Internet Engineering Task Force   T. Mizrahi
Internet-Draft   HUAWEI
Intended status: Informational   E. Grossman, Ed.
Expires: August 6, 2020   DOLBY
                                                             A. Hacker
                                                                MISTIQ
                                                                S. Das
                                           Applied Communication Sciences
                                                            J. Dowdell
                                              Airbus Defence and Space
                                                             H. Austad
                                                        SINTEF Digital
                                                               N. Finn
                                                                HUAWEI
                                                      February 3, 2020

                Deterministic Networking (DetNet) Security Considerations
                        draft-ietf-detnet-security-08

Abstract

   A deterministic network is one that can carry data flows for real-
   time applications with extremely low data loss rates and bounded
   latency. Deterministic networks have been successfully deployed in
   real-time operational technology (OT) applications for some years.
   However, such networks are typically isolated from external access,
   and thus the security threat from external attackers is low. IETF
   Deterministic Networking (DetNet) specifies a set of technologies
   that enable creation of deterministic networks on IP-based networks
   of potentially wide area (on the scale of a corporate network)
   potentially bringing the OT network into contact with Information
   Technology (IT) traffic and security threats that lie outside of a
   tightly controlled and bounded area (such as the internals of an
   aircraft). These DetNet technologies have not previously been
   deployed together on a wide area IP-based network, and thus can
   present security considerations that may be new to IP-based wide area
   network designers. This document, intended for use by DetNet network
   designers, provides insight into these security considerations.

working documents as Internet-Drafts. The list of current Internet-
Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months
and may be updated, replaced, or obsoleted by other documents at any
time. It is inappropriate to use Internet-Drafts as reference
material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 6, 2020.

Copyright Notice

Table of Contents

1. Introduction

   Security is of particularly high importance in DetNet networks
   because many of the use cases which are enabled by DetNet [RFC8578]
   include control of physical devices (power grid components,
   industrial controls, building controls) which can have high
   operational costs for failure, and present potentially attractive
   targets for cyber-attackers.

   This situation is even more acute given that one of the goals of
   DetNet is to provide a "converged network", i.e. one that includes
   both IT traffic and OT traffic, thus exposing potentially sensitive
   OT devices to attack in ways that were not previously common (usually
   because they were under a separate control system or otherwise
   isolated from the IT network, for example [ARINC664P7]). Security
   considerations for OT networks are not a new area, and there are many
   OT networks today that are connected to wide area networks or the
   Internet; this document focuses on the issues that are specific to
   the DetNet technologies and use cases.

   Given the above considerations, securing a DetNet starts with a
   scrupulously well-designed and well-managed engineered network
   following industry best practices for security at both the data plane
   and control plane; this is the assumed starting point for the
   considerations discussed herein. In this context we view the network
   design and managment aspects of network security as being primarily
   concerned with denial-of service prevention by ensuring that DetNet
   traffic goes where it's supposed to and that an external attacker

can't inject traffic that disrupts the DetNet's delivery timing
assurance. The time-specific aspects of DetNet security presented
here take up where the design and management aspects leave off.

The security requirements for any given DetNet network are
necessarily specific to the use cases handled by that network. Thus
the reader is assumed to be familiar with the specific security
requirements of their use cases, for example those outlined in the
DetNet Use Cases [RFC8578] and the Security Considerations sections
of the DetNet documents applicable to the network technologies in
use, for example [I-D.ietf-detnet-ip]).

The DetNet technologies include ways to:

o Reserve data plane resources for DetNet flows in some or all of
   the intermediate nodes (e.g. bridges or routers) along the path of
   the flow

o Provide explicit routes for DetNet flows that do not rapidly
   change with the network topology

o Distribute data from DetNet flow packets over time and/or space to
   ensure delivery of each packet's data' in spite of the loss of a
   path

This document includes sections on threat modeling and analysis,
threat impact and mitigation, and the association of attacks with use
cases based on the Use Case Common Themes section of the DetNet Use
Cases [RFC8578].

2. Abbreviations

IT   Information technology (the application of computers to
store, study, retrieve, transmit, and manipulate data or information,
often in the context of a business or other enterprise - Wikipedia).

OT   Operational Technology (the hardware and software
dedicated to detecting or causing changes in physical processes
through direct monitoring and/or control of physical devices such as
valves, pumps, etc. - Wikipedia)

MITM   Man in the Middle

SN   Sequence Number

STRIDE   Addresses risk and severity associated with threat
categories: Spoofing identity, Tampering with data, Repudiation,
Information disclosure, Denial of service, Elevation of privilege.

   DREAD   Compares and prioritizes risk represented by these threat
   categories: Damage potential, Reproducibility, Exploitability, how
   many Affected users, Discoverability.

   PTP   Precision Time Protocol [IEEE1588]

3. Security Threats

   This section presents a threat model, and analyzes the possible
   threats in a DetNet-enabled network. The threats considered in this
   section are independent of any specific technologies used to
   implement the DetNet; Section 7) considers attacks that are
   associated with the DetNet technologies encompassed by
   [I-D.ietf-detnet-data-plane-framework].

   We distinguish control plane threats from data plane threats. The
   attack surface may be the same, but the types of attacks as well as
   the motivation behind them, are different. For example, a delay
   attack is more relevant to data plane than to control plane. There
   is also a difference in terms of security solutions: the way you
   secure the data plane is often different than the way you secure the
   control plane.

3.1. Threat Model

   The threat model used in this memo is based on the threat model of
   Section 3.1 of [RFC7384]. This model classifies attackers based on
   two criteria:

   o Internal vs. external: internal attackers either have access to a
      trusted segment of the network or possess the encryption or
      authentication keys. External attackers, on the other hand, do
      not have the keys and have access only to the encrypted or
      authenticated traffic.

   o Man in the Middle (MITM) vs. packet injector: MITM attackers are
      located in a position that allows interception and modification of
      in-flight protocol packets, whereas a traffic injector can only
      attack by generating protocol packets.

   Care has also been taken to adhere to Section 5 of [RFC3552], both
   with respect to which attacks are considered out-of-scope for this
   document, but also which are considered to be the most common threats
   (explored further in Section 3.2. Most of the direct threats to
   DetNet are Active attacks, but it is highly suggested that DetNet
   application developers take appropriate measures to protect the
   content of the streams from passive attacks.

DetNet-Service, one of the service scenarios described in
[I-D.varga-detnet-service-model], is the case where a service
connects DetNet networking islands, i.e. two or more otherwise
independent DetNet network domains are connected via a link that is
not intrinsically part of either network. This implies that there
could be DetNet traffic flowing over a non-DetNet link, which may
provide an attacker with an advantageous opportunity to tamper with
DetNet traffic. The security properties of non-DetNet links are
outside of the scope of DetNet Security, but it should be noted that
use of non-DetNet services to interconnect DetNet networks merits
security analysis to ensure the integrity of the DetNet networks
involved.

3.2. Threat Analysis

3.2.1. Delay

3.2.1.1. Delay Attack

An attacker can maliciously delay DetNet data flow traffic. By
delaying the traffic, the attacker can compromise the service of
applications that are sensitive to high delays or to high delay
variation. The delay may be constant or modulated.

3.2.2. DetNet Flow Modification or Spoofing

An attacker can modify some header fields of en route packets in a
way that causes the DetNet flow identification mechanisms to
misclassify the flow. Alternatively, the attacker can inject traffic
that is tailored to appear as if it belongs to a legitimate DetNet
flow. The potential consequence is that the DetNet flow resource
allocation cannot guarantee the performance that is expected when the
flow identification works correctly.

