Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Call Home

https://tools.ietf.org/html/draft-reddy-dots-home-network-01

IETF 103, Bangkok

November 2018

Presenter: T. Reddy (McAfee)

J.Harsha (McAfee)

M. Boucadair (Orange)

J. Shallow (NCC)

Agenda

- Problem Statement
- Solution Overview
- DOTS Signal Channel Extension
- Questions & Comments

Problem Statement (1)

- Endpoints (including IoT devices) in home networks can be compromised and used to launch DDoS attacks on target
  - The problem is also applicable to other networks like branch and SOHO offices

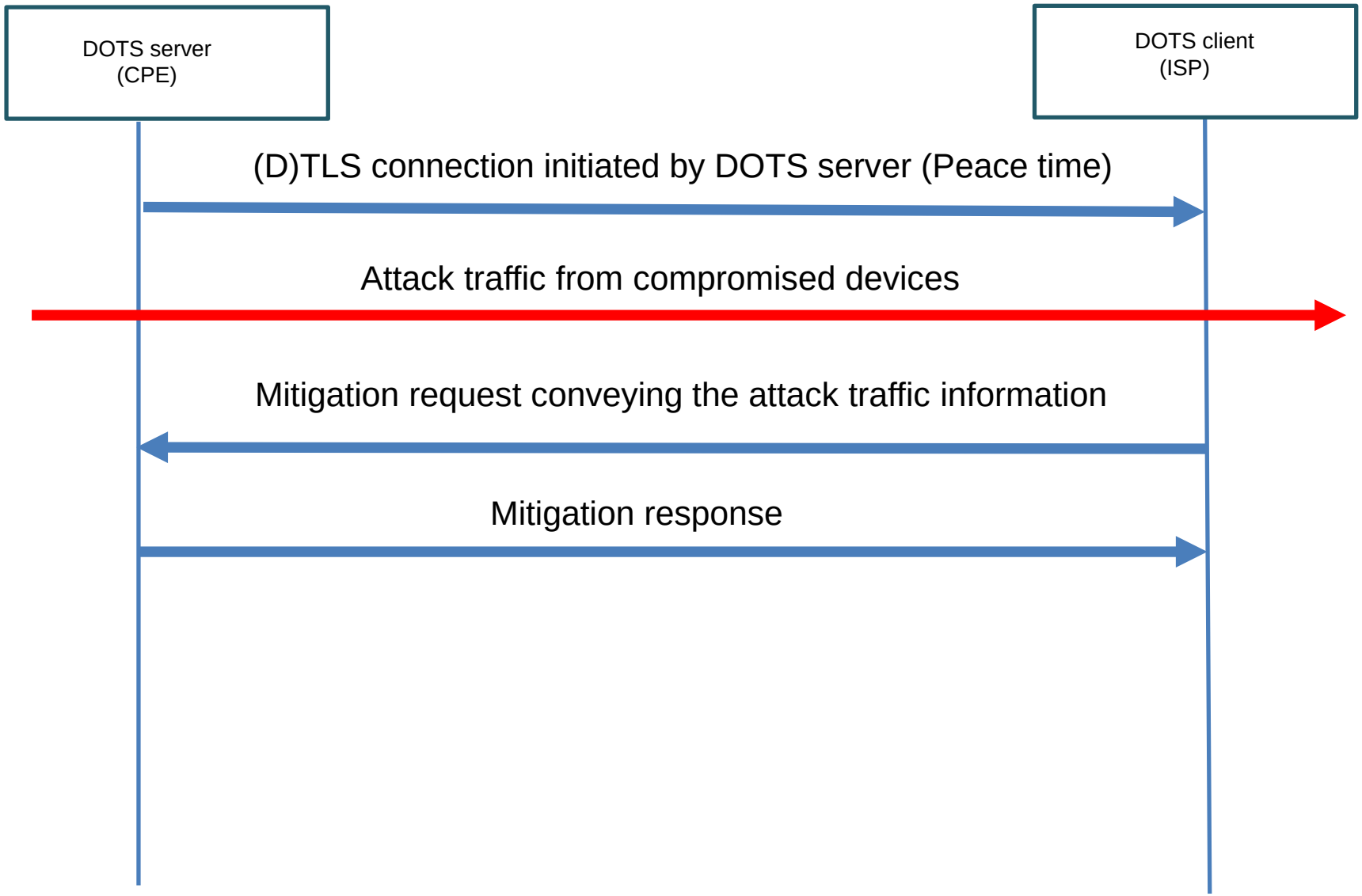
- Network devices in home networks offer some security functions:
  - E.g., McAfee, Trend Micro Security, Dojo, Bitdefender, Cujo and other security vendors offer Home network security (stand-alone gateway or home router)
  - Home routers have fast-path to boost the throughput and not all packets in a flow are punted through the slow path for inspection
  - Home routers cannot detect attack traffic sent to the target after the flow is switched to fast path
  - Home routers may not have the capability to detect new emerging and sophisticated attacks

Problem Statement (2)

