DOTS
1st Interoperability Test

IETF 100 Hackathon

DOTS is now working!

- DDoS protection is one of the biggest issues of the Int ernet.
- DOTS(DDoS Open Threat Signaling) is:
  - Automation and Standardization of signaling for DDoS prote ction
- DOTS WG is aiming to make it standardized in this year
  - Now we have several individual implementations
    - go-dots (open-sourced project) from NTT
    - NCC's private implementation
  - This 1st interoperability test at this hackathon is a giant step for it.
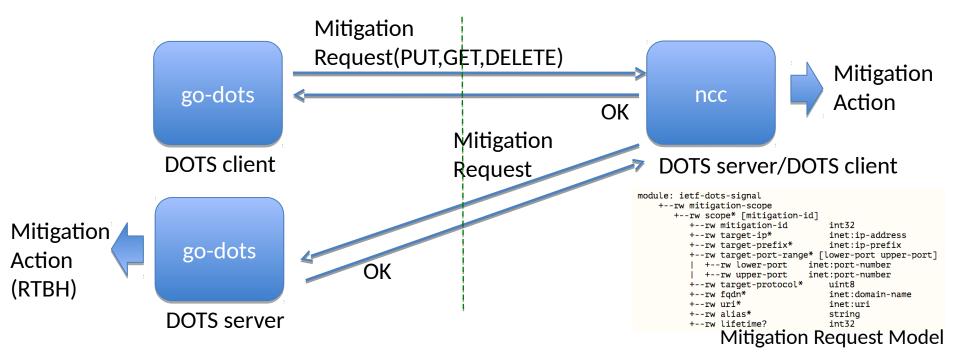
What happened in the Hackathon

- Drive 3 projects with 7 participants
  - include 3 remotely from Tokyo, London, Nanjing
- 3 Projects are:
1. 1st Interoperability test of 2 individual implementations
2. Adding new features and extensions to the open-sourced implementation
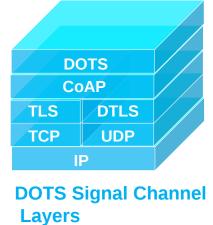3. (Integration with a detection system of Mirai bot net)

Result of the Interop Test

Purpose: Check interoperability of the messages on the signal channel

Item #	Messages	CoAP Method	Interop Testing (client -> server)		Internal Testing		
			go-dots -> ncc	ncc -> go-dots	ncc	go-dots(ntt)	huawei
1	Mitigation Request	PUT	☑	☑	☑	☑	☑
2	Mitigation Request Withdraw	DELETE	☑	▲	☑	☑	☑
3	Mitigation Request Status	GET	☑	▲	☑	☑	☑
4	Mitigation Request Status All	GET	☑	▲	☑	☑	☑
5	Mitigation Status Notify	observe	-	-	☑	-	-
6	Efficacy Update	PUT	-	-	☑	-	☑
7	Session Configuration	PUT	☑	▲	☑	☑	☑
8	Session Configuration Delete	DELETE	▲	▲	☑	☑	☑
9	Session Configuration Retrieve	GET	☑	▲	☑	☑	☑
10	Heartbeat	COAP ping	-	-	☑	-	-

What we proved in the Interop

Mitigation Request(PUT,GET,DELETE)

go-dots

DOTS client

Mitigation Request

go-dots

DOTS server

Mitigation Action (RTBH)

OK

ncc

DOTS server/DOTS client

Mitigation Action

OK

```
module: ietf-dots-signal
    +--rw mitigation-scope
        +--rw scope* [mitigation-id]
            +--rw mitigation-id        int32
            +--rw target-ip*           inet:ip-address
            +--rw target-prefix*       inet:ip-prefix
            +--rw target-port-range* [lower-port upper-port]
            |  +--rw lower-port    inet:port-number
            |  +--rw upper-port    inet:port-number
            +--rw target-protocol*     uint8
            +--rw fqdn*                inet:domain-name
            +--rw uri*                 inet:uri
            +--rw alias*               string
            +--rw lifetime?            int32
```

Mitigation Request Model

- We can start and handle a mitigation from each client over DOTS signal-channel (CoAP over DTLS)
- Plus, NCC's implementation can act as a DOTS relay(gateway), so we proved that relayed mitigation requests can work over multiple organizations.

DOTS
CoAP
TLS | DTLS
TCP | UDP
IP

DOTS Signal Channel Layers

Feedback to DOTS WG

- Implementation Experiences
  - ex. most of the code modification was related to en code/decode of CoAP mapping
  - there were many implicit specifications we need to figure out and compromise
- Need more description of the content and code
- approx. 60% of the signal-channel spec has been proved to work
  - The rest will be done until the next IETF