3.2.3. Resource Segmentation or Slicing

3.2.3.1. Inter-segment Attack

An attacker can inject traffic, consuming network device resources,
thereby affecting DetNet flows. This can be performed using non-
DetNet traffic that affects DetNet traffic, or by using DetNet
traffic from one DetNet flow that affects traffic from different
DetNet flows.

[3.2.4](). Packet Replication and Elimination

[3.2.4.1](). Replication: Increased Attack Surface

Redundancy is intended to increase the robustness and survivability
of DetNet flows, and replication over multiple paths can potentially
mitigate an attack that is limited to a single path. However, the
fact that packets are replicated over multiple paths increases the
attack surface of the network, i.e., there are more points in the
network that may be subject to attacks.

[3.2.4.2](). Replication-related Header Manipulation

An attacker can manipulate the replication-related header fields
(R-TAG). This capability opens the door for various types of
attacks. For example:

o Forward both replicas - malicious change of a packet SN (Sequence
   Number) can cause both replicas of the packet to be forwarded.
   Note that this attack has a similar outcome to a replay attack.

o Eliminate both replicas - SN manipulation can be used to cause
   both replicas to be eliminated. In this case an attacker that has
   access to a single path can cause packets from other paths to be
   dropped, thus compromising some of the advantage of path
   redundancy.

o Flow hijacking - an attacker can hijack a DetNet flow with access
   to a single path by systematically replacing the SNs on the given
   path with higher SN values. For example, an attacker can replace
   every SN value S with a higher value S+C, where C is a constant
   integer. Thus, the attacker creates a false illusion that the
   attacked path has the lowest delay, causing all packets from other
   paths to be eliminated. Once the flow is hijacked the attacker
   can either replace en route packets with malicious packets, or
   simply injecting errors, causing the packets to be dropped at
   their destination.

[3.2.5](). Path Choice

[3.2.5.1](). Path Manipulation

An attacker can maliciously change, add, or remove a path, thereby
affecting the corresponding DetNet flows that use the path.

[3.2.5.2](#). Path Choice: Increased Attack Surface

One of the possible consequences of a path manipulation attack is an increased attack surface. Thus, when the attack described in the previous subsection is implemented, it may increase the potential of other attacks to be performed.

[3.2.6](#). Control Plane

[3.2.6.1](#). Control or Signaling Packet Modification

An attacker can maliciously modify en route control packets in order to disrupt or manipulate the DetNet path/resource allocation.

[3.2.6.2](#). Control or Signaling Packet Injection

An attacker can maliciously inject control packets in order to disrupt or manipulate the DetNet path/resource allocation.

[3.2.7](#). Scheduling or Shaping

[3.2.7.1](#). Reconnaissance

A passive eavesdropper can identify DetNet flows and then gather information about en route DetNet flows, e.g., the number of DetNet flows, their bandwidths, their schedules, or other temporal properties. The gathered information can later be used to invoke other attacks on some or all of the flows.

Note that in some cases DetNet flows may be identified based on an explicit DetNet header, but in some cases the flow identification may be based on fields from the L3/L4 headers. If L3/L4 headers are involved, for purposes of this document we assume they are encrypted and/or integrity-protected from external attackers.

[3.2.8](#). Time Synchronization Mechanisms

An attacker can use any of the attacks described in [[RFC7384](#)] to attack the synchronization protocol, thus affecting the DetNet service.

[3.3](#). Threat Summary

A summary of the attacks that were discussed in this section is presented in Figure 1. For each attack, the table specifies the type of attackers that may invoke the attack. In the context of this summary, the distinction between internal and external attacks is under the assumption that a corresponding security mechanism is being

used, and that the corresponding network equipment takes part in this
mechanism.

```
+--------------------------------------+----+----+----+----+
| Attack                               |    Attacker Type  |
|                                      +---------+---------+
|                                      |Internal |External |
|                                      |MITM|Inj.|MITM|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       | +  | +  | +  | +  |
+--------------------------------------+----+----+----+----+
```

Figure 1: Threat Analysis Summary

4. Security Threat Impacts

This section describes and rates the impact of the attacks described
in Section 3. In this section, the impacts as described assume that
the associated mitigation is not present or has failed. Mitigations
are discussed in Section 5.

In computer security, the impact (or consequence) of an incident can
be measured in loss of confidentiality, integrity or availability of
information. In the case of time sensitive networks, the impact of a
network exploit can also include failure or malfunction of mechanical
and/or other OT systems.

DetNet raises these stakes significantly for OT applications,
particularly those which may have been designed to run in an OT-only
environment and thus may not have been designed for security in an IT
environment with its associated devices, services and protocols.

The severity of various components of the impact of a successful
vulnerability exploit to use cases by industry is available in more
detail in [RFC8578]. Each of the use cases in the DetNet Use Cases
is represented in the table below, including Pro Audio, Electrical
Utilities, Industrial M2M (split into two areas, M2M Data Gathering
and M2M Control Loop), and others.

Components of Impact (left column) include Criticality of Failure,
Effects of Failure, Recovery, and DetNet Functional Dependence.
Criticality of failure summarizes the seriousness of the impact. The
impact of a resulting failure can affect many different metrics that
vary greatly in scope and severity. In order to reduce the number of
variables, only the following were included: Financial, Health and
Safety, People well being (People WB), Affect on a single
organization, and affect on multiple organizations. Recovery
outlines how long it would take for an affected use case to get back
to its pre-failure state (Recovery time objective, RTO), and how much
of the original service would be lost in between the time of service
failure and recovery to original state (Recovery Point Objective,
RPO). DetNet dependence maps how much the following DetNet service
objectives contribute to impact of failure: Time dependency, data
integrity, source node integrity, availability, latency/jitter.

The scale of the Impact mappings is low, medium, and high. In some
use cases there may be a multitude of specific applications in which
DetNet is used. For simplicity this section attempts to average the
varied impacts of different applications. This section does not
address the overall risk of a certain impact which would require the
likelihood of a failure happening.

In practice any such ratings will vary from case to case; the ratings
shown here are given as examples.

Table, Part One (of Two)

