

IETF Hackathon: DOTS Interop

IETF 101

17-18 March, 2018

London



DOTS Hackathon Plan

- Test the interoperability between independent implementations:
 - See the maturity of these core specs of DOTS protocol
 - draft-ietf-dots-signal-channel-17
 - draft-ietf-dots-data-channel-13
- Implementations
 - OSS by NTT: nttdots: <https://github.com/nttdots/go-dots>
 - Proprietary implementation of NCC Group
 - Proprietary implementation of Arbor (couldn't attend this time)
 - Proprietary implementation of Huawei based on nttdots

DOTS Hackathon Achieved

draft version: draft-ietf-dots-signal-channel-17 or later

<https://datatracker.ietf.org/doc/draft-ietf-dots-signal-channel/>

Purpose: Check interoperability of the messages on the signal channel

DOTS Signal Channel Features implementation status

#	feature	ncc*	nttdots*	huawei	arbor
1	Session Configuration	✓	✓		
2	Mitigation Request	✓	✓		
3	CoAP Ping	✓	✓		
4	observe	✓			
5	efficacy update	✓			
6	request confliction handling	✓			
7	confliction notify				
8	deadman's trigger				
9	gateway function	✓			
10	redirection				
11	happy eyeballs	✓			

* supporting both PKI and PSK

DOTS Data Channel Features implementation status

#	feature	ncc	nttdots	huawei	arbor
1	Register DOTS clients				
2	Register Alias	✓			
3	Register Filtering Rules	✓			

Interoperability Testing Results

1. Session Configuration		DOTS Server			
		ncc	nttdots	huawei	arbor
DOTS Client	ncc	✓	✓		
	go-dots(ntt)	✓	✓		
	huawei				
	arbor				

2. Mitigation Request		DOTS Server			
		ncc	nttdots	huawei	arbor
DOTS Client	ncc	✓ *	✓ *		
	go-dots(ntt)	✓ *	✓ *		
	huawei				
	arbor				

* supporting mid/cuid in URI-Path(the latest spec)

3. CoAP Ping		DOTS Server			
		ncc	nttdots	huawei	arbor
DOTS Client	ncc	✓	✓		
	go-dots(ntt)	✓	✓		
	huawei				
	arbor				

We are getting there!

- DOTS (DDoS Open Threat Signaling) protocol
 - Makes Distributed Denial of Service (DDoS) Protection more effective with its programmatic capability.
 - Protects the Internet from DDoS attacks.
- We confirmed that we can do cooperative DDoS Protection operations between (at least 2) independent implementations

Example Protection of IP

- Successful Mitigation Request from OSS DOTS client (nttdots) to proprietary DOTS server (NCC Group) – and vice versa.

The screenshot displays the nccgroup DDoS Secure interface. The main section is titled "Mitigations Info - Appliance" and shows a table of active mitigations. The table has columns for State, Destination IP, Portal, Requester, and Thresholds (Lower and Upper for Pkts/s and Bits/s). It also shows the current and peak values for Pkts/s and Bits/s for the requesting device(s). The table lists two active mitigations, both with zero current and peak values.

	State	Destination IP	Portal	Requester	Thresholds				Requesting device(s)				Mitigation	
					Pkts/s		Bits/s		Pkts/s		Bits/s		Pkts/s	
					Lower	Upper	Lower	Upper	Current	Peak	Current	Peak	Current	Peak
1	Active	1.1.2.201	ex-portal1	13.115.156.186	0	0	0	0	0	0	0	0	0	0
2	Configured-Active	1.1.1.69	ex-portal1	192.168.191.2	0	0	0	0	0	0	0	0	0	0

On the right side of the interface, there is a sidebar with the following information:

- Date and Time: Sat Mar 17 2018 11:05:07 UTC
- IP Address: 192.168.191.2
- Status: DEFENDING
- Mode: STANDALONE
- Link: [Demo Replay]
- Appliance Statistics:
 - Inb'd: 2.282M Bits/s
 - Outb'd: 3.635M Bits/s
 - Inb'd: 3.214k Pkts/s
 - Outb'd: 759 Pkts/s
- Legend:
 - Bandwidth
 - Packet Rate
 - Blocked Protocol (highlighted in red)

What we learned

- We can meet the expectations for DOTS protocol from the market soon
 - Draft Signal Channel spec is almost stable
- In the Hackathon, we tested based on proposing spec (to be included in the coming -18 draft), so it is proven to work!
- Discussed and clarified a lot about the current drafts text
- Discussed adding new feature on the protocol, which could be included in the DOTS spec in future

Achievements in detail (for WG)

Achievement 1. During the Hackathon

Successfully worked interoperable features

- CRUD operations on session configuration and mitigation request
- gateway function (on NCC Group side)
 - Nttdots client traffic to NCC Group DOTS Gateway relayed to nttdots server + cdid addition
 - the usage of "cdid" is now under discussion
- PKI and PSK mode on DTLS
- cuid/mid in URI-path: it helps an implementation using libcoap

Achievement 2. In preparation for the Hackathon

Actually nttdots and NCC Group did interop tests internally 3 times! before the Hackathon

- Agreed on trying with the latest spec (-17 or later)
 - Updated models so as to comply with that
- Added CoAP ping capability (on nttdots side)
- Many fixes of the code on both side

Wrap Up

Team members:

Kaname Nishizuka (NTTCom)

Jon Shallow (NCC Group)

Liang 'Frank' Xia (Huawei)

First timers @ IETF/Hackathon:

Nagata Takahiko (Lepidum)

Dong Yue (Huawei)

Thank You