MADINAS BoF: Mitigating DDoS Attacks Close to the Sources

M. Boucadair

October 2020

Context

- DDoS attacks are increasing
  - Residential and Enterprises are among top targets
  - Attack are more large (volume) and complex
  - Generalized because of the advent of “DDoS as a Service” offerings

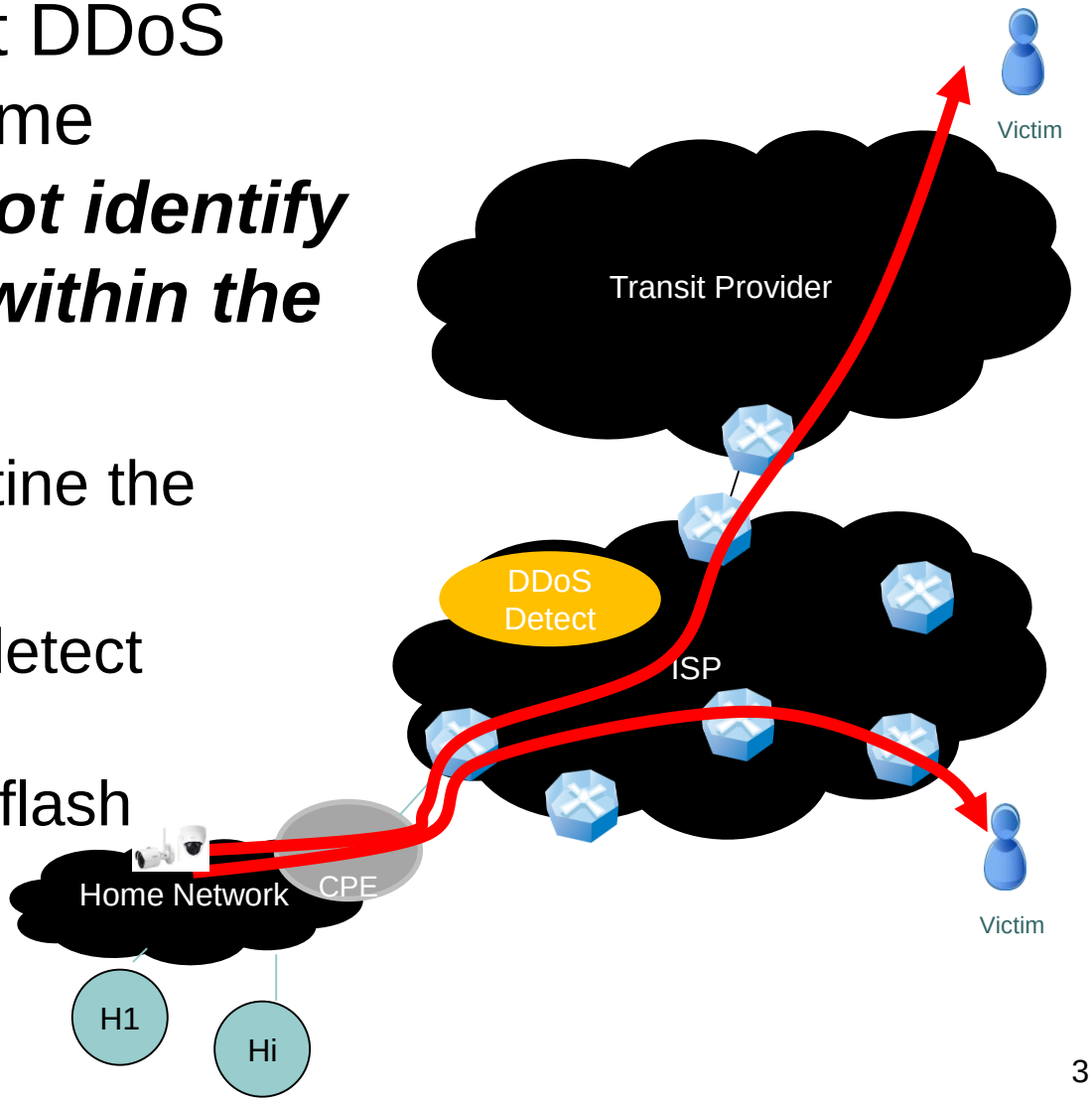
*“Poor security on many IoT devices makes them soft targets and often victims **may not even know they have been infected**”*
Symantec

“OVH CTO Octave Klaba said the attacks OVH suffered were “close to 1 Tbps” and noted that the flood of traffic was a botnet made up of nearly 150,000 digital video recorders and IP cameras capable of sending 1.5 Tbps in DDoS traffic.”