	Pro A	Util	Bldg	Wire-less	Cell	M2M Data	M2M Ctrl
Criticality	Med	Hi	Low	Med	Med	Med	Med
Effects							

```
| Financial       | Med   | Hi   | Med  | Med  | Low  | Med | Med |
+-----------------+-----------------------------------------+-----+
| Health/Safety   | Med   | Hi   | Hi   | Med  | Med  | Med | Med |
+-----------------+-----------------------------------------+-----+
| People WB       | Med   | Hi   | Hi   | Low  | Hi   | Low | Low |
+-----------------+-----------------------------------------+-----+
| Effect 1 org    | Hi    | Hi   | Med  | Hi   | Med  | Med | Med |
+-----------------+-----------------------------------------+-----+
| Effect >1 org   | Med   | Hi   | Low  | Med  | Med  | Med | Med |
+-----------------+-----------------------------------------+-----+
|Recovery
+-----------------+-----------------------------------------+-----+
| Recov Time Obj  | Med   | Hi   | Med  | Hi   | Hi   | Hi  | Hi  |
+-----------------+-----------------------------------------+-----+
| Recov Point Obj | Med   | Hi   | Low  | Med  | Low  | Hi  | Hi  |
+-----------------+-----------------------------------------+-----+
|DetNet Dependence
+-----------------+-----------------------------------------+-----+
| Time Dependency | Hi    | Hi   | Low  | Hi   | Med  | Low | Hi  |
+-----------------+-----------------------------------------+-----+
| Latency/Jitter  | Hi    | Hi   | Med  | Med  | Low  | Low | Hi  |
+-----------------+-----------------------------------------+-----+
| Data Integrity  | Hi    | Hi   | Med  | Hi   | Low  | Hi  | Low |
+-----------------+-----------------------------------------+-----+
| Src Node Integ  | Hi    | Hi   | Med  | Hi   | Med  | Hi  | Hi  |
+-----------------+-----------------------------------------+-----+
| Availability    | Hi    | Hi   | Med  | Hi   | Low  | Hi  | Hi  |
+-----------------+-----------------------------------------+-----+


Table, Part Two (of Two)
+-----------------+--------------------------+
|                 | Mining | Block | Network |
|                 |        | Chain | Slicing |
+-----------------+--------------------------+
| Criticality     | Hi     | Med   | Hi      |
+-----------------+--------------------------+
| Effects
+-----------------+--------------------------+
| Financial       | Hi     | Hi    | Hi      |
+-----------------+--------------------------+
| Health/Safety   | Hi     | Low   | Med     |
+-----------------+--------------------------+
| People WB       | Hi     | Low   | Med     |
+-----------------+--------------------------+
| Effect 1 org    | Hi     | Hi    | Hi      |
+-----------------+--------------------------+
| Effect >1 org   | Hi     | Low   | Hi      |
+-----------------+--------------------------+
```

```
|Recovery
+------------------+--------------------------+
|  Recov Time Obj  | Hi      | Low    | Hi      |
+------------------+--------------------------+
|  Recov Point Obj | Hi      | Low    | Hi      |
+------------------+--------------------------+
|DetNet Dependence
+------------------+--------------------------+
|  Time Dependency | Hi      | Low    | Hi      |
+------------------+--------------------------+
|  Latency/Jitter  | Hi      | Low    | Hi      |
+------------------+--------------------------+
|  Data Integrity  | Hi      | Hi     | Hi      |
+------------------+--------------------------+
|  Src Node Integ  | Hi      | Hi     | Hi      |
+------------------+--------------------------+
|  Availability    | Hi      | Hi     | Hi      |
+------------------+--------------------------+
```

Figure 2: Impact of Attacks by Use Case Industry

The rest of this section will cover impact of the different groups in
more detail.

4.1. Delay-Attacks

4.1.1. Data Plane Delay Attacks

Note that 'delay attack' also includes the possibility of a 'negative
delay' or early arrival of a packet, or possibly adversely changing
the timestamp value.

Delayed messages in a DetNet link can result in the same behavior as
dropped messages in ordinary networks as the services attached to the
stream has strict deterministic requirements.

For a single path scenario, disruption is a real possibility, whereas
in a multipath scenario, large delays or instabilities in one stream
can lead to increased buffer and CPU resources on the elimination
bridge.

A data-plane delay attack on a system controlling substantial moving
devices, for example in industrial automation, can cause physical
damage. For example, if the network promises a bounded latency of
2ms for a flow, yet the machine receives it with 5ms latency, the
machine's control loop can become unstable.

[4.1.2](#). Control Plane Delay Attacks

In and of itself, this is not directly a threat to the DetNet
service, but the effects of delaying control messages can have quite
adverse effects later.

o Delayed tear-down can lead to resource leakage, which in turn can
   result in failure to allocate new streams finally giving rise to a
   denial of service attack.

o Failure to deliver, or severely delaying, signalling messages
   adding an end-point to a multicast-group will prevent the new EP
   from receiving expected frames thus disrupting expected behavior.

o Delaying messages removing an EP from a group can lead to loss of
   privacy as the EP will continue to receive messages even after it
   is supposedly removed.

[4.2](#). Flow Modification and Spoofing

[4.2.1](#). Flow Modification

If the contents of a packet header or body can be modified by the
attacker, this can cause the packet to be routed incorrectly or
dropped, or the payload to be corrupted or subtly modified.

[4.2.2](#). Spoofing

[4.2.2.1](#). Dataplane Spoofing

Spoofing dataplane messages can result in increased resource
consumptions on the bridges throughout the network as it will
increase buffer usage and CPU utilization. This can lead to resource
exhaustion and/or increased delay.

If the attacker manages to create valid headers, the false messages
can be forwarded through the network, using part of the allocated
bandwidth. This in turn can cause legitimate messages to be dropped
when the budget has been exhausted.

Finally, the endpoint will have to deal with invalid messages being
delivered to the endpoint instead of (or in addition to) a valid
message.

4.2.2.2. Control Plane Spoofing

A successful control plane spoofing-attack will potentionally have adverse effects. It can do virtually anything from:

o modifying existing streams by changing the available bandwidth

o add or remove endpoints from a stream

o drop streams completly

o falsely create new streams (exhaust the systems resources, or to enable streams outside the Network engineer's control)

4.3. Segmentation attacks (injection)

4.3.1. Data Plane Segmentation

Injection of false messages in a DetNet stream could lead to exhaustion of the available bandwidth for a stream if the bridges accounts false messages to the stream's budget.

In a multipath scenario, injected messages will cause increased CPU utilization in elimination bridges. If enough paths are subject to malicious injection, the legitimate messages can be dropped. Likewise it can cause an increase in buffer usage. In total, it will consume more resources in the bridges than normal, giving rise to a resource exhaustion attack on the bridges.

If a stream is interrupted, the end application will be affected by what is now a non-deterministic stream.

4.3.2. Control Plane segmentation

A successful Control Plane segmentation attack control messages to be interpreted by nodes in the network, unbeknownst to the central controller or the network engineer. This has the potential to create

o new streams (exhausting resources)

o drop existing (denial of service)

o add/remove end-stations to a multicast group (loss of privacy)

o modify the stream attributes (affecting available bandwidth

4.4. Replication and Elimination

The Replication and Elimination is relevant only to Data Plane
messages as Signalling is not subject to multipath routing.

4.4.1. Increased Attack Surface

Covered briefly in Section 4.3

4.4.2. Header Manipulation at Elimination Bridges

Covered briefly in Section 4.3

4.5. Control or Signaling Packet Modification

If the control plane packets are subject to manipulation undetected,
the network can be severely compromised.

4.6. Control or Signaling Packet Injection

If an attacker can inject control plane packets undetected, the
network can be severely compromised.

4.7. Reconnaissance

Of all the attacks, this is one of the most difficult to detect and
counter. Often, an attacker will start out by observing the traffic
going through the network and use the knowledge gathered in this
phase to mount future attacks.

The attacker can, at their leisure, observe over time all aspects of
the messaging and signalling, learning the intent and purpose of all
traffic flows. At some later date, possibly at an important time in
an operational context, the attacker can launch a multi-faceted
attack, possibly in conjunction with some demand for ransom.

The flow-id in the header of the data plane-messages gives an
attacker a very reliable identifier for DetNet traffic, and this
traffic has a high probability of going to lucrative targets.

Applications which are ported from a private OT network to the higher
visibility DetNet environment may need to be adapted to limit
distinctive flow properties that could make them susceptible to
reconnaissance.

4.8. Attacks on Time Sync Mechanisms

   Attacks on time sync mechanisms are addressed in [RFC7384].

4.9. Attacks on Path Choice

   This is covered in part in Section 4.3, and as with Replication and
   Elimination (Section 4.4), this is relevant for DataPlane messages.

5. Security Threat Mitigation

   This section describes a set of measures that can be taken to
   mitigate the attacks described in Section 3. These mitigations
   should be viewed as a toolset that includes several different and
   diverse tools. Each application or system will typically use a
   subset of these tools, based on a system-specific threat analysis.

