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-ietf-detnet-security-01

IETF 100, Singapore, November 2017

Draft Outline

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

History of this Draft

- March 2017 – draft 00
  - Presented in IETF 98
- July 2017 – draft 01 (major revision)
  - Presented in IETF 99

- September 2017 – accepted as a WG doc 00
- October 2017 – draft 01

Main Changes vs. Previous Version

- Impact section
  - Clarifications
  - Revised the Impact by Use Case mapping
- Association of Attacks to Use Cases
  - Major revision

Impact by Use Case Industry

	Pro A	Util	Bldg	Wire-less	Cell	M2M Data	M2M Ctrl	Mining	Block Chain	Network Slicing
Criticality	Med	Hi	Low	Med	Med	Med	Med	Hi	Med	Hi
Effects										
Financial	Med	Hi	Med	Med	Low	Med	Med	Hi	Hi	Hi
Health/Safety	Med	Hi	Hi	Med	Med	Med	Med	Hi	Low	Med
People WB	Med	Hi	Hi	Low	Hi	Low	Low	Hi	Low	Med
Effect 1 org	Hi	Hi	Med	Hi	Med	Med	Med	Hi	Hi	Hi
Effect >1 org	Med	Hi	Low	Med	Med	Med	Med	Hi	Low	Hi
Recovery										
Recov Time Obj	Med	Hi	Med	Hi	Hi	Hi	Hi	Hi	Low	Hi
Recov Point Obj	Med	Hi	Low	Med	Low	Hi	Hi	Hi	Low	Hi
DetNet Dependence										
Time Dependency	Hi	Hi	Low	Hi	Med	Low	Hi	Hi	Low	Hi
Latency/Jitter	Hi	Hi	Med	Med	Low	Low	Hi	Hi	Low	Hi
Data Integrity	Hi	Hi	Med	Hi	Low	Hi	Low	Hi	Hi	Hi
Src Node Integ	Hi	Hi	Med	Hi	Med	Hi	Hi	Hi	Hi	Hi
Availability	Hi	Hi	Med	Hi	Low	Hi	Hi	Hi	Hi	Hi

Association of Attacks to Use Cases

- Before:

6.1.1. Network Layer - AVB/TSN Ethernet

Presumably it will be possible to run DetNet over other underlying network layers besides Ethernet, but Ethernet is explicitly supported. Is the attack specific to the Ethernet AVB/TSN protocols? Does the threat affect only Ethernet, or any underlying network layer?

- After:

6.1.1. Network Layer - AVB/TSN Ethernet

DetNet is expected to run over various transmission mediums, with Ethernet being explicitly supported. Attacks such as Delay or Reconnaissance might be implemented differently on a different transmission medium, however the impact on the DetNet as a whole would be essentially the same. We thus conclude that all attacks and impacts that would be applicable to DetNet over Ethernet (i.e. all those named in this draft) would also be applicable to DetNet over other transmission mediums.

With respect to mitigations, some methods are specific to the Ethernet medium, for example time-aware scheduling using 802.1Qbv can protect against excessive use of bandwidth at the ingress - for other mediums, other mitigations would have to be implemented to provide analogous protection.

Next Steps

- Reconsider the ‘design team’ format
- Solicit review from a wider audience
- Consider security aspects of the emerging data plane solution

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-ietf-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, D. Huang, X. Geng, D. Dujovne, M. Seewald, "Deterministic Networking Use Cases", draft-ietf-detnet-use-cases-13 (work in progress), 2017.

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