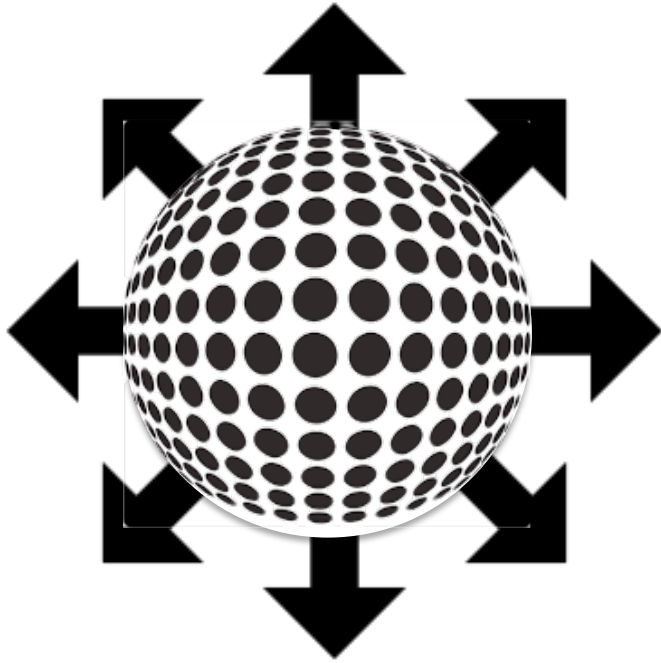IETF 95

DDoS Open Threat Signaling (DOTS) Working Group

draft-ietf-dots-use-cases-01

Roland Dobbins – Arbor Networks

Stefan Fouant – Corero Network Security

Daniel Migault – Ericsson

Robert Moskowitz – HTT Consulting

Nik Teague – Verisign

Liang 'Frank' Xia – Huawei

draft-ietf-dots-use-cases-01 Summary

- Provides example use-cases for DOTS (actually, categories).

- All examples can be CE/PE or PE/PE.

- Room for wide variation within each category.

- All DOTS communications in each example can be directly between DOTS servers and DOTS clients, or mediated by DOTS relays.

- DOTS relays can forward messages between DOTS clients and servers using either stateless transport, stateful transport, or a combination of the two.

- DOTS relays can aggregate service requests, status messages, and responses.

- DOTS relays can filter service requests, status messages, and responses

DOTS WG

draft-ietf-dots-use-cases-01 Summary (cont.)

- Use-cases in -01 are not exhaustive, are illustrative.
- Use-cases in -01 focus on DDoS mitigation using dedicated mitigation devices. S/RTBH, flowspec, OpenFlow, etc. can also be used to leverage network infrastructure for DDoS mitigation.

DOTS WG   IETF 95

Changes from -01

- Some repetitive verbiage elided.
- Introductory verbiage added to provide context.
- Minor clarification of use-case archetypes.
- Sections renumbered.
- *Not* a major update.

DOTS WG

Changes for -02

- Consolidation with `draft-nishizuka-dots-inter-domain-usecases-01`.

- Major re-factoring of document!

- Focus on minimum viable capability (MVC) for DOTS Phase I, reproducing and supplementing current non-standard signaling mechanisms via standards-based method (e.g., DOTS); additional optional capabilities outlined in use-cases.

- Prosaic use-cases more accessible to non-specialists.

- Current -01 use-case archetypes simplified, de-duplicated, and described in an appendix.

- New use-cases will combine components, exchanges, and processes.

- Additional co-authors.

Themes of -02

- Produce a working model of what's currently possible, along with reasonable and desirable evolutionary innovation for DOTS Phase I.

- Explore and describe additional useful functionality which may be optional.

- Create a document that is easily understood by non-specialists.

- Broaden participation to ensure more viewpoints are represented.

- Capture all the above in a single document, which is more easily referenced than multiple documents.

- *Is* a major update!

DOTS WG

This Presentation – http://bit.ly/1N6u8za

IETF 95
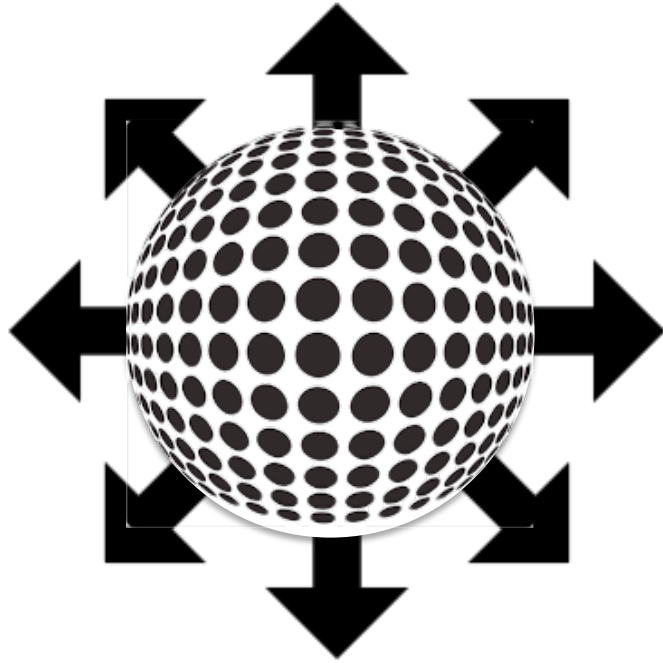
DDoS Open Threat Signaling (DOTS) Working Group

Thank You!

Roland Dobbins – Arbor Networks

Stefan Fouant – Corero Network Security

Daniel Migault – Ericsson

Robert Moskowitz – HTT Consulting

Nik Teague – Verisign

Liang 'Frank' Xia – Huawei