5.1. Path Redundancy

   Description

      A DetNet flow that can be forwarded simultaneously over multiple
      paths. Path replication and elimination [RFC8655] provides
      resiliency to dropped or delayed packets. This redundancy
      improves the robustness to failures and to man-in-the-middle
      attacks.

   Related attacks

      Path redundancy can be used to mitigate various man-in-the-middle
      attacks, including attacks described in Section 3.2.1,
      Section 3.2.2, Section 3.2.3, and Section 3.2.8. However it is
      also possible that multiple paths may make it more difficult to
      locate the source of a MITM attacker.

      A delay modulation attack could result in extensively exercising
      parts of the code that wouldn't normally be extensively exercised
      and thus might expose flaws in the system that might otherwise not
      be exposed.

5.2. Integrity Protection

   Description

      An integrity protection mechanism, such as a Hash-based Message
      Authentication Code (HMAC) can be used to mitigate modification
      attacks on IP packets. Integrity protection in the control plane
      is discussed in Section 5.6.

Packet Sequence Number Integrity Considerations

   The use of PREOF in a DetNet implementation implies the use of a
   sequence number for each packet. There is a trust relationship
   between the device that adds the sequence number and the device
   that removes the sequence number. The sequence number may be end-
   to-end source to destination, or may be added/deleted by network
   edge devices. The adder and remover(s) have the trust
   relationship because they are the ones that ensure that the
   sequence numbers are not modifiable. Between those two points,
   there may or may not be replication and elimination functions.
   The elimination functions must be able to see the sequence
   numbers. Therefore any encryption that is done between adders and
   removers must not obscure the sequence number. If the sequence
   removers and the eliminators are in the same physical device, it
   may be possible to obscure the sequence number, however that is a
   layer violation, and is not recommended practice.

Related attacks

   Integrity protection mitigates attacks related to modification and
   tampering, including the attacks described in Section 3.2.2 and
   Section 3.2.4.

5.3. DetNet Node Authentication

Description

   Source authentication verifies the authenticity of DetNet sources,
   enabling mitigation of spoofing attacks. Note that while
   integrity protection (Section 5.2) prevents intermediate nodes
   from modifying information, authentication can provide traffic
   origin verification, i.e. to verify that each packet in a DetNet
   flow is from a trusted source. Authentication may be implemented
   as part of ingress filtering, for example.

Related attacks

   DetNet node authentication is used to mitigate attacks related to
   spoofing, including the attacks of Section 3.2.2, and
   Section 3.2.4.

5.4. Dummy Traffic Insertion

Description

With some queueing methods such as [IEEE802.1Qch-2017] it is
possible to introduce dummy traffic in order to regularize the
timing of packet transmission.

Related attacks

Removing distinctive temporal properties of individual packets or
flows can be used to mitigate against reconnaissance attacks
Section 3.2.7.

5.5. Encryption

Description

DetNet flows can in principle be forwarded in encrypted form at
the DetNet layer, however, regarding encryption of IP headers see
Section 7.

Alternatively, if the payload is end-to-end encrypted at the
application layer, the DetNet nodes should not have any need to
inspect the payload itself, and thus the DetNet implementation can
be data-agnostic.

Related attacks

Encryption can be used to mitigate recon attacks (Section 3.2.7).
However, for a DetNet network to give differentiated quality of
service on a flow-by-flow basis, the network must be able to
identify the flows individually. This implies that in a recon
attack the attacker may also be able to track individual flows to
learn more about the system.

5.5.1. Encryption Considerations for DetNet

Any compute time which is required for encryption and decryption
processing ('crypto') must be included in the flow latency
calculations. Thus, crypto algorithms used in a DetNet must have
bounded worst-case execution times, and these values must be used in
the latency calculations.

Some crypto algorithms are symmetric in encode/decode time (such as
AES) and others are asymmetric (such as public key algorithms).
There are advantages and disadvantages to the use of either type in a
given DetNet context. The discussion in this document relates to the
timing implications of crypto for DetNet; it is assumed that
integrity considerations are covered elsewhere in the literature.

Asymmetrical crypto is typically not used in networks on a packet-by-packet basis due to its computational cost. For example, if only endpoint checks or checks at a small number of intermediate points are required, asymmetric crypto can be used to authenticate distribution or exchange of a secret symmetric crypto key; a successful check based on that key will provide traffic origin verification, as long as the key is kept secret by the participants. TLS and IKE (for IPsec) are examples of this for endpoint checks.

However, if secret symmetrical keys are used for this purpose the key must be given to all relays, which increases the probability of a secret key being leaked. Also, if any relay is compromised or misbehaving it may inject traffic into the flow.

Alternatively, asymmetric crypto can provide traffic origin verification at every intermediate node. For example, a DetNet flow can be associated with an (asymmetric) keypair, such that the private key is available to the source of the flow and the public key is distributed with the flow information, allowing verification at every node for every packet. However, this is more computationally expensive.

In either case, origin verification also requires replay detection as part of the security protocol to prevent an attacker from recording and resending traffic, e.g., as a denial of service attack on flow forwarding resources.

If crypto keys are to be regenerated over the duration of the flow then the time required to accomplish this must be accounted for in the latency calculations.

5.6. Control and Signaling Message Protection

Description

   Control and sigaling messages can be protected using authentication and integrity protection mechanisms.

Related attacks

   These mechanisms can be used to mitigate various attacks on the control plane, as described in Section 3.2.6, Section 3.2.8 and Section 3.2.5.

5.7. Dynamic Performance Analytics

Description

   The expectation is that the network will have a way to monitor to
   detect if timing guarantees are not being met, and a way to alert
   the control plane in that event. Information about the network
   performance can be gathered in real-time in order to detect
   anomalies and unusual behavior that may be the symptom of a
   security attack. The gathered information can be based, for
   example, on per-flow counters, bandwidth measurement, and
   monitoring of packet arrival times. Unusual behavior or
   potentially malicious nodes can be reported to a management
   system, or can be used as a trigger for taking corrective actions.
   The information can be tracked by DetNet end systems and transit
   nodes, and exported to a management system, for example using
   NETCONF.

Related attacks

   Performance analytics can be used to mitigate various attacks,
   including the ones described in Section 3.2.1 (Delay Attack),
   Section 3.2.3 (Resource Segmentation Attack), and Section 3.2.8
   (Time Sync Attack).

   For example, in the case of data plane delay attacks, one possible
   mitigation is to timestamp the data at the source, and timestamp
   it again at the destination, and if the resulting latency exceeds
   the promised bound, discard that data and warn the operator (and/
   or enter a fail-safe mode). Note that DetNet specifies packet
   sequence numbering, however it does not specify use of packet
   timestamps, although they may be used by the underlying transport
   (for example TSN) to provide the service.

5.8. Mitigation Summary

   The following table maps the attacks of Section 3 to the impacts of
   Section 4, and to the mitigations of the current section. Each row
   specifies an attack, the impact of this attack if it is successfully
   implemented, and possible mitigation methods.

   Editor's note: Is this tabular summary of the above information
   useful or necessary in this draft? If we opt to maintain the tables
   then the WG needs to validate them for completeness and correctness
   after all other draft comments have been addressed.

