NBIP nationale beheersorganisatie internet providers 20 jaar!

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

DDoS Clearing House for Europe

NBIP@20

Utrecht, NL, and online

July 8, 2021

Cristian Hesselman (SIDN Labs)

Partners: SIDN, University of Twente, Telecom Italia, FORTH, University of Zurich, SURF, University of Lancaster, CODE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

Objective DDoS Research

- Enable European critical infrastructure to proactively and collaboratively protect themselves against DDoS attacks

- Approach: pilot a Clearing House for **exchanging DDoS metadata** with European industry for Europe

Key challenge: increase to TRL 5-7 and grow deployment

- Key outputs: pilots in the Netherlands and Italy, DDoS clearing house blueprint

Key innovations

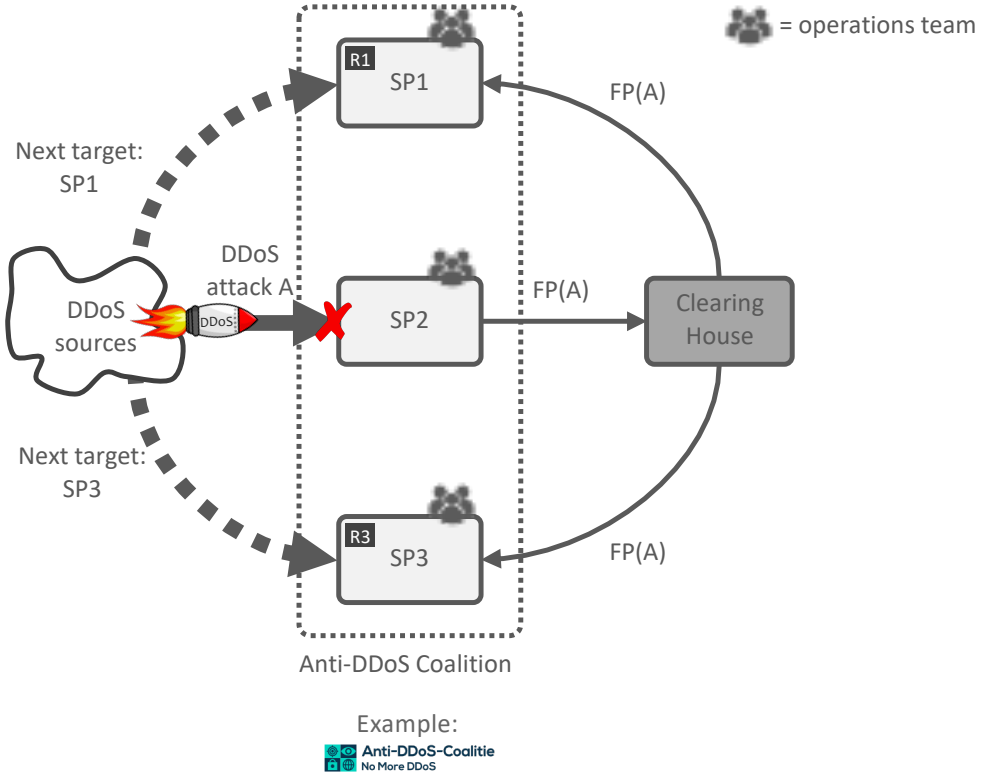
- Bridge **multidisciplinary gap** to deployment, more than tech!

- **Opensource design** that we make available through a “cookbook”
  - Technology, legal, organizational, experiences, lessons learned
  - Enable federations of organizations to set up their own DDoS clearing house
  - Main use case is the Dutch Anti-DDoS Coalition (NL-ADC)