- Have impacts on the reputation of networks hosting these devices

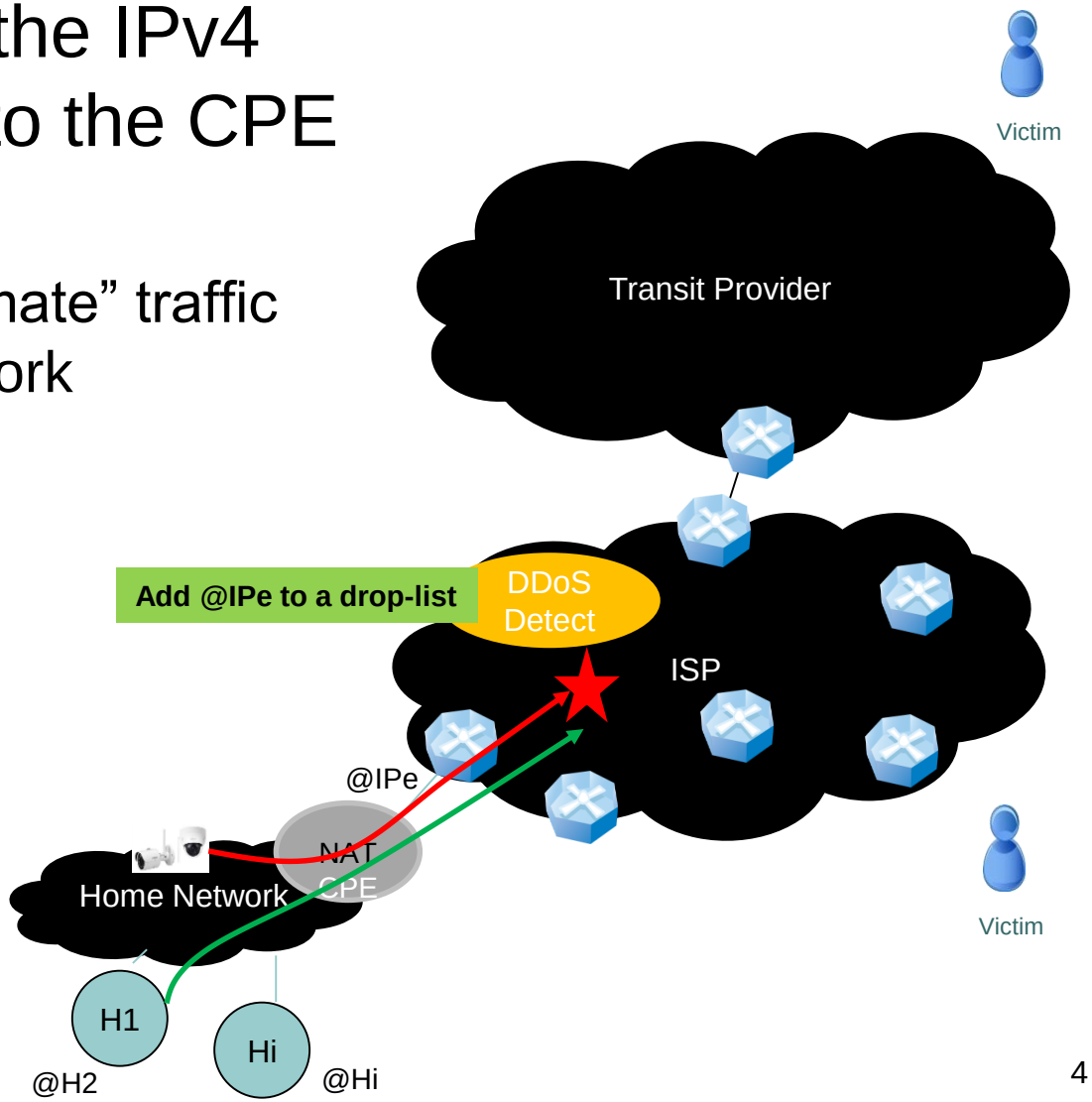
Filter Close to Sources: ISP

- The ISP can detect DDoS traffic sent from home networks but ***cannot identify infected devices within the home network***
  - ISP cannot quarantine the infected device
  - Some heuristic to detect attacks may not be deterministic (e.g., flash crowds)



