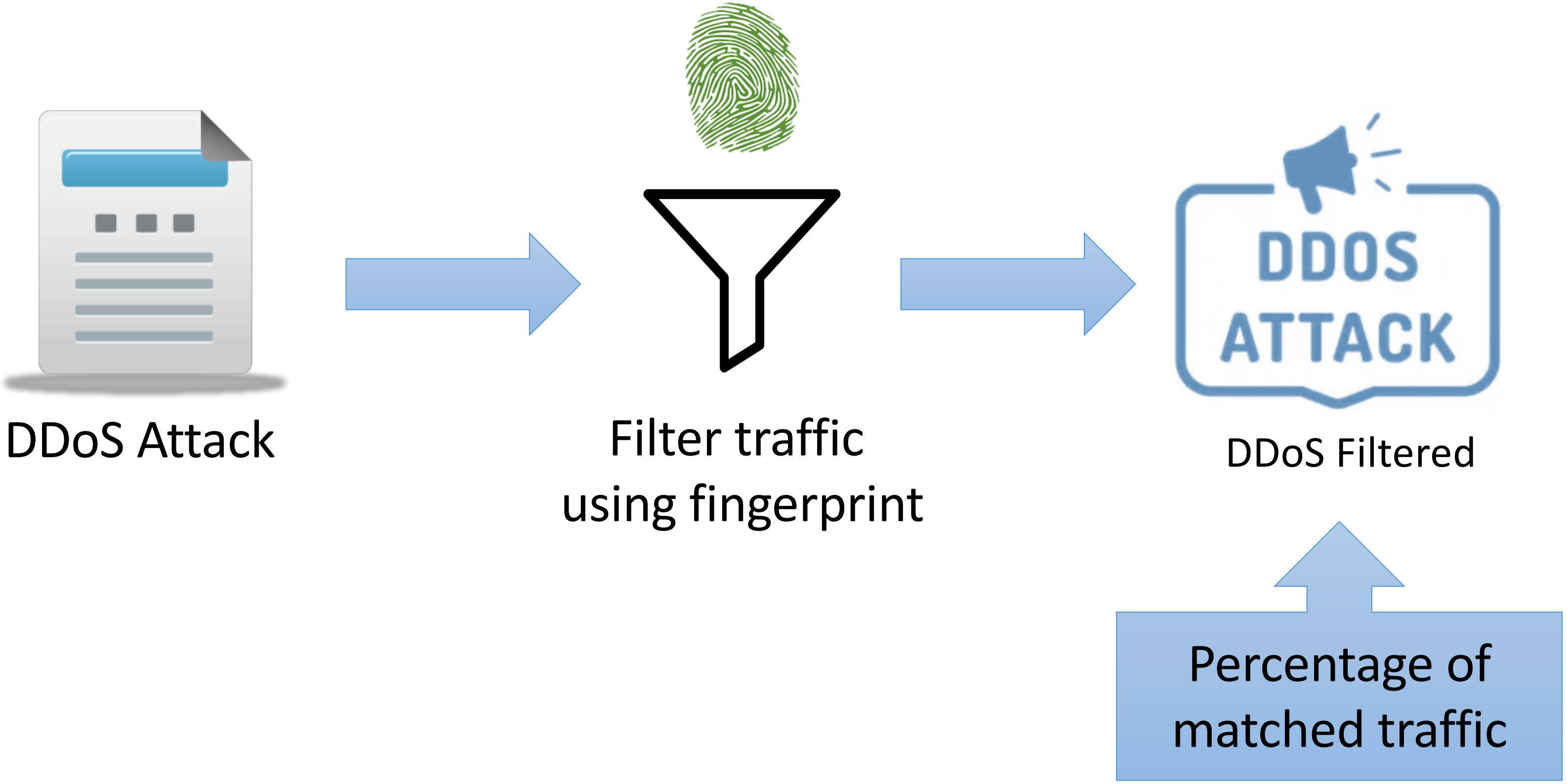
- DDoS traffic from NBIP
  - 9 PCAP files
  - Multiples attack types
- Software improvements
  - Clustering methodology
  - Fingerprint evaluation
- Flow-based version in addition to PCAP



No More DDoS
Anti-DDoS-Coalitie

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Fingerprint evaluation



DDoS Attack

Filter traffic using fingerprint

DDoS Filtered

Percentage of matched traffic

NBIP Dataset (pcap)

Attack Type	IP matching ratio
DNS Amplification	89%
Multiprotocol Amplification	99%
LDAP Reflection	93%
GRE Flood	94%
DNS Water Torture	74%
SNMP Amplification	51%
Multiprotocol (type 2)	86%
LDAP Amplification with Fragmentation	76%
DNS Amplification	64%

Fingerprints examples

1. {'srcport': 389, 53, 'frame_len': 1350, 'fragmentation': True},
2. {'ip_proto': 'GRE', 'highest_protocol': 'IPX', 'ip_ttl': 121, 'fragmentation': False},
3. {'dns_qry_type': 1, 'ip_proto': 'UDP', 'highest_protocol': 'DNS', 'dstport': 53, 'fragmentation': False},
4. {'srcport': 161, 672, 'frame_len': 1350, 'fragmentation': True},
5. {'srcport': 389, 53, 'frame_len': 1350, 'fragmentation': True},
6. {'srcport': 389, 'frame_len': 1350, 'fragmentation': True},
7. {'srcport': 53, 389, 'frame_len': 1350, 'fragmentation': True},

- We decided not to use the SRC IPs as part of the fingerprint.
- Although, it is more complex to generate them this turns fingerprints more generic.