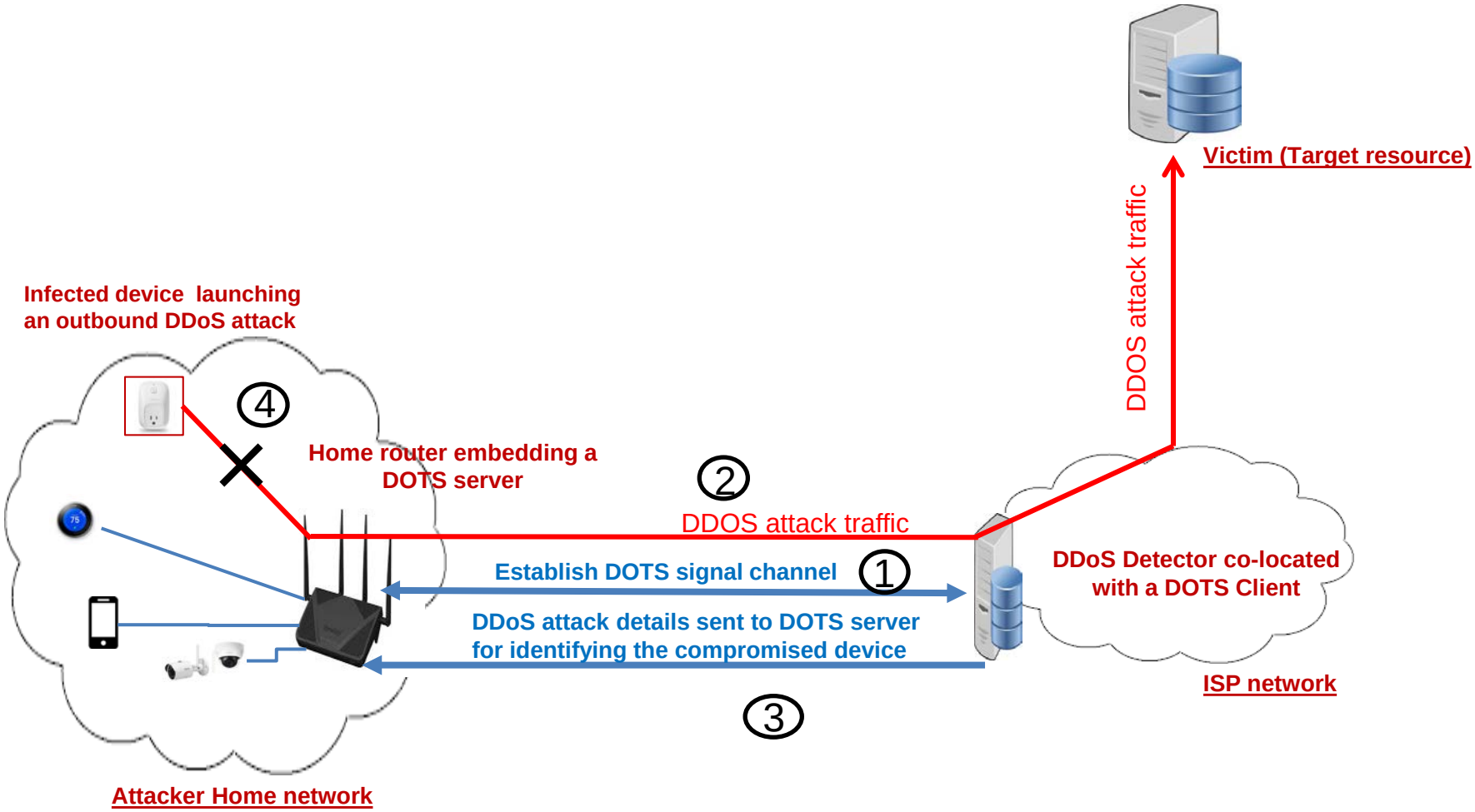
- ISP can detect DDoS traffic from the home network but cannot identify infected devices (behind NAT) in the home network
  - ISP cannot quarantine the infected device
  - Some heuristic to detect attacks may not be deterministic (e.g., flash crowds)

- Compromised IPv6 devices can easily change the IPv6 addresses (e.g., SLAAC, use an IP address not assigned by the DHCP server), and ISP cannot identify such devices

Solution Overview: Call Home (1)



Solution Overview: Call Home (2)



Solution Overview: Call Home (3)

- The Call Home function enables the DOTS server behind a NAT to be reachable by only the intended DOTS client
- The home router identifies the infected device based on the DDoS attack traffic information sent by the ISP and take appropriate mitigation actions
  - If NAT is on-path, the home router uses the attack flow information to find the internal source IP address of the compromised device
- CPE can punt all the traffic from the compromised device (to target) to slow path to detect and block outgoing DDoS attack traffic

DOTS Signal Channel Extension (1)

- New IANA-assigned port to accept (D)TLS connection for call home
  - Port number 4647 is strongly suggested
- Mitigation request is enhanced to convey the attacker information
  - Source-prefix : list of attacker prefixes
  - Source-port-range : list of port numbers used by attack traffic flows
  - Source-icmp-type-range : list of ICMP types

DOTS Signal Channel Extension (2)

- ‘target-prefix’ and ‘source-prefix’ become mandatory attributes

- DOTS server domain administrator consent MAY be required to block the traffic from a compromised device to the attack target

- New “request-rejected” conflict-cause code returned by the DOTS server to indicate the attack traffic has been classified as legitimate traffic

Open Questions

- Does DOTS client also need to convey Attack Name/type or ID for diagnostics ?
  - The home router may not be capable of detecting new merging/sophisticated attacks.

- Is DOTS data channel Call Home service required (if required, can RESTCONF Call Home defined in RFC8071 be used) ?

- Comments and suggestions are welcome!