Security Considerations in DetNet / TSN

Tal Mizrahi	Huawei Network.IO Innovation Lab
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

IEEE 802.1 / IETF Joint Workshop
Bangkok, November 2018

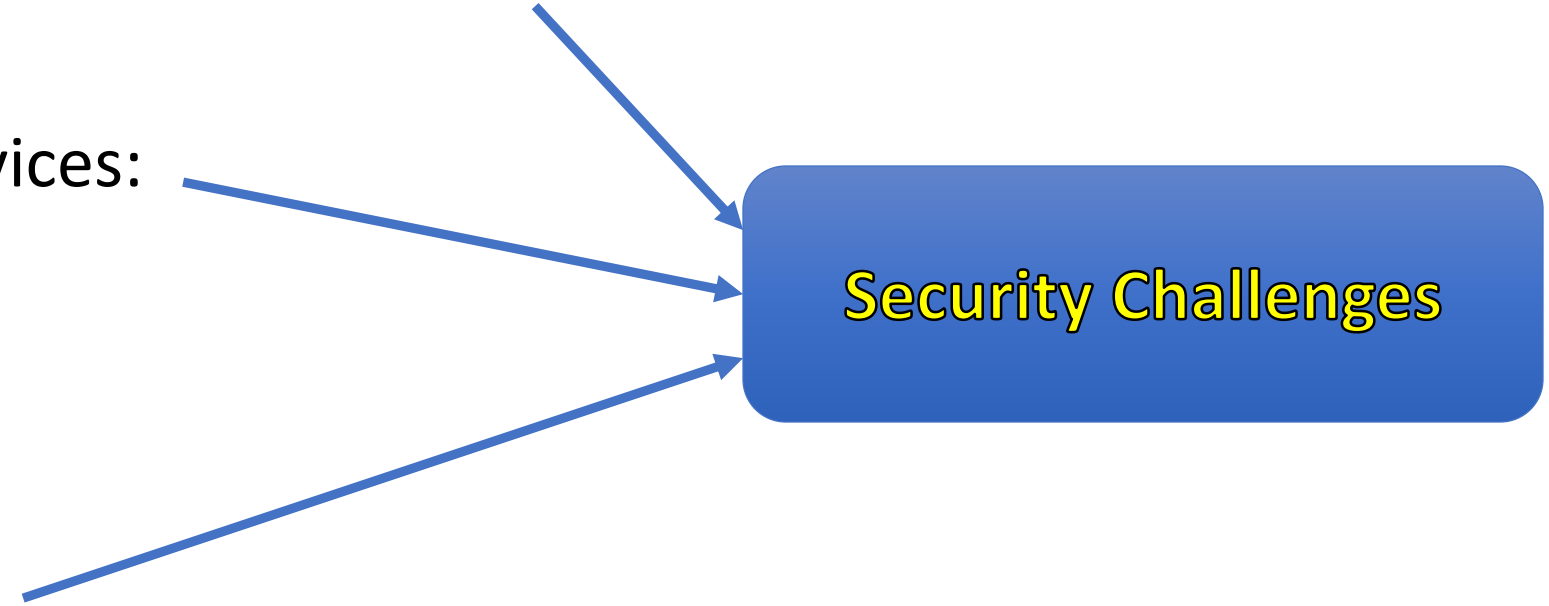
Background

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 grids
  - Industrial controls
  - Building controls
- Converged network:
  - Non-DetNet traffic
  - DetNet traffic
  - Control / signaling



