DDoS Open Threat Signaling BOF (DOTS)

IETF 92, Dallas, Texas

Russ Housley
Roman Danyliw

Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances.

The IETF's IPR Policy is set forth in **BCP 79**; please read it carefully.

The brief summary:

❖**By participating with the IETF, you agree to follow IETF processes.**

❖**If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.**

❖**You understand that meetings might be recorded, broadcast, and publicly archived.**

For further information, talk to a WG chair, ask an Area Director, or review the following:
BCP 9 (on the Internet Standards Process)
BCP 25 (on the Working Group processes)
BCP 78 (on the IETF Trust)
BCP 79 (on Intellectual Property Rights in the IETF)

Administrative Tasks

- Blue sheets
- Note takers
- Jabber scribe

Agenda

1. Logistics and introduction of BOF (chairs, 10 min)
2. draft-teague-open-threat-signaling-00 (Nik Teague, 20 min)
3. draft-fu-ipfix-network-security-00 (Ana Hedanping, 15 min)
4. Panel discussion on suitability (40 min)
   - (moderator) Nik Teague
   - Rich Groves
   - Vince Berk
   - David Larson
   - Andrew Mortensen
5. Further discussion (30 min)
6. Closing (chairs/AD, 5 min)

Description

- The purpose of DOTS is to enable any on premises DDoS mitigation device to communicate the current threat landscape, load and response data to a mitigation service provider in a standardized way.
- The on-premises device communicates threat and telemetry data.

- Non-WG forming BOF

Relationship to Other WG

- OPSAWG
  - Entails sending telemetry and configuring devices
- MILE
  - Entails exchanging threat information

Questions?

- Do we understand the problem space sufficiently?
- Does this problem need standardization? In the IETF?
- Who is willing to contribute to an IETF effort?
- How should this work be done in the IETF?