dots implementation report

IETF98 DOTS WG

2017.03.28

Kaname Nishizuka, NTT Communications
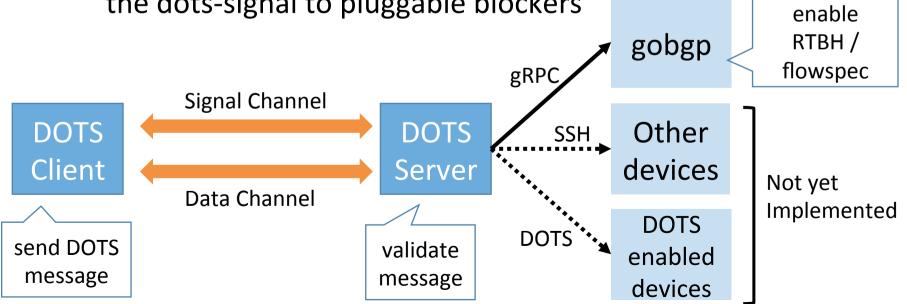
Implementation Summary

- NTT Communications is developing a DOTS client and server software with specifications on:
    - draft-reddy-dots-signal-channel
    - draft-reddy-dots-data-channel

- It works well ☺

- It will be open-sourced

- It is aimed to implement full DOTS protocol specification in accordance with maturing of DOTS protocol itself

Demo

- We can show you a demo
- Please contact us

Application

- Capability of DOTS client:
  - sending DOTS message to DOTS server in CoAP over DTLS as dots-signal

- Capability of DOTS server:
  - receiving and validating dots-signal
  - starting mitigation by handing over the dots-signal to pluggable blockers

Pluggable Blockers

gobgp — enable RTBH / flowspec

DOTS Client ←Signal Channel→ DOTS Server

DOTS Client ←Data Channel→ DOTS Server

gRPC → gobgp

SSH → Other devices

DOTS → DOTS enabled devices

Not yet Implemented

send DOTS message
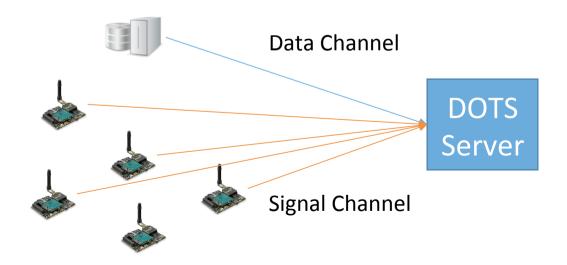
validate message

Implementation experience

- It is implemented in go-lang.
- Core specification of signaling is mature to be implemented
- Finding good libraries(CoAP, RESTCONF, especially DTLS) is rather difficult.
  - We are trying several DTLS libraries, but we haven't found any good DTLS library which fully work with full specification of DOTS signal channel.

Issue1: Coupling of data-channel & signal-channel

- Two drafts require the same CN(CommonName) for client side in DTLS(signal-channel) and TLS(data-channel)
  - 5.3.1 "The DOTS server couples the DOTS signal and data channel sessions using the DOTS client identity"
- If DOTS is going to use other mutual authentication technologies, it needs generalized concept of CN
  - "Customer" ? "Organization" ? "mitigation-id"?
  - Should it be included in signal and data messages in order to couple them?

Issue2: data-channel only host & signal-channel only host

- Do you think there is a usecase of a separated DOTS signal-channel clients and data-channel clients?
  - Data channel only controller and other small signal-channel only devices

Data Channel

DOTS Server

Signal Channel

Thank you!

- Q and A
- Comments