DetNet Security Considerations IETF Draft

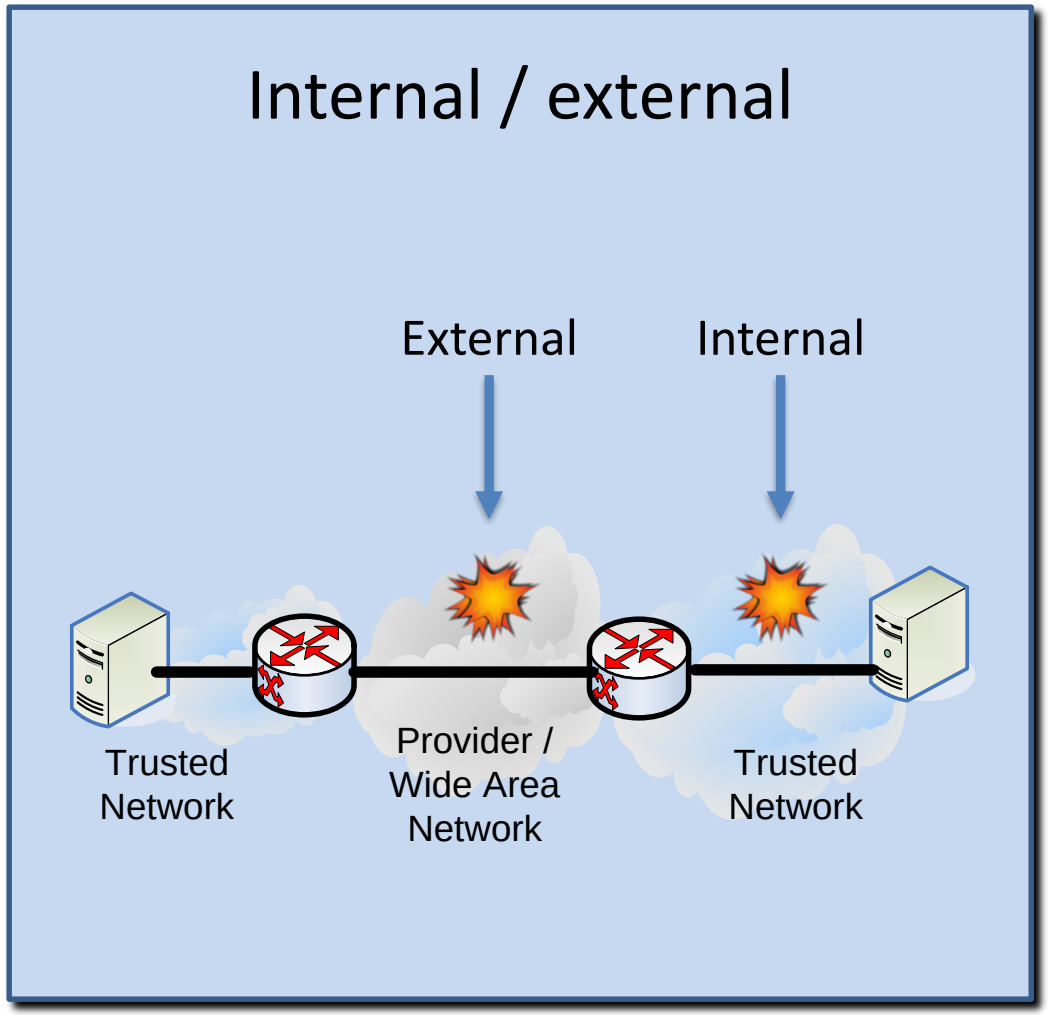
draft-ietf-detnet-security-03

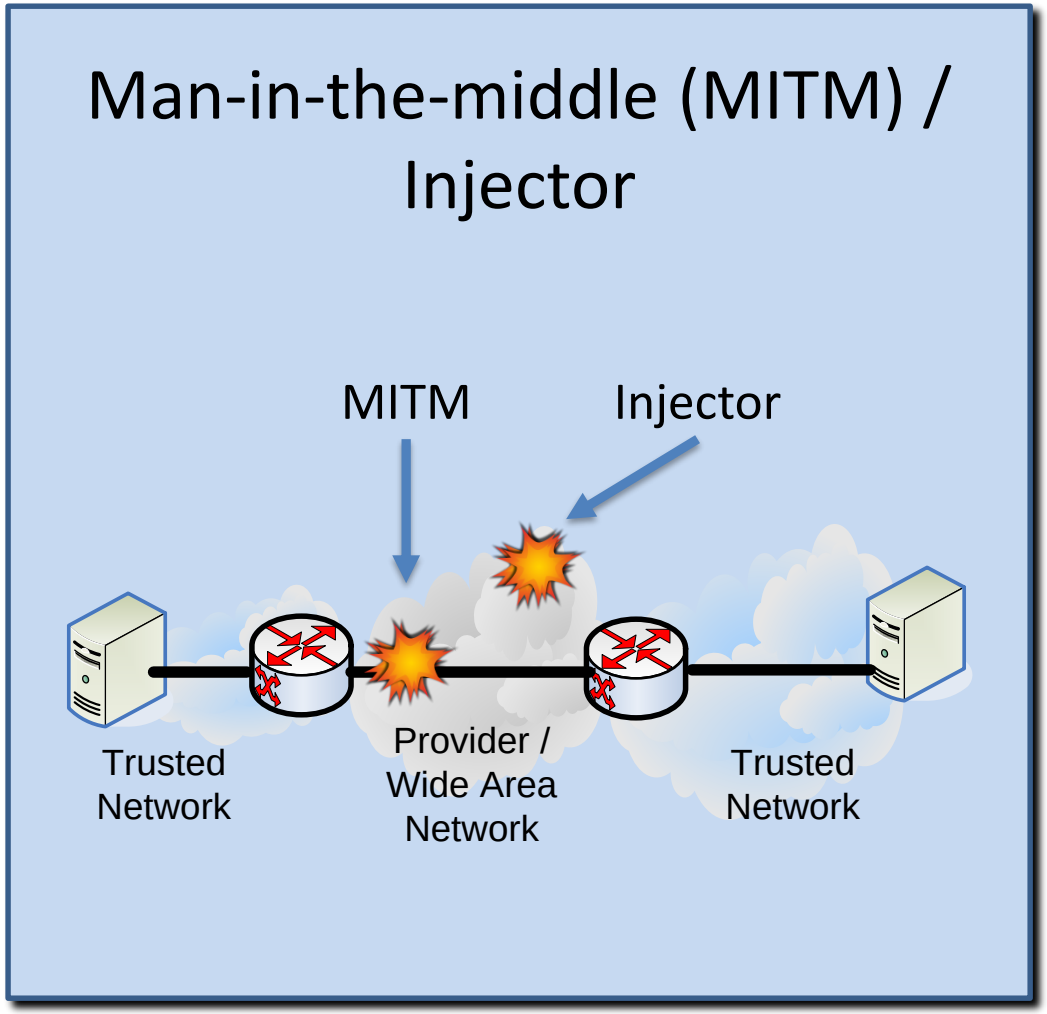
Draft Outline

- Security threats
- Impact of security threats
- Mitigations
- Association of attacks to use cases

Attacker Types

[Based on RFC 7384]





Threats

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	+	+	+	+

Impact

Impact

	Control Plane	Data Plane

Impact of Recon and Delay Attacks

	Control Plane	Data Plane
Reconnaissance	• Monitor changes in the network • Monitor flows and their IDs • Identify controllers	• Identify active targets • Determine type of targets based on observed stream parameters. • Find opportune moment to conduct final attack

Impact of Recon and Delay Attacks

	Control Plane	Data Plane
Reconnaissance	• Monitor changes in the network • Monitor flows and their IDs • Identify controllers	• Identify active targets • Determine type of targets based on observed stream parameters. • Find opportune moment to conduct final attack
Delay attacks	• Resource exhaustion (removing old links delayed) • Reduces QoS (creating new links delayed) • Denial of Service (due to exhaustion, not enough to form new link) • Loss of privacy (data sent to old target)	• Increased buffering in bridges • Elimination nodes consume more resources • Skew path metrics • Outage (single path)

Impact of Spoofing and Modification Attacks

	Control Plane	Data Plane
Modification / spoofing	• Create/Remove/Modify streams • Modify network paths	• Skew path metrics • Consume resources • Disrupt links • Affect voting at elimination bridges • Crash application

Mitigations

Mitigations

Mitigation Method	Relevant Attack(s)
• Path redundancy	• Man-in-the-middle attacks

Mitigations

Mitigation Method	Relevant Attack(s)
• Path redundancy • Integrity protection • DetNet node authentication • Encryption	• Man-in-the-middle attacks • Modification/tampering • Spoofing • Recon

