# DetNet Security Considerations


| | |
|---|---|
| Tal Mizrahi | Marvell |
| Ethan Grossman | Dolby Laboratories |
| Andrew Hacker | MistIQ Technologies |
| Subir Das | Applied Communication Sciences |
| John Dowdell | Airbus |



draft-sdt-detnet-security-00

IETF 98, Chicago, March 2017

# Draft Outline

- Background

- Security threats
- Impact of security threats
- Mitigations

To be added in later versions of the draft

- Collection of security-related statements

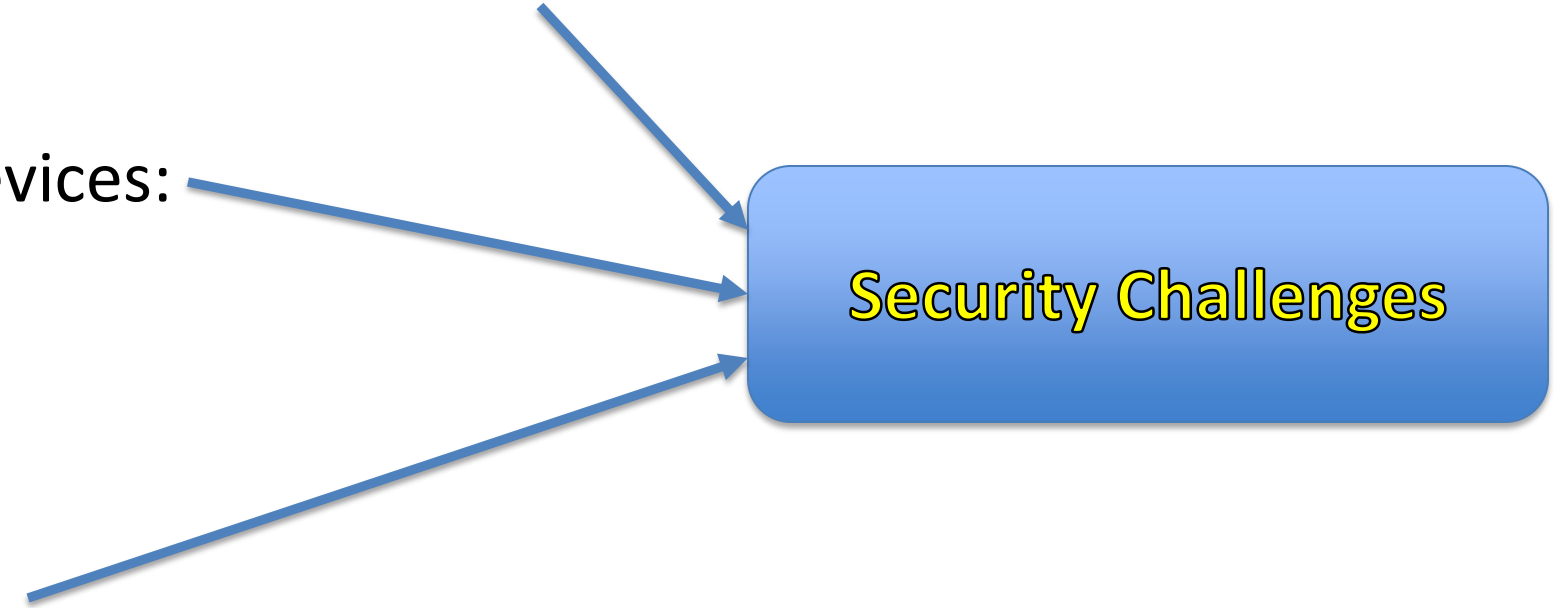
# Background

# Background

- The DetNet evolution:
  - Local area (isolated) networks ➔ wide area networks
- Control of physical devices:
  - Power grids
  - Industrial controls
  - Building controls
- Converged network:
  - Non-DetNet traffic
  - DetNet traffic
  - Control / signaling