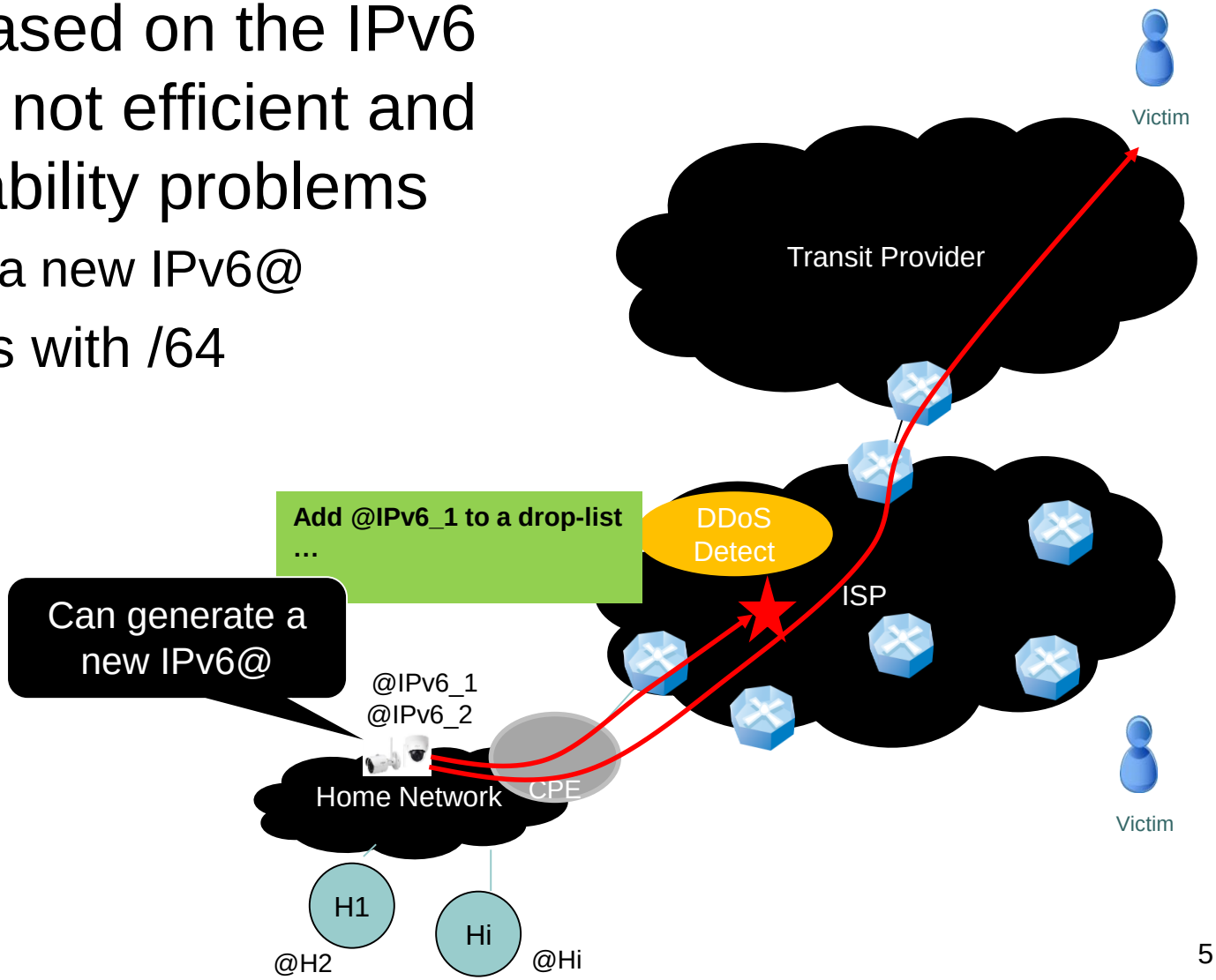
Filter Close to Sources: ISP

- Filtering based on the IPv4 address assigned to the CPE is sub-optimal
  - Impacts other “legitimate” traffic from that home network



