DetNet Security Considerations

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-sdt-detnet-security-01

IETF 99, Prague, July 2017

Draft Outline

- Background

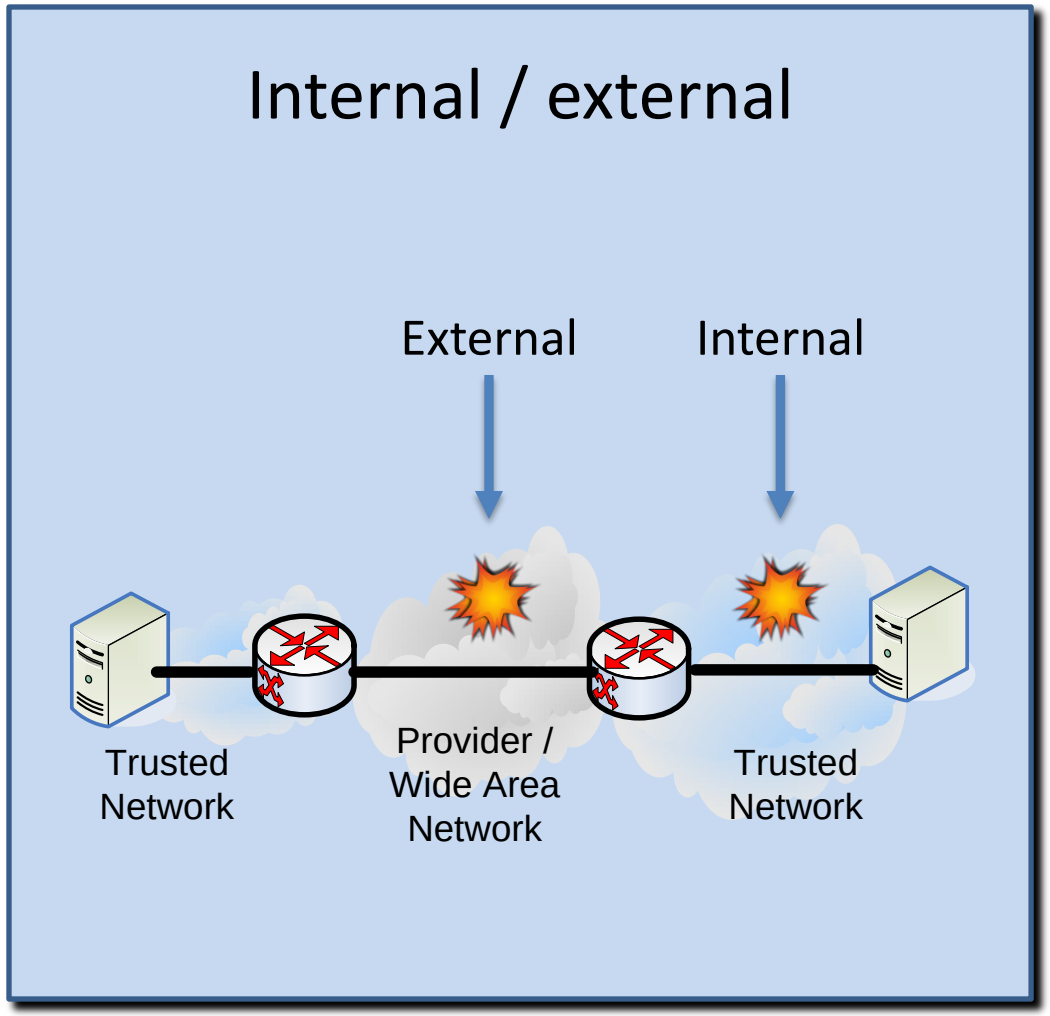
- Security threats
- Impact of security threats
- Mitigations
- Association of attacks to use cases