# Background

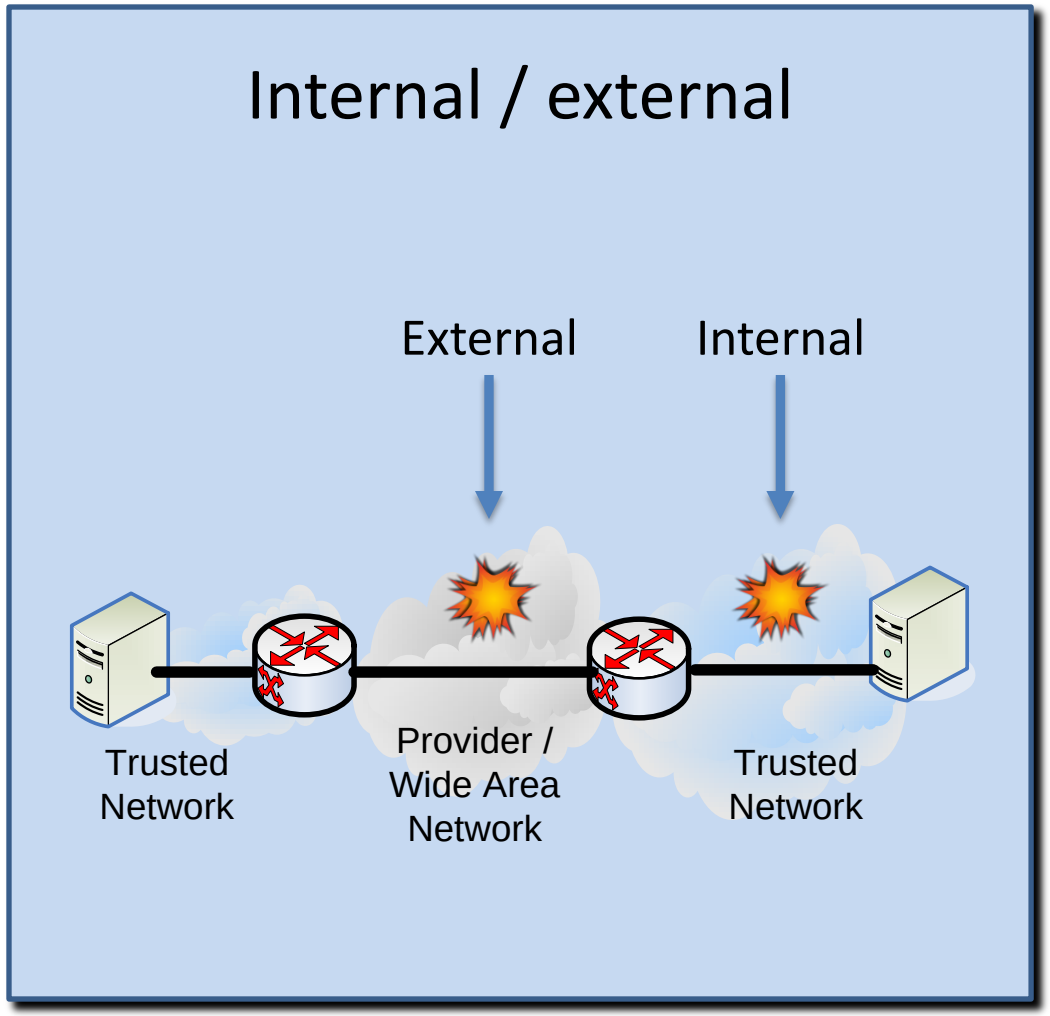
- The DetNet evolution:
  - Local area (isolated) networks ➔ wide area networks
- Control of physical devices:
  - Power grid
  - Industrial control
  - Building controls
- Converged network:
  - Non-DetNet traffic
  - DetNet traffic
  - Control / signaling