- Can operate across **heterogeneous networks**

DDoS Clearing House Concept

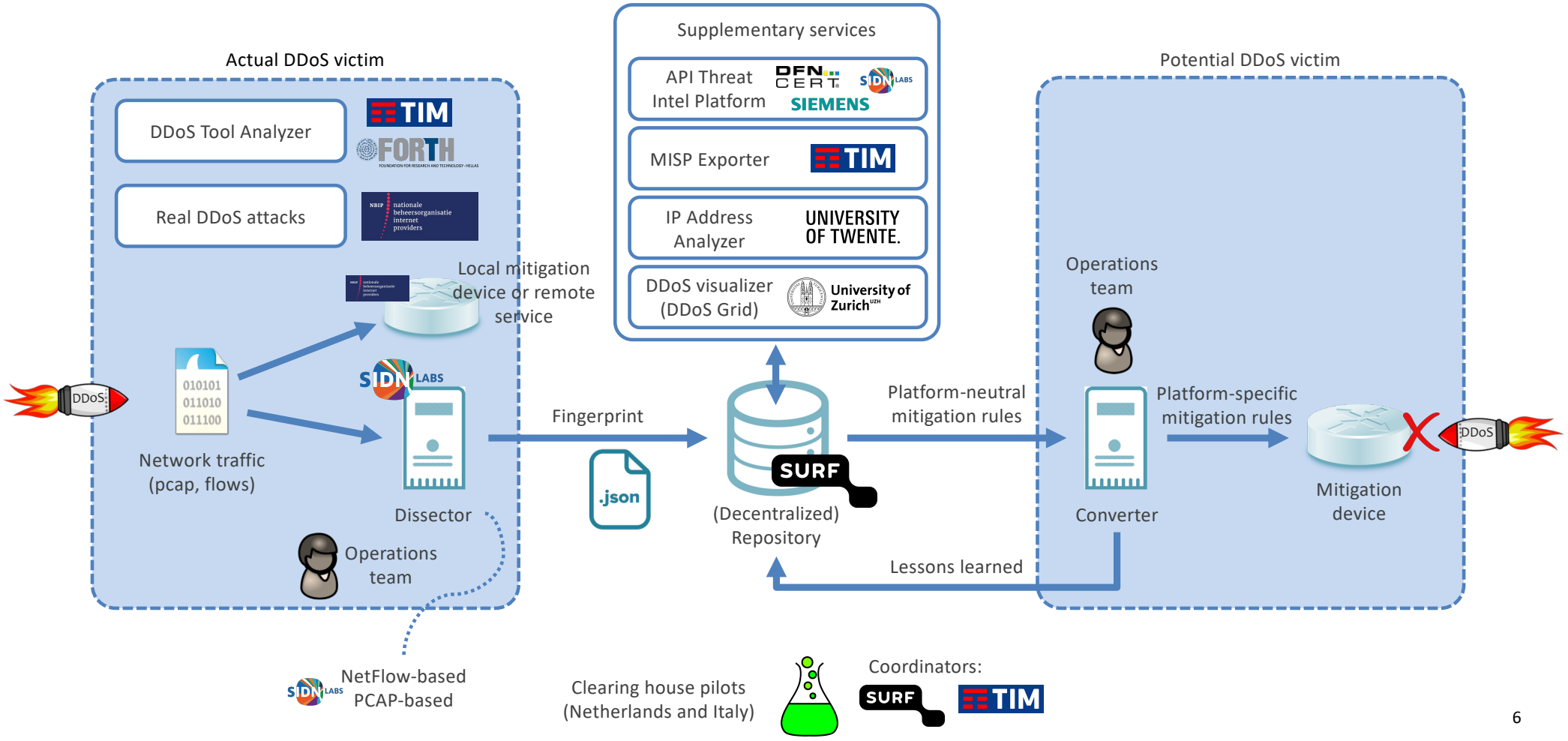
- Continuous and automatic sharing of **DDoS fingerprints**, buys providers time (proactive)
- **Extends DDoS protection services** that service providers use and does not replace them
- Generic concept: across sectors, Member States, business units, etc.



DDoS Fingerprint Example


```
{
  "attack_vector": [
      "src_ips": [
        ommited;
      ],
      "attack_vector_key": "66f2e83fde0e6351d3f5ad967c6230aa3b60dbc498ad13b074296cb5f84c7734",
      "one_line_fingerprint": "{'dns_qry_type': 1, 'ip_proto': 'UDP',
      'highest_protocol': 'DNS', 'dns_qry_name': 'a.packetdevil.com',
      'frame_len': 1514, 'udp_length': 4103, 'srcport': 53,
      'fragmentation': True, 'src_ips': 'omitted'}"
    }
  ],
  "start_time": "2013-08-14 23:04:00",
  "duration_sec": 0.16,
  "total_dst_ports": 4649,
  "avg_bps": 143426993,
  "total_packets": 16471,
  "ddos_attack_key": "44518107642b9ac7098174a16cbf220395c862bf26389c734e0b109b318e9291",
  "key": "44518107642b9ac",
  "total_ips": 2065,
  "tags": [
    "AMPLIFICATION",
    "DNS",
    "FRAGMENTATION",
    "UDP_SUSPECT_LENGTH",
    "DNS_QUERY",
    "SINGLE_VECTOR_ATTACK"
  ]
}
```