Filter Close to Sources: ISP

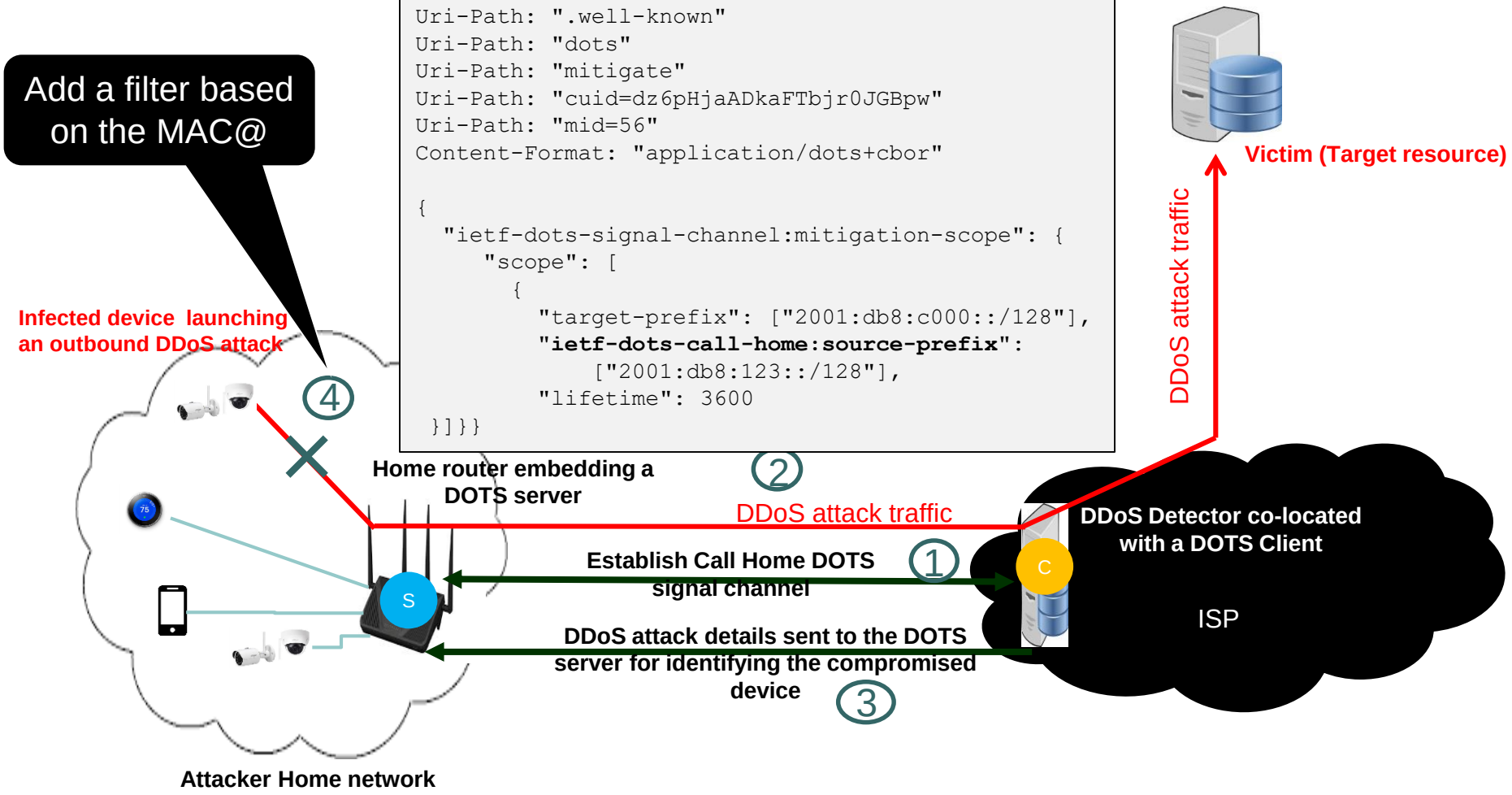
- Filtering based on the IPv6 address is not efficient and have scalability problems
  - Generate a new IPv6@
- Same issues with /64



Filter Close to Sources: CPE

```
Header: PUT (Code=0.03)
Uri-Path: ".well-known"
Uri-Path: "dots"
Uri-Path: "mitigate"
Uri-Path: "cuid=dz6pHjaADkaFTbjr0JGBpw"
Uri-Path: "mid=56"
Content-Format: "application/dots+cbor"

{
  "ietf-dots-signal-channel:mitigation-scope": {
     "scope": [
       {
         "target-prefix": ["2001:db8:c000::/128"],
         "ietf-dots-call-home:source-prefix":
             ["2001:db8:123::/128"],
         "lifetime": 3600
 }]}}
```



DOTS stands for DDoS Open Threat Signaling (RFC8782)

The Requirement

- **Means to unambiguously and persistently identify devices within a home network are required to enforce policies**
  - MAC filtering is broken if a new MAC@ is generated by the infected device
  - The problem is even exacerbated with MAC randomization