Mitigations

Mitigation Method	Relevant Attack(s)
• Path redundancy	• Man-in-the-middle attacks
• Integrity protection	• Modification/tampering
• DetNet node authentication	• Spoofing
• Encryption	• Recon
• Control message protection	• Control plane attacks
• Performance analytics	• Resource exhaustion attacks

Association of Attacks to Use Case Themes

Association of Attacks to Use Cases

- A set of use case themes
- For each theme: a discussion about specific security considerations

  - Network Layer - AVB/TSN Ethernet
  - Central Administration
  - Hot Swap
  - Data Flow Information Models
  - L2 and L3 Integration
  - End-to-End Delivery
  - Proprietary Deterministic Ethernet Networks
  - Replacement for Proprietary Fieldbuses
  - Deterministic vs Best-Effort Traffic
  - Deterministic Flows
  - Unused Reserved Bandwidth
  - Interoperability
  - Cost Reductions
  - Insufficiently Secure Devices
  - DetNet Network Size
  - Multiple Hops
  - Level of Service
  - Bounded Latency
  - Low Latency
  - Symmetrical Path Delays
  - Reliability and Availability
  - Redundant Paths
  - Security Measures

Mapping Attacks to Use Case Themes

Theme	Attack									
	1	2	3	4	5	6	7	8	9	10	11
Network Layer - AVB/TSN Eth.	+	+	+	+	+	+	+	+	+	+	+
Central Administration						+	+	+	+	+	+
Hot Swap		+	+								+
Data Flow Information Models											
L2 and L3 Integration					+	+					

...

Summary

Applicability to IEEE 802.1

- Attacks and mitigation are mostly relevant for IEEE 802.1
- Impacts and use cases are partly relevant to IEEE 802.1
- This document is a useful reference for IEEE 802.1
- This document does not define security solutions

Status of this Work

- Early 2017 – work started
- Early 2018 – taking a timeout until DetNet data plane solutions will be stable
- Solicit review from a wide audience