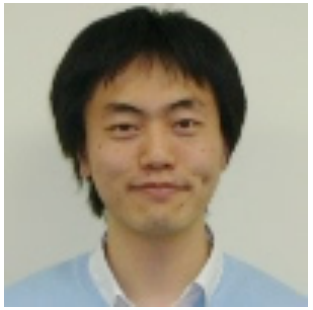
IETF101報告会
DOTS WG

2018.4.27

Kaname Nishizuka@NTT Communications
@__kaname__

自己紹介

- 2006年 NTTコミュニケーションズ入社
- OCNアクセス系ネットワークの設計に従事した後、
  大規模ISP向けのトータル保守運用サービスを担当
- メインフィールド
  - トラフィック分析
  - DDoS対策ソリューション
  - IPv4枯渇対策関連技術
- IETF提案活動
  - DOTS WG
- JPNIC「IPv6教育専門家チーム」



NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

IETF101@ロンドン
DOTS 関連報告

3

dots WG

- **DDoS Open Threat Signaling (dots)**
- **設立：2015-06**
- **Chairs: Roman Danyliw(CERT)**

Tobias Gondrom（OWASP, Huawei)

- 新しいWG(BoF:IETF92 / Meeting:IETF93～)
- DDoS対策を効率的に実現するために、DDoSに関連した情報のリアルタイムでのシグナリングを規格化する
  - 自動化
  - より大規模な防御システム
  - ベンダ独自なソリューションからの開放

DOTSプロトコルが実現すること

■ 攻撃を受けるネットワーク(加入者ネットワークや、企業ネットワーク、データセンタネットワークなど)から、攻撃を防御する機能を持つ上流のネットワーク(トランジット事業者やDDoS対策事業者)への防御依頼を標準化・自動化します。

■ DOTSプロトコルは以下を実現します。

1. 防御依頼を機械的に行うことができるため、DDoS攻撃の検知から防御までを、組織を超えて自動化することが期待できます。
2. 防御依頼のシグナルが標準化されることにより、ベンダ独自のDDoS対策ソリューションからの開放が期待できます。
3. 防御依頼をリレーして伝搬することで、より大規模な防御システムを構築できることが期待できます。

IETF101におけるDOTS関連進捗まとめ

- 3つの独立した実装が揃った
  - OSS実装: go-dots
  - ベンダ実装: NCCGroup
  - ベンダ実装: Arbor (NEW!)
- コアな仕様の一つがWGLCとなる見込み
  - シグナルチャンネル -> 相互接続試験済み, WGLC間近
  - データチャンネル -> 今後の相互接続試験のターゲット
- 仕様をサポートするドラフトも大きく進展
  - 要求事項(Requirement): 2回目のWGLCへ
  - アーキテクチャ: WGLCへ
  - ユースケース: 内容のシンプル化へ(後述)

DOTS WG ミーティング

1. Note well, logistics and introduction (chairs, 5 min)

2. Hackathon Report(s) (Kaname Nishizuka/Jon Shallow, 20 min)

3. Additional Implementation Reports (25 min)
   (a) Arbor Networks Report (Andrew Mortensen*)
   (b) NCC Group Report (Jon Shallow)
   (c) open mic

4. Protocol drafts (30 min)
   (a) draft-ietf-dots-signal-channel-17 (Mohamed Boucadair)
   (b) draft-ietf-dots-data-channel-13 (Mohamed Boucadair)

5. Architecture (draft-ietf-dots-architecture-05) (Andrew Mortensen*, 10 min)

6. Use Cases (draft-ietf-dots-use-cases-09) (Daniel Migault, 15 min)

7. Open Mic (15 min)

8. Closing (chairs, 5 min)

* Remote Presenter

IETF Hackathon Report: DOTS Interop

Kaname Nishizuka/Jon Shallow

IETF 101 DOTS WG

20 March, 2018

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
	ncc	☑	☑		
	go-dots(ntt)	☑	☑		
	huawei				
DOTS Client	arbor				

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

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

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

Features and implementation status

# 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

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				

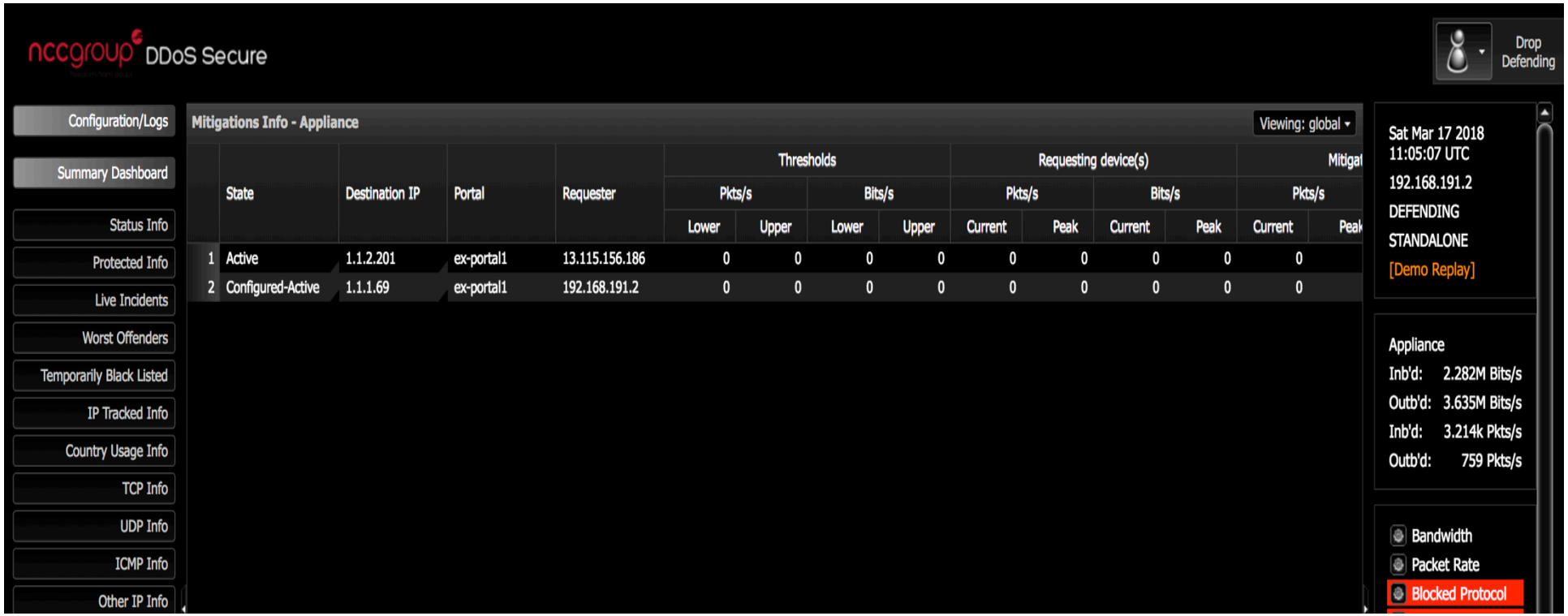
We are getting there!

- 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.



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

Achievements in detail (for WG)

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 (nttdots)
- Many fixes of the code on both side

成果と進捗

- OSSはリファレンス実装に
  - 実装をオープンにしたことで、標準化の進みを加速

- WGの今後の方向性
  - 引き続きgo-dotsとNCCグループは Interop を実施
    - ✓ データチャンネルが今後のターゲットに
  - さらに Interop に参加する実装を集める
    - ✓ 業界最大手のArborの参加が見えてきた