   +----------------------+--------------------+--------------------+

Attack	Impact	Mitigations
Delay Attack	-Non-deterministic delay -Data disruption -Increased resource consumption	-Path redundancy -Performance analytics
Reconnaissance	-Enabler for other attacks	-Encryption -Dummy traffic insertion
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
Attacks on Time Sync	-Non-deterministic	-Path redundancy

```
|Mechanisms            | delay             |-Control message     |
|                      |-Increased resource| protection          |
|                      | consumption       |-Performance         |
|                      |-Data disruption   | analytics           |
+----------------------+-------------------+---------------------+
```

              Figure 3: Mapping Attacks to Impact and Mitigations

6. Association of Attacks to Use Cases

   Different attacks can have different impact and/or mitigation
   depending on the use case, so we would like to make this association
   in our analysis. However since there is a potentially unbounded list
   of use cases, we categorize the attacks with respect to the common
   themes of the use cases as identified in the Use Case Common Themes
   section of the DetNet Use Cases [RFC8578].

   See also Figure 2 for a mapping of the impact of attacks per use case
   by industry.

6.1. Use Cases by Common Themes

   In this section we review each theme and discuss the attacks that are
   applicable to that theme, as well as anything specific about the
   impact and mitigations for that attack with respect to that theme.
   The table Figure 5 then provides a summary of the attacks that are
   applicable to each theme.

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 document) 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.

6.1.2. Central Administration

   A DetNet network is expected to be controlled by a centralized
   network configuration and control system (CNC). Such a system may be
   in a single central location, or it may be distributed across
   multiple control entities that function together as a unified control
   system for the network.

   In this document we distinguish between attacks on the DetNet Control
   plane vs. Data plane. But is an attack affecting control plane
   packets synonymous with an attack on the CNC itself? For purposes of
   this document let us consider an attack on the CNC itself to be out
   of scope, and consider all attacks named in this document which are
   relevant to control plane packets to be relevant to this theme,
   including Path Manipulation, Path Choice, Control Packet Modification
   or Injection, Reconaissance and Attacks on Time Sync Mechanisms.

6.1.3. Hot Swap

   A DetNet network is not expected to be "plug and play" - it is
   expected that there is some centralized network configuration and
   control system. However, the ability to "hot swap" components (e.g.
   due to malfunction) is similar enough to "plug and play" that this
   kind of behavior may be expected in DetNet networks, depending on the
   implementation.

   An attack surface related to Hot Swap is that the DetNet network must
   at least consider input at runtime from devices that were not part of
   the initial configuration of the network. Even a "perfect" (or
   "hitless") replacement of a device at runtime would not necessarily
   be ideal, since presumably one would want to distinguish it from the
   original for OAM purposes (e.g. to report hot swap of a failed
   device).

   This implies that an attack such as Flow Modification, Spoofing or
   Inter-segment (which could introduce packets from a "new" device
   (i.e. one heretofore unknown on the network) could be used to exploit
   the need to consider such packets (as opposed to rejecting them out
   of hand as one would do if one did not have to consider introduction
   of a new device).

   Similarly if the network was designed to support runtime replacement
   of a clock device, then presence (or apparent presence) and thus
   consideration of packets from a new such device could affect the
   network, or the time sync of the network, for example by initiating a
   new Best Master Clock selection process. Thus attacks on time sync
   should be considered when designing hot swap type functionality (see
   [RFC7384]).

6.1.4. Data Flow Information Models

   Data Flow Information Models specific to DetNet networks are
   specified by DetNet, and thus are 'new' and thus potentially present
   a new attack surface.

6.1.5. L2 and L3 Integration

   A DetNet network integrates Layer 2 (bridged) networks (e.g. AVB/TSN
   LAN) and Layer 3 (routed) networks via the use of well-known
   protocols such as IP, MPLS-PW, and Ethernet.

   There are no specific entries in our table, however that does not
   imply that there could be no relevant attacks related to L2,L3
   integration.

6.1.6. End-to-End Delivery

   Packets sent over DetNet are not to be dropped by the network due to
   congestion. (Packets may however intentionally be dropped for
   intended reasons, e.g. per security measures).

   A Data plane attack may force packets to be dropped, for example a
   "long" Delay or Replication/Elimination or Flow Modification attack.

   The same result might be obtained by a Control plane attack, e.g.
   Path Manipulation or Signaling Packet Modification.

   It may be that such attacks are limited to Internal MITM attackers,
   but other possibilities should be considered.

   An attack may also cause packets that should not be delivered to be
   delivered, such as by forcing packets from one (e.g. replicated) path
   to be preferred over another path when they should not be
   (Replication attack), or by Flow Modification, or by Path Choice or
   Packet Injection. A Time Sync attack could cause a system that was
   expecting certain packets at certain times to accept unintended
   packets based on compromised system time or time windowing in the
   scheduler.

   Packets may also be dropped due to malfunctioning software or
   hardware.

6.1.7. Proprietary Deterministic Ethernet Networks

   There are many proprietary non-interoperable deterministic Ethernet-
   based networks currently available; DetNet is intended to provide an
   open-standards-based alternative to such networks. In cases where a

DetNet intersects with remnants of such networks or their protocols, such as by protocol emulation or access to such a network via a gateway, new attack surfaces can be opened.

For example an Inter-Segment or Control plane attack such as Path Manipulation, Path Choice or Control Packet Modification/Injection could be used to exploit commands specific to such a protocol, or that are interpreted differently by the different protocols or gateway.

6.1.8. Replacement for Proprietary Fieldbuses

There are many proprietary "field buses" used in today's industrial and other industries; DetNet is intended to provide an open-standards-based alternative to such buses. In cases where a DetNet intersects with such fieldbuses or their protocols, such as by protocol emulation or access via a gateway, new attack surfaces can be opened.

For example an Inter-Segment or Control plane attack such as Path Manipulation, Path Choice or Control Packet Modification/Injection could be used to exploit commands specific to such a protocol, or that are interpreted differently by the different protocols or gateway.

6.1.9. Deterministic vs Best-Effort Traffic

Most of the themes described in this document address OT (reserved) streams - this item is intended to address issues related to IT traffic on a DetNet.

DetNet is intended to support coexistence of time-sensitive operational (OT, deterministic) traffic and information (IT, "best effort") traffic on the same ("unified") network.

With DetNet, this coexistance will become more common, and mitigations will need to be established. The fact that the IT traffic on a DetNet is limited to a corporate controlled network makes this a less difficult problem compared to being exposed to the open Internet, however this aspect of DetNet security should not be underestimated.

An Inter-segment attack can flood the network with IT-type traffic with the intent of disrupting handling of IT traffic, and/or the goal of interfering with OT traffic. Presumably if the stream reservation and isolation of the DetNet is well-designed (better-designed than the attack) then interference with OT traffic should not result from an attack that floods the network with IT traffic.

However the DetNet's handling of IT traffic may not (by design) be as
resilient to DOS attack, and thus designers must be otherwise
prepared to mitigate DOS attacks on IT traffic in a DetNet.

6.1.10. Deterministic Flows

Reserved bandwidth data flows (deterministic flows) must provide the
allocated bandwidth, and must be isolated from each other.

A Spoofing or Inter-segment attack which adds packet traffic to a
bandwidth-reserved stream could cause that stream to occupy more
bandwidth than it is allocated, resulting in interference with other
deterministic flows.

A Flow Modification or Spoofing or Header Manipulation or Control
Packet Modification attack could cause packets from one flow to be
directed to another flow, thus breaching isolation between the flows.

6.1.11. Unused Reserved Bandwidth

If bandwidth reservations are made for a stream but the associated
bandwidth is not used at any point in time, that bandwidth is made
available on the network for best-effort traffic. However, note that
security considerations for best-effort traffic on a DetNet network
is out of scope of the present document, provided that such an attack
does not affect performance for DetNet OT traffic.

