# DetNet Security Considerations Draft Update

| | |
|---|---|
| Tal Mizrahi | Marvell |
| Ethan Grossman | Dolby Laboratories |
| Andrew Hacker | MistIQ Technologies |
| Subir Das | Applied Communication Sciences |
| John Dowdell | Airbus |
| Henrik Austad | Cisco Systems |
| Kevin Stanton | Intel |
| Norman Finn | Huawei |

draft-ietf-detnet-security-01

IETF 101, London, March 2018

# DetNet Security Considerations Draft Update

- Current Status
  - Draft is still at 01, unchanged since last IETF 100
  - Draft is considered to adequately cover the general topic
  - Scope is limited to security considerations that are specific to DetNet, e.g. time sensitivity
  - Does not yet include security considerations specific to Data Plane protocols
- Future Plans
  - Add security considerations specific to Data Plane protocols, once these decisions are made
- Very Brief Draft Overview (2 slides)

# DetNet Security Considerations Draft Overview

- Security threats
  - Examples include Delay, Spoofing, Reconnaissance, etc.
- Impact of security threats
  - Components of Impact include Criticality, Financial, Health and Safety, etc.
- Mitigations
  - A toolset of measures that can be taken against threats, e.g. authentication, encryption, analytics
- Association of attacks to use case common themes
  - Narrowing down the problems of securing a DetNet, based on knowledge of the specific application
  - Difficult because there are so many use cases
  - Instead of “by use case”, we organize “by use case common theme” (DetNet Use Cases draft sec 11)
  - If that theme is important to your use case, you should pay attention to that section

# Associating Attacks with Use Case Common Themes

An example for the “Deterministic Flows” common theme (DetNet Use Cases draft 14, sec 11.6)

6.1.10. Deterministic Flows

Reserved bandwidth data flows (deterministic flows) must provide the allocated bandwidth, and must be isolated from each other.

A Spoofing or Inter-segment attack which adds packet traffic to a bandwidth-reserved stream could cause that stream to occupy more bandwidth than it is allocated, resulting in interference with other deterministic flows.

A Flow Modification or Spoofing or Header Manipulation or Control Packet Modification attack could cause packets from one flow to be directed to another flow, thus breaching isolation between the flows.