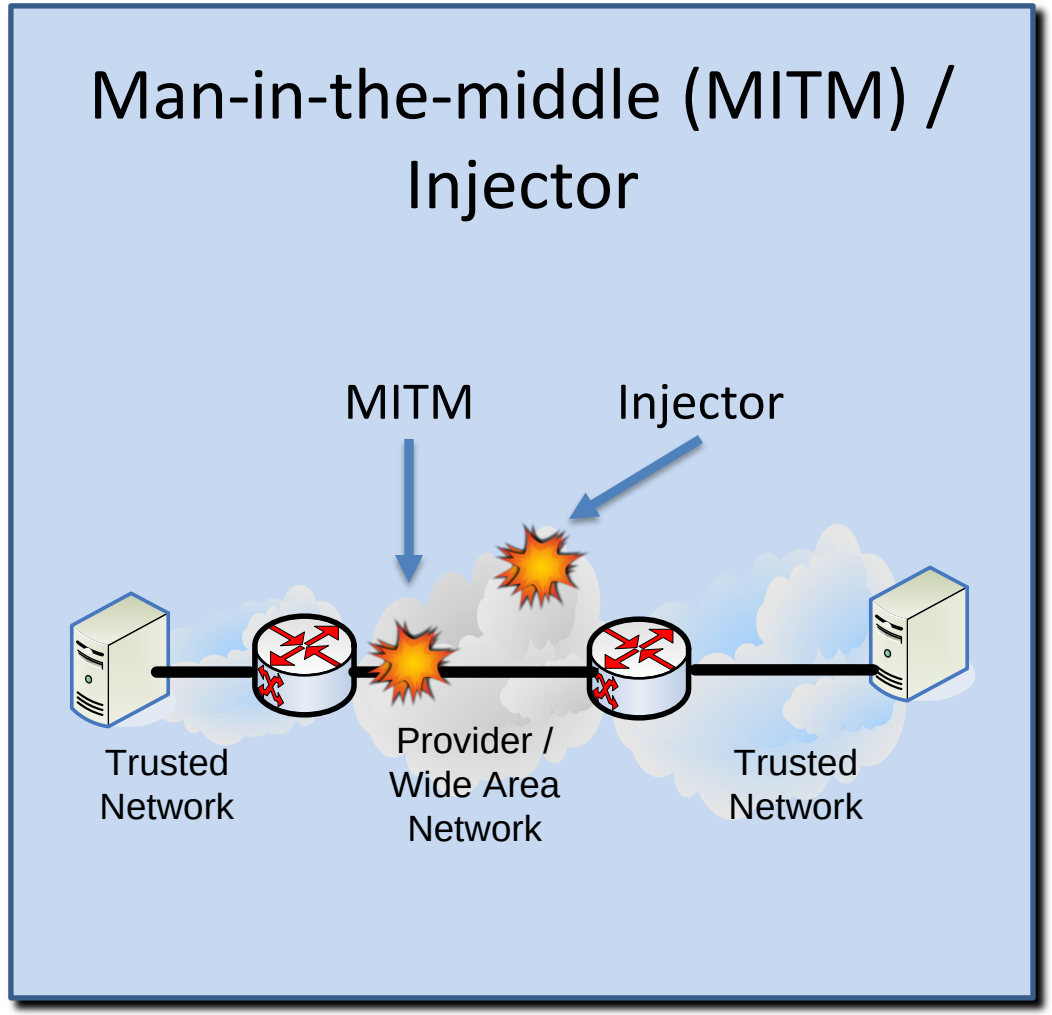


# Security Threats

# Attacker Types

[Based on RFC 7384]



# Threats

- **Delay attack**
  - Attacker maliciously delays DetNet data flow traffic.
- **DetNet flow modification and spoofing**
  - Attacker modifies the headers of en route DetNet packets, or spoofs DetNet packets ➔ manipulating the resource consumption.
- **Inter-segment attack**
  - Attacker injects traffic from one segment, affecting the performance of other segments.

# Threats (2)

- **Replication: Increased Attack Surface**
  - Multiple paths ➔ more points in the network that can potentially be attacked.
- **Replication-related Header Manipulation**
  - Attacker modifies replication header ➔ Forward both replicas / eliminate both replicas / flow hijacking.
- **Path Manipulation**
  - Attack control plane ➔ manipulate the paths being used.
- **Path Choice: Increased Attack Surface**
  - Attack control plane ➔ increase number of points that can potentially be attacked.

# Threats (3)

- **Control or Signaling Packet Modification**
  - Modify control / signaling packets ➔ manipulate path / resource allocation.
- **Control or Signaling Packet Injection**
  - Inject control / signaling packets ➔ manipulate path / resource allocation.
- **Reconnaissance**
  - Passive eavesdropping ➔ gather information about DetNet flows, bandwidths, schedules.
- **Attacks on Time Sync Mechanisms**
  - Attack time sync mechanism ➔ disrupt DetNet flow forwarding.

# Summary of Threats

| Attack | Attacker Type | | | |
|---|---|---|---|---|
| | Internal MITM | Internal Inj. | External MITM | External Inj. |
| Delay attack | + | | + | |
| DetNet Flow Modification or Spoofing | + | + | | |
| Inter-segment Attack | + | + | | |
| Replication: Increased Attack Surface | + | + | + | + |
| Replication-related Header Manipulation | + | | | |
| Path Manipulation | + | + | | |
| Path Choice: Increased Attack Surface | + | + | + | + |
| Control or Signaling Packet Modification | + | | | |
| Control or Signaling Packet Injection | | + | | |
| Reconnaissance | + | | + | |
| Attacks on Time Sync Mechanisms | + | + | + | + |

# Next Steps

- March 2017 – draft 00

- Next steps:
  - Working group feedback
  - Add content (security impact, mitigations
  - Working group adoption

# Thanks!

# References


[1] T. Mizrahi, E. Grossman, A. Hacker, S. Das, J. Dowdell, “Deterministic Networking (DetNet) Security Considerations”, draft-sdt-detnet-security-00 (work in progress), 2017.

[2] E. Grossman, C. Gunther, P. Thubert, P. Wetterwald, J. Raymond, J. Korhonen, Y. Kaneko, S. Das, Y. Zha, B. Varga, J. Farkas, F. Goetz, J. Schmitt, X. Vilajosana, T. Mahmoodi, S. Spirou, and P. Vizarreta, "Deterministic Networking Use Cases", draft-ietf-detnet-use-cases-11 (work in progress), 2016.

[3] T. Mizrahi, "Security Requirements of Time Protocols in Packet Switched Networks", RFC 7384, 2014.