6.1.12. Interoperability

The DetNet network specifications are intended to enable an ecosystem
in which multiple vendors can create interoperable products, thus
promoting device diversity and potentially higher numbers of each
device manufactured.

Given that the DetNet specifications are unambiguously written and
that the implementations are accurate, then this should not in and of
itself cause a security concern; however, in the real world, it could
be. The network operator can mitigate this through sufficient
interoperability testing.

6.1.13. Cost Reductions

The DetNet network specifications are intended to enable an ecosystem
in which multiple vendors can create interoperable products, thus
promoting higher numbers of each device manufactured, promoting cost
reduction and cost competition among vendors. Such "low cost"
hardware or software components might present security concerns.

Network operators can mitigate such concerns through sufficient
product testing.

6.1.14. Insufficiently Secure Devices

The DetNet network specifications are intended to enable an ecosystem
in which multiple vendors can create interoperable products, thus
promoting device diversity and potentially higher numbers of each
device manufactured. Software that was originally designed for
operation in isolated OT networks (and thus may not have been
designed to be sufficiently secure, or secure at all) but is then
deployed on a DetNet network that is intended to be highly secure may
present an attack surface. (For example IoT exploits like the Mirai
video-camera botnet ([MIRAI]).

The DetNet network operator may need to take specific actions to
protect such devices.

6.1.15. DetNet Network Size

DetNet networks range in size from very small, e.g. inside a single
industrial machine, to very large, for example a Utility Grid network
spanning a whole country.

The size of the network might be related to how the attack is
introduced into the network, for example if the entire network is
local, there is a threat that power can be cut to the entire network.
If the network is large, perhaps only a part of the network is
attacked.

A Delay attack might be as relevant to a small network as to a large
network, although the amount of delay might be different.

Attacks sourced from IT traffic might be more likely in large
networks, since more people might have access to the network,
presenting a larger attack surface. Similarly Path Manipulation,
Path Choice and Time Sync attacks seem more likely relevant to large
networks.

6.1.16. Multiple Hops

Large DetNet networks (e.g. a Utility Grid network) may involve many
"hops" over various kinds of links for example radio repeaters,
microwave links, fiber optic links, etc..

An attack that takes advantage of flaws (or even normal operation) in
the device drivers for the various links (through internal knowledge
of how the individual driver or firmware operates, perhaps like the

Stuxnet attack) could take proportionately greater advantage of this
topology. We don't currently have an attack like this defined; we
have only "protocol" (time or packet) based attacks. Perhaps we need
to define an attack like this? Or is that out of scope for DetNet?

It is also possible that this DetNet topology will not be in as
common use as other more homogeneous topologies so there may be more
opportunity for attackers to exploit software and/or protocol flaws
in the implementations which have not been wrung out by extensive
use, particularly in the case of early adopters.

Of the attacks we have defined, the ones identified above as relevant
to "large" networks seem to be most relevant.

6.1.17. Level of Service

A DetNet is expected to provide means to configure the network that
include querying network path latency, requesting bounded latency for
a given stream, requesting worst case maximum and/or minimum latency
for a given path or stream, and so on. It is an expected case that
the network cannot provide a given requested service level. In such
cases the network control system should reply that the requested
service level is not available (as opposed to accepting the parameter
but then not delivering the desired behavior).

Control plane attacks such as Signaling Packet Modification and
Injection could be used to modify or create control traffic that
could interfere with the process of a user requesting a level of
service and/or the network's reply.

Reconnaissance could be used to characterize flows and perhaps target
specific flows for attack via the Control plane as noted above.

6.1.18. Bounded Latency

DetNet provides the expectation of guaranteed bounded latency.

Delay attacks can cause packets to miss their agreed-upon latency
boundaries.

Time Sync attacks can corrupt the system's time reference, resulting
in missed latency deadlines (with respect to the "correct" time
reference).

6.1.19. Low Latency

   Applications may require "extremely low latency" however depending on
   the application these may mean very different latency values; for
   example "low latency" across a Utility grid network is on a different
   time scale than "low latency" in a motor control loop in a small
   machine. The intent is that the mechanisms for specifying desired
   latency include wide ranges, and that architecturally there is
   nothing to prevent arbitrarily low latencies from being implemented
   in a given network.

   Attacks on the Control plane (as described in the Level of Service
   theme) and Delay and Time attacks (as described in the Bounded
   Latency theme) both apply here.

6.1.20. Bounded Jitter (Latency Variation)

   DetNet is expected to provide bounded jitter (packet to packet
   latency variation).

   Delay attacks can cause packets to vary in their arrival times,
   resulting in packet to packet latency variation, thereby violating
   the jitter specification.

6.1.21. Symmetrical Path Delays

   Some applications would like to specify that the transit delay time
   values be equal for both the transmit and return paths.

   Delay attacks can cause path delays to materially differ between
   paths.

   Time Sync attacks can corrupt the system's time reference, resulting
   in path delays that may be perceived to be different (with respect to
   the "correct" time reference) even if they are not materially
   different.

6.1.22. Reliability and Availability

   DetNet based systems are expected to be implemented with essentially
   arbitrarily high availability (for example 99.9999% up time, or even
   12 nines). The intent is that the DetNet designs should not make any
   assumptions about the level of reliability and availability that may
   be required of a given system, and should define parameters for
   communicating these kinds of metrics within the network.

   Any attack on the system, of any type, can affect its overall
   reliability and availability, thus in our table we have marked every

attack. Since every DetNet depends to a greater or lesser degree on
reliability and availability, this essentially means that all
networks have to mitigate all attacks, which to a greater or lesser
degree defeats the purpose of associating attacks with use cases. It
also underscores the difficulty of designing "extremely high
reliability" networks.

6.1.23. Redundant Paths

DetNet based systems are expected to be implemented with essentially
arbitrarily high reliability/availability. A strategy used by DetNet
for providing such extraordinarily high levels of reliability is to
provide redundant paths that can be seamlessly switched between, all
the while maintaining the required performance of that system.

Replication-related attacks are by definition applicable here.
Control plane attacks can also interfere with the configuration of
redundant paths.

6.1.24. Security Measures

A DetNet network must be made secure against devices failures,
attackers, misbehaving devices, and so on. Does the threat affect
such security measures themselves, e.g. by attacking SW designed to
protect against device failure?

This is TBD, thus there are no specific entries in our table, however
that does not imply that there could be no relevant attacks.

6.2. Attack Types by Use Case Common Theme

The following table lists the attacks of Section 3, assigning a
number to each type of attack. That number is then used as a short
form identifier for the attack in Figure 5.

