Security Considerations for Deterministic Networking

Draft Update

IETF 106 Singapore 2019

Ethan Grossman
Senior Software Engineering Manager
Dolby Laboratories, San Francisco

DetNet Security Considerations Scope

- Draft: https://datatracker.ietf.org/doc/draft-ietf-detnet-security/
- Scope
  - A reference/toolkit for those who have not built time-sensitive networks before
  - Exclusively addresses time-related threats
  - Other DetNet drafts address draft-topic-specific considerations then refer here (as informational)

DetNet Security Considerations Status

- Status
  - Data plane technology-independent sections
    - Mature, but still some editing and a few small sections to fill in
  - IP- and MPLS-specific sections
    - No unique threats identified – discussion on this later
  - TSN-specific section
    - Not started
  - Security-related statements from Use Cases
    - Update? Delete?

DetNet Security Considerations Discussion and Next Steps

- Discussion
  - Data plane technology-specific threats - are we missing something?
    - There will be more data planes – so maybe that info should not be in here?
  - Security-related statements from Use Cases – Update? Delete?
  - SecDir review – before or after WG LC?

- Next Steps
  - Finish edits, add any new material
  - Working Group Last Call

DetNet Security Considerations

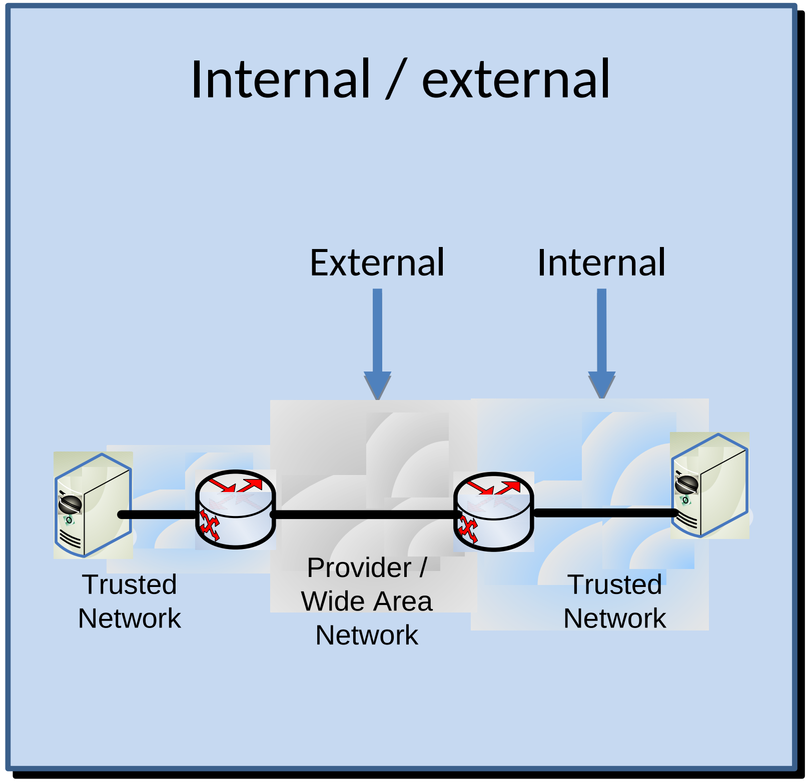
- The End
- Remaining slides are optional, a brief overview of the draft

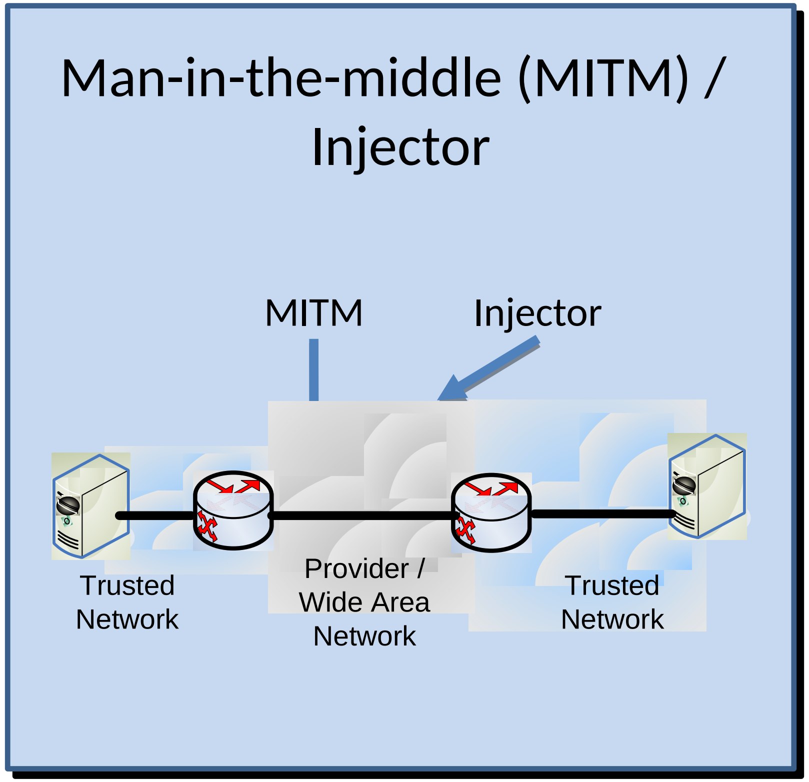
DetNet Security Considerations

- Security Considerations draft as ”toolkit”
  - Attackers
  - Attacks
  - Impacts
  - Mitigations
  - Table of attacks to impacts and mitigation
  - Table of use cases to relevant attacks

Attacker Types

[Based on RFC 7384]




Man-in-the-middle (MITM) / Injector
MITM
Injector
Trusted Network
Provider / Wide Area Network
Trusted Network

Attacks

Attack	Attacker Type			
	Internal		External	
	MITM	Inj.	MITM	Inj.
Delay attack	+		+	
Replication: Increased Attack Surface	+	+	+	+
Path Manipulation	+	+		
Packet Modification / Injection	+	+		
Reconnaissance	+		+	
Attacks on Time Sync Mechanisms	+	+	+	+

(and others)

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)

Mitigations

Mitigation Method

- Path redundancy
- Integrity protection
- DetNet node authentication
- Encryption
- Control message protection
- Performance analytics

Relevant Attack(s)

- Man-in-the-middle attacks
- Modification/tampering
- Spoofing
- Recon
- Control plane attacks
- Resource exhaustion attacks

Mapping Attacks to Impacts / Mitigations

Attack	Impact	Mitigations
Delay Attack	-Non-deterministic delay -Data disruption -Increased resource consumption	-Path redundancy -Performance analytics
DetNet Flow Modification or Spoofing	-Increased resource consumption -Data disruption	-Path redundancy -Integrity protection -DetNet Node authentication

(etc)

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					+	+					

...