Main Components and Data Flows

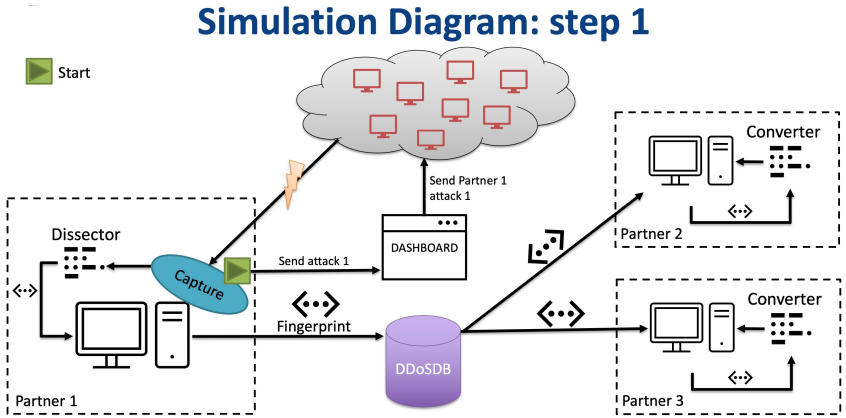


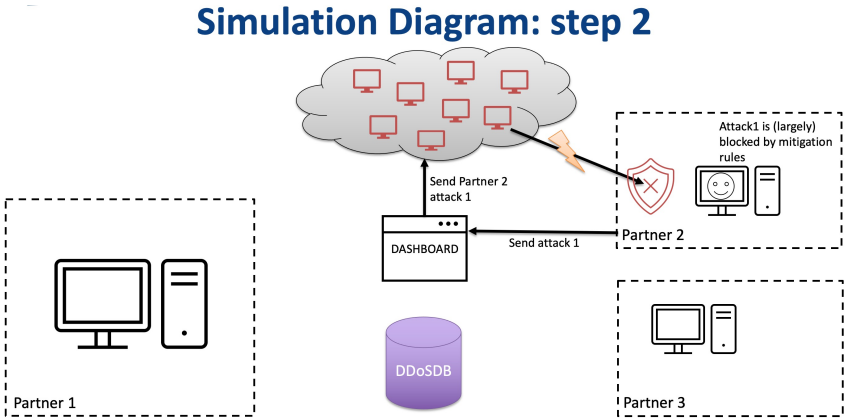
Component Maturity Indication

Name	Function	Maturity
Dissector	Generate DDoS fingerprints using PCAP files or flow data	High
DDoSDB	Insert, update, search, and retrieve DDoS fingerprints	High
Converter	Generate mitigation rules based on DDoS fingerprints	Medium
DDoS Grid	Dashboard for the visualization of DDoS fingerprints	High
IP Address Analyzer	Enriches fingerprints with details about IP addresses involved in an attack, based on measurements	Low
DDoS Tool Analyzer	Generate DDoS fingerprints of tools used to launch DDoS attacks	Low
MISP Exporter	Generate MISP events based on DDoS fingerprints	Medium

New Concept: Distributed CH Simulator

- The “DDoS target” manually initiates a stream of **test traffic** to itself through distributed cloud VMs
- Target’s Dissector creates fingerprint and sends it to the other partners through DDoS-DB, **without PII**
- Receivers locally construct filtering rules and manually initiate the same stream to **test the rules**





DDoS clearing house in the Netherlands

- DDoS clearing house R&D
- DDoS clearing house cookbook
- Technical evaluation through pilots in the Netherlands and Italy

- Sharing of operational experience
- Large-scale multi-party DDoS drills
- **DDoS clearing house operations**
- Operational ADC organization

CONCORDIA is funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: https://www.concordia-h2020.eu/

Dutch Anti-DDoS Coalition (NL-ADC)

DDoS Clearing House Planning @NL-ADC

Phase		Q1-2021	Q2-2021	Q3-2021	Q4-2021	Q1-2022	Q2-2022
-1	**Distributed simulation** NEW!						
0	Pilot						
1	Basic production						
2	Full production						

Dev: CONCORDIA team
Ops: SIDN Labs + CONCORDIA team

Dev: CONCORDIA team
Ops: database operator (NBIP) + NL-ADC members

Dev: CONCORDIA team
Ops: SIDN Labs + NL-ADC members

Dev: software developer (TBD)
Ops: database operator (NBIP) + NL-ADC members

NBIP plays a key role in the DDoS-CH

- Highly aligned mission
  - Robust Internet for NaWas members and society
  - Ambition to grow to EU-level
  - Collaboration is in NBIP's DNA
  - Open and not-for-profit

- Great people
  - Widely acknowledged DDoS experts
  - Data for collaborative DDoS research
  - Vocal on importance of collaborative DDoS mitigation

Further reading

https://www.sidnlabs.nl/en/news-and-blogs/new-ddos-classifiers-for-the-ddos-clearing-house

https://www.sidnlabs.nl/en/news-and-blogs/work-in-progress-the-concordia-platform-for-threat-intelligence

https://www.sidnlabs.nl/en/news-and-blogs/new-version-of-the-ddos-clearing-house-core-components

https://www.sidnlabs.nl/en/news-and-blogs/dutch-anti-ddos-coalition-lessons-learned-and-the-way-forward

https://www.sidnlabs.nl/en/news-and-blogs/setting-up-a-national-ddos-clearing-house

https://www.sidnlabs.nl/en/news-and-blogs/increasing-the-netherlands-ddos-resilience-together

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

www.linkedin.com/in/concordia-h2020

www.youtube.com/concordiah2020

Dutch Anti-DDoS Coalition:
https://www.nomoreddos.org/en/

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

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

Thijs van den Hout
thijs.vandenhout@sidn.nl
@thijsvandenhout

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