Editor's note: Is this tabular summary of the above information
useful or necessary in this draft? If we opt to maintain the tables
then the WG needs to validate them for completeness and correctness
after all other draft comments have been addressed.

```
+--+----------------------------------------+--------------------+
|  | Attack                                 |      Section        |
+--+----------------------------------------+--------------------+
| 1|Delay Attack                            |  Section 3.2.1      |
+--+----------------------------------------+--------------------+
| 2|DetNet Flow Modification or Spoofing    |  Section 3.2.2      |
+--+----------------------------------------+--------------------+
| 3|Inter-Segment Attack                    |  Section 3.2.3      |
+--+----------------------------------------+--------------------+
| 4|Replication: Increased attack surface   |  Section 3.2.4.1    |
+--+----------------------------------------+--------------------+
| 5|Replication-related Header Manipulation |  Section 3.2.4.2    |
+--+----------------------------------------+--------------------+
| 6|Path Manipulation                       |  Section 3.2.5.1    |
+--+----------------------------------------+--------------------+
| 7|Path Choice: Increased Attack Surface   |  Section 3.2.5.2    |
+--+----------------------------------------+--------------------+
| 8|Control or Signaling Packet Modification|  Section 3.2.6.1    |
+--+----------------------------------------+--------------------+
| 9|Control or Signaling Packet Injection   |  Section 3.2.6.2    |
+--+----------------------------------------+--------------------+
|10|Reconnaissance                          |  Section 3.2.7      |
+--+----------------------------------------+--------------------+
|11|Attacks on Time Sync Mechanisms         |  Section 3.2.8      |
+--+----------------------------------------+--------------------+
```

                      Figure 4: List of Attacks

   The following table maps the use case themes presented in this memo
   to the attacks of Figure 4. Each row specifies a theme, and the
   attacks relevant to this theme are marked with a '+'.

```
+---------------------------+-----------------------------+
| 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      |  |  |  |  |  |  |  |  |  |  |  |
+---------------------------+--+--+--+--+--+--+--+--+--+--+--+
```

Theme	1	2	3	4	5	6	7	8	9	10	11
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	+							+	+	+	+
Bounded Jitter	+										
Symmetric Path Delays	+										+
Reliability and Availability	+	+	+	+	+	+	+	+	+	+	+
Redundant Paths				+	+			+	+		
Security Measures											

Figure 5: Mapping Between Themes and Attacks

6.3. Security Considerations for OAM Traffic

   This section considers DetNet-specific security considerations for
   packet traffic that is generated and transmitted over a DetNet as
   part of OAM (Operations, Administration and Maintenance). For
   purposes of this discussion, OAM traffic falls into one of two basic
   types:

   o OAM traffic generated by the network itself. The additional
      bandwidth required for such packets is added by the network
      administration, presumably transparent to the customer. Security
      considerations for such traffic are not DetNet-specific (apart
      from such traffic being subject to the same DetNet-specific
      security considerations as any other DetNet data flow) and are
      thus not covered in this document.

   o OAM traffic generated by the customer. From a DetNet security
      point of view, DetNet security considerations for such traffic are
      exactly the same as for any other customer data flows.

   Thus OAM traffic presents no additional (i.e. OAM-specific) DetNet
   security considerations.

7. DetNet Technology-Specific Threats

   Section 3 described threats which are independent of a DetNet
   implementation. This section considers threats specifically related
   to the IP- and MPLS-specific aspects of DetNet implementations.

   The primary security considerations for the data plane specifically
   are to maintain the integrity of the data and the delivery of the
   associated DetNet service traversing the DetNet network.

   The primary relevant differences between IP and MPLS implementations
   are in flow identification and OAM methodologies.

   As noted in [RFC8655], DetNet operates at the IP layer
   ([I-D.ietf-detnet-ip]) and delivers service over sub-layer
   technologies such as MPLS ([I-D.ietf-detnet-mpls]) and IEEE 802.1
   Time-Sensitive Networking (TSN) ([I-D.ietf-detnet-ip-over-tsn]).
   Application flows can be protected through whatever means are
   provided by the layer and sub-layer technologies. For example,
   technology-specific encryption may be used, such as that provided by
   IPSec [RFC4301] for IP flows and/or by an underlying sub-net using
   MACSec [IEEE802.1AE-2018] for IP over Ethernet (Layer-2) flows.

   However, if the DetNet nodes cannot decrypt IPsec traffic, IPSec may
   not be a valid option; this is because the DetNet IP data plane

identifies flows via a 6-tuple that consists of two IP addresses, the
transport protocol ID, two transport protocol port numbers and the
DSCP in the IP header. When IPsec is used, the transport header is
encrypted and the next protocol ID is an IPsec protocol, usually ESP,
and not a transport protocol (e.g., neither TCP nor UDP, etc.)
leaving only three components of the 6-tuple, which are the two IP
addresses and the DSCP, which are in general not sufficient to
identify a DetNet flow.

Sections below discuss threats specific to IP and MPLS in more
detail.

7.1. IP

The IP protocol has a long history of security considerations and
architectural protection mechanisms. From a data plane perspective
DetNet does not add or modify any IP header information, and its use
as a DetNet Data Plane does not introduce any new security issues
that were not there before, apart from those already described in the
data-plane-independent threats section Section 3.

Thus the security considerations for a DetNet based on an IP data
plane are purely inherited from the rich IP Security literature and
code/application base, and the data-plane-independent section of this
document.

Maintaining security for IP segments of a DetNet may be more
challenging than for the MPLS segments of the network, given that the
IP segments of the network may reach the edges of the network, which
are more likely to involve interaction with potentially malevolent
outside actors. Conversely MPLS is inherently more secure than IP
since it is internal to routers and it is well-known how to protect
it from outside influence.

Another way to look at DetNet IP security is to consider it in the
light of VPN security; as an industry we have a lot of experience
with VPNs running through networks with other VPNs, it is well known
how to secure the network for that. However for a DetNet we have the
additional subtlety that any possible interaction of one packet with
another can have a potentially deleterious effect on the time
properties of the flows. So the network must provide sufficient
isolation between flows, for example by protecting the forwarding
bandwidth and related resources so that they are available to detnet
traffic, by whatever means are appropriate for that network's data
plane.

In a VPN, bandwidth is generally guaranteed over a period of time,
whereas in DetNet it is not aggregated over time. This implies that

any VPN-type protection mechanism must also maintain the DetNet
timing constraints.

7.2. MPLS

An MPLS network carrying DetNet traffic is expected to be a "well-
managed" network. Given that this is the case, it is difficult for
an attacker to pass a raw MPLS encoded packet into a network because
operators have considerable experience at excluding such packets at
the network boundaries, as well as excluding MPLS packets being
inserted through the use of a tunnel.

MPLS security is discussed extensively in [RFC5920] ("Security
Framework for MPLS and GMPLS Networks") to which the reader is
referred.

[RFC6941] builds on [RFC5920] by providing additional security
considerations that are applicable to the MPLS-TP extensions
appropriate to the MPLS Transport Profile [RFC5921], and thus to the
operation of DetNet over some types of MPLS network.

[RFC5921] introduces to MPLS new Operations, Administration, and
Maintenance (OAM) capabilities, a transport-oriented path protection
mechanism, and strong emphasis on static provisioning supported by
network management systems.

The operation of DetNet over an MPLS network is modeled on the
operation of multi-segment pseudowires (MS-PW). Thus for guidance on
securing the DetNet elements of DetNet over MPLS the reader is
referred to the MS-PW security mechanisms as defined in [RFC4447],
[RFC3931], [RFC3985], [RFC6073], and [RFC6478].

Having attended to the conventional aspects of network security it is
necessary to attend to the dynamic aspects. The closest experience
that the IETF has with securing protocols that are sensitive to
manipulation of delay are the two way time transfer protocols (TWTT),
which are NTP [RFC5905] and Precision Time Protocol [IEEE1588]. The
security requirements for these are described in [RFC7384].

One particular problem that has been observed in operational tests of
TWTT protocols is the ability for two closely but not completely
synchronized streams to beat and cause a sudden phase hit to one of
the streams. This can be mitigated by the careful use of a
scheduling system in the underlying packet transport.

Further consideration of protection against dynamic attacks is work
in progress.

8. IANA Considerations

   This memo includes no requests from IANA.

9. Security Considerations

   The security considerations of DetNet networks are presented
   throughout this document.