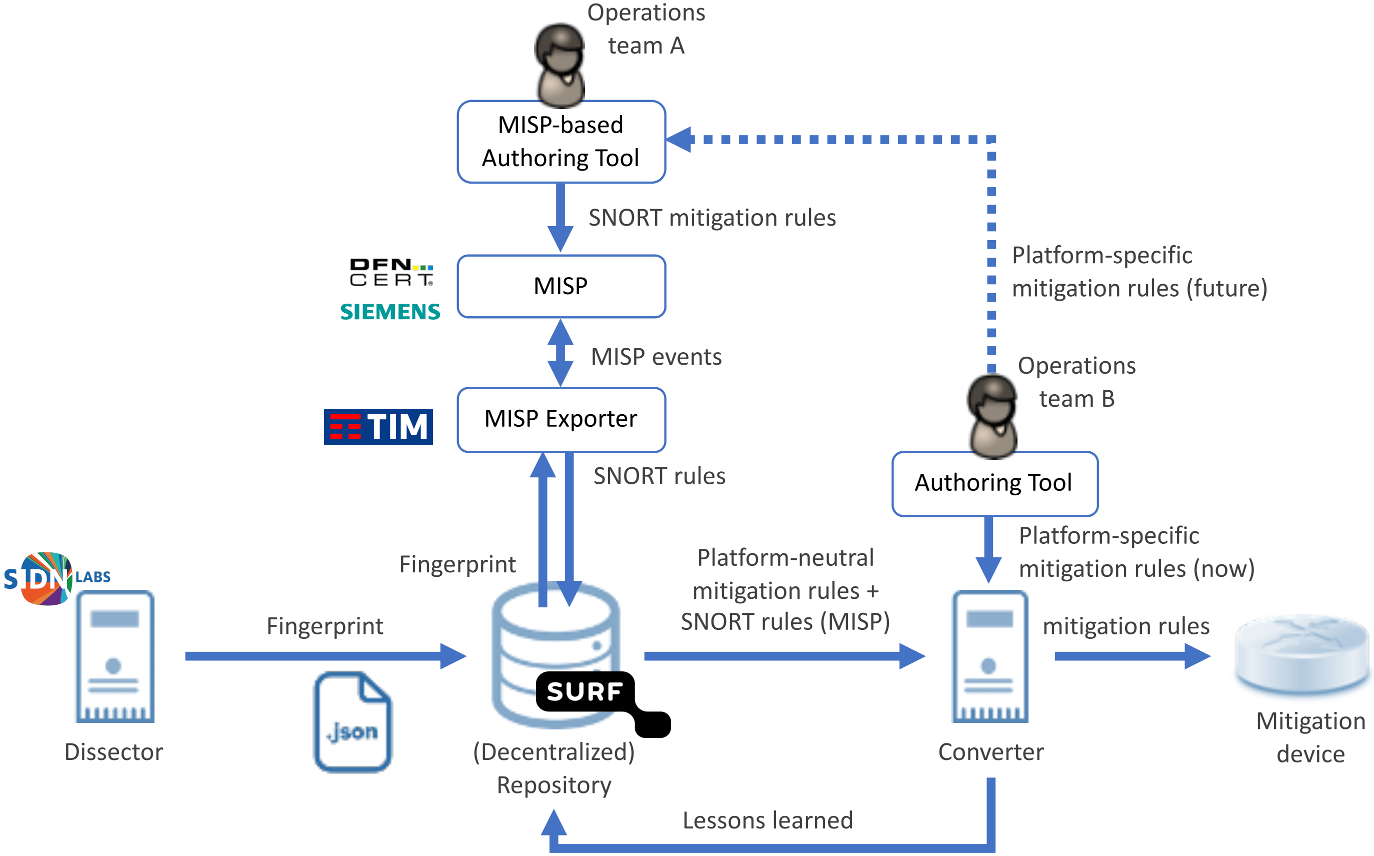
Challenges next 6 months

- Improve the software for other attack types
- We do need more attack files (pcap and flows)
- Fingerprint enrichment (IPs etc)
    - In the central repository
    - In the local repository
- Enable local plugins on dissector
- Repository upload (you can decide where to upload the fingerprints)
- **Get and share fingerprints from production systems**

CONCORDIA-specific

- Progress report on clearing house work in Task 3.2
- Publish first version of DDoS clearing house cookbook
- Interworking with cross-sector threat intel platform for Europe

Interaction with MISP (draft)



No More DDoS Anti-DDoS-Coalitie

CONCORDIA Cyber security cOmpeteNCe fOr Research anD InnovAtion

Q&A

Clearing house on GitHub:
https://github.com/ddos-clearing-house/

Cristian Hesselman
cristian.hesselman@sidn.nl
@hesselma
+31 6 25 07 87 33

This work was partly funded by the European Union’s Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: https://www.concordia-h2020.eu/