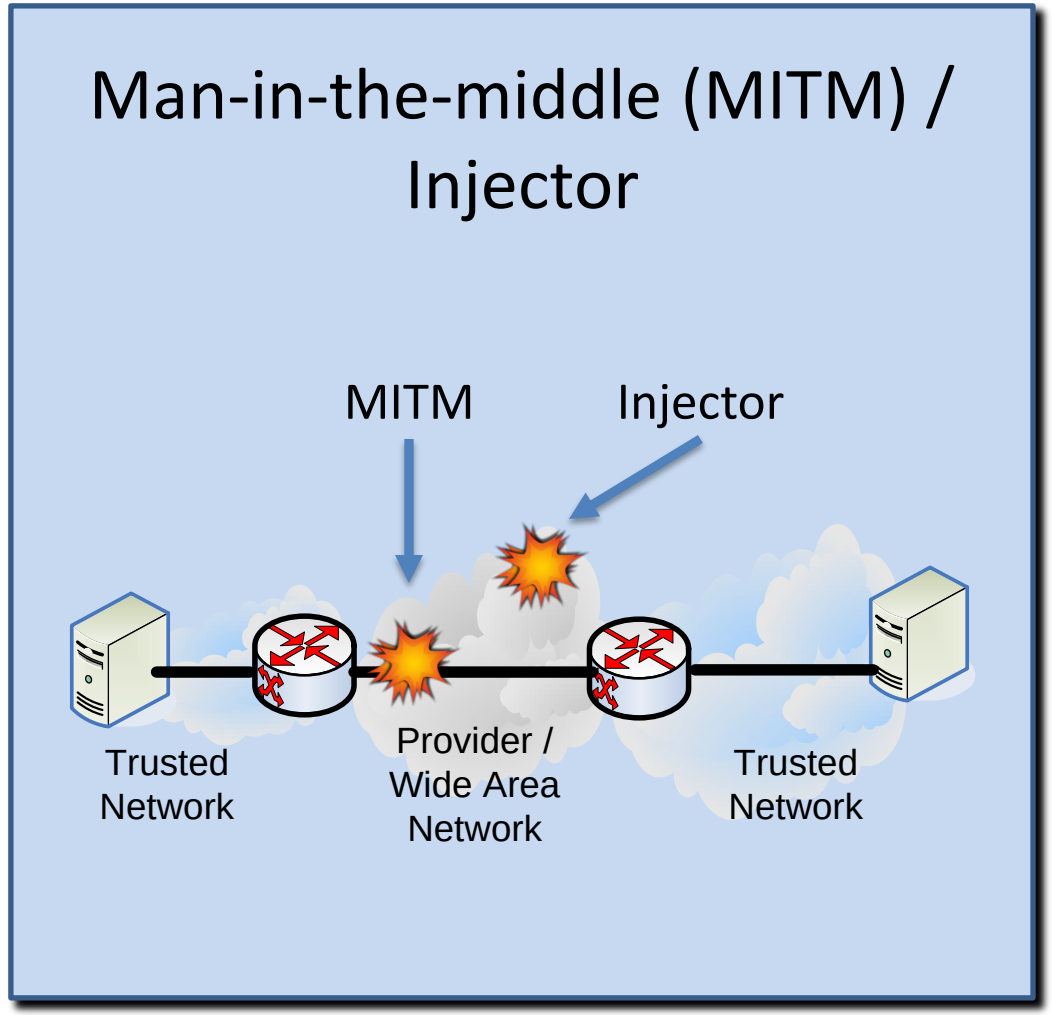
Added in version 01

Security Threats

Attacker Types

[Based on RFC 7384]





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 • Integrity protection • DetNet node authentication • Encryption • Control message protection • Performance analytics	• 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
Inter-Segment Attack	-Increased resource consumption -Data disruption	-Path redundancy -Performance analytics
Replication: Increased attack surface	-All impacts of other attacks	-Integrity protection -DetNet Node authentication
Replication-related Header Manipulation	-Non-deterministic delay -Data disruption	-Integrity protection -DetNet Node authentication
Path Manipulation	-Enabler for other attacks	-Control message protection
Path Choice: Increased Attack Surface	-All impacts of other attacks	-Control message protection
Control or Signaling Packet Modification	-Increased resource consumption -Non-deterministic delay -Data disruption	-Control message protection
Control or Signaling Packet Injection	-Increased resource consumption -Non-deterministic delay -Data disruption	-Control message protection
Reconnaissance	-Enabler for other attacks	-Encryption
Attacks on Time Sync Mechanisms	-Non-deterministic delay -Increased resource consumption -Data disruption	-Path redundancy -Control message protection -Performance analytics

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

Next Steps

- March 2017 – draft 00
  - Good feedback
  - Wide support
- July 2017 – draft 01
  - Significant progress
- Next steps:
  - Call for working group adoption

Thanks!

References

[1] T. Mizrahi, E. Grossman, A. Hacker, S. Das, J. Dowdell, H. Austad, K. Stanton, N. Finn, “Deterministic Networking (DetNet) Security Considerations”, draft-sdt-detnet-security-01 (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-12 (work in progress), 2017.

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