10. Informative References

   [ARINC664P7]
              ARINC, "ARINC 664 Aircraft Data Network, Part 7, Avionics
              Full-Duplex Switched Ethernet Network", 2009.

   [I-D.ietf-detnet-data-plane-framework]
              Varga, B., Farkas, J., Berger, L., Fedyk, D., Malis, A.,
              Bryant, S., and J. Korhonen, "DetNet Data Plane
              Framework", draft-ietf-detnet-data-plane-framework-03
              (work in progress), October 2019.

   [I-D.ietf-detnet-ip]
              Varga, B., Farkas, J., Berger, L., Fedyk, D., Malis, A.,
              Bryant, S., and J. Korhonen, "DetNet Data Plane: IP",
              draft-ietf-detnet-ip-04 (work in progress), November 2019.

   [I-D.ietf-detnet-ip-over-tsn]
              Varga, B., Farkas, J., Malis, A., and S. Bryant, "DetNet
              Data Plane: IP over IEEE 802.1 Time Sensitive Networking
              (TSN)", draft-ietf-detnet-ip-over-tsn-01 (work in
              progress), October 2019.

   [I-D.ietf-detnet-mpls]
              Varga, B., Farkas, J., Berger, L., Fedyk, D., Malis, A.,
              Bryant, S., and J. Korhonen, "DetNet Data Plane: MPLS",
              draft-ietf-detnet-mpls-04 (work in progress), November
              2019.

   [I-D.varga-detnet-service-model]
              Varga, B. and J. Farkas, "DetNet Service Model", draft-
              varga-detnet-service-model-02 (work in progress), May
              2017.

   [IEEE1588]
              IEEE, "IEEE 1588 Standard for a Precision Clock
              Synchronization Protocol for Networked Measurement and
              Control Systems Version 2", 2008.

   [IEEE802.1AE-2018]
             IEEE Standards Association, "IEEE Std 802.1AE-2018 MAC
             Security (MACsec)", 2018,
             <https://ieeexplore.ieee.org/document/8585421>.

   [IEEE802.1Qch-2017]
             IEEE Standards Association, "IEEE Standard for Local and
             metropolitan area networks--Bridges and Bridged Networks--
             Amendment 29: Cyclic Queuing and Forwarding", 2017,
             <https://ieeexplore.ieee.org/document/7961303>.

   [MIRAI]   krebsonsecurity.com, "https://krebsonsecurity.com/2016/10/
             hacked-cameras-dvrs-powered-todays-massive-internet-
             outage/", 2016.

   [RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z.,
             and W. Weiss, "An Architecture for Differentiated
             Services", RFC 2475, DOI 10.17487/RFC2475, December 1998,
             <https://www.rfc-editor.org/info/rfc2475>.

   [RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC
             Text on Security Considerations", BCP 72, RFC 3552,
             DOI 10.17487/RFC3552, July 2003,
             <https://www.rfc-editor.org/info/rfc3552>.

   [RFC3931] Lau, J., Ed., Townsley, M., Ed., and I. Goyret, Ed.,
             "Layer Two Tunneling Protocol - Version 3 (L2TPv3)",
             RFC 3931, DOI 10.17487/RFC3931, March 2005,
             <https://www.rfc-editor.org/info/rfc3931>.

   [RFC3985] Bryant, S., Ed. and P. Pate, Ed., "Pseudo Wire Emulation
             Edge-to-Edge (PWE3) Architecture", RFC 3985,
             DOI 10.17487/RFC3985, March 2005,
             <https://www.rfc-editor.org/info/rfc3985>.

   [RFC4301] Kent, S. and K. Seo, "Security Architecture for the
             Internet Protocol", RFC 4301, DOI 10.17487/RFC4301,
             December 2005, <https://www.rfc-editor.org/info/rfc4301>.

   [RFC4447] Martini, L., Ed., Rosen, E., El-Aawar, N., Smith, T., and
             G. Heron, "Pseudowire Setup and Maintenance Using the
             Label Distribution Protocol (LDP)", RFC 4447,
             DOI 10.17487/RFC4447, April 2006,
             <https://www.rfc-editor.org/info/rfc4447>.

   [RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch,
              "Network Time Protocol Version 4: Protocol and Algorithms
              Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010,
              <https://www.rfc-editor.org/info/rfc5905>.

   [RFC5920] Fang, L., Ed., "Security Framework for MPLS and GMPLS
              Networks", RFC 5920, DOI 10.17487/RFC5920, July 2010,
              <https://www.rfc-editor.org/info/rfc5920>.

   [RFC5921] Bocci, M., Ed., Bryant, S., Ed., Frost, D., Ed., Levrau,
              L., and L. Berger, "A Framework for MPLS in Transport
              Networks", RFC 5921, DOI 10.17487/RFC5921, July 2010,
              <https://www.rfc-editor.org/info/rfc5921>.

   [RFC6073] Martini, L., Metz, C., Nadeau, T., Bocci, M., and M.
              Aissaoui, "Segmented Pseudowire", RFC 6073,
              DOI 10.17487/RFC6073, January 2011,
              <https://www.rfc-editor.org/info/rfc6073>.

   [RFC6478] Martini, L., Swallow, G., Heron, G., and M. Bocci,
              "Pseudowire Status for Static Pseudowires", RFC 6478,
              DOI 10.17487/RFC6478, May 2012,
              <https://www.rfc-editor.org/info/rfc6478>.

   [RFC6941] Fang, L., Ed., Niven-Jenkins, B., Ed., Mansfield, S., Ed.,
              and R. Graveman, Ed., "MPLS Transport Profile (MPLS-TP)
              Security Framework", RFC 6941, DOI 10.17487/RFC6941, April
              2013, <https://www.rfc-editor.org/info/rfc6941>.

   [RFC7384] Mizrahi, T., "Security Requirements of Time Protocols in
              Packet Switched Networks", RFC 7384, DOI 10.17487/RFC7384,
              October 2014, <https://www.rfc-editor.org/info/rfc7384>.

   [RFC8578] Grossman, E., Ed., "Deterministic Networking Use Cases",
              RFC 8578, DOI 10.17487/RFC8578, May 2019,
              <https://www.rfc-editor.org/info/rfc8578>.

   [RFC8655] Finn, N., Thubert, P., Varga, B., and J. Farkas,
              "Deterministic Networking Architecture", RFC 8655,
              DOI 10.17487/RFC8655, October 2019,
              <https://www.rfc-editor.org/info/rfc8655>.

Authors' Addresses

   Tal Mizrahi
   Huawei Network.IO Innovation Lab

   Email: tal.mizrahi.phd@gmail.com

Ethan Grossman (editor)
Dolby Laboratories, Inc.
1275 Market Street
San Francisco, CA 94103
USA

Phone: +1 415 645 4726
Email: ethan.grossman@dolby.com
URI: http://www.dolby.com

Andrew J. Hacker
MistIQ Technologies, Inc

Harrisburg, PA
USA

Phone:
Email: ajhacker@mistiqtech.com
URI: http://www.mistiqtech.com

Subir Das
Applied Communication Sciences
150 Mount Airy Road, Basking Ridge
New Jersey, 07920
USA

Email: sdas@appcomsci.com

John Dowdell
Airbus Defence and Space
Celtic Springs
Newport NP10 8FZ
United Kingdom

Email: john.dowdell.ietf@gmail.com

Henrik Austad
SINTEF Digital
Klaebuveien 153
Trondheim 7037
Norway

Email: henrik@austad.us

Norman Finn
Huawei

Email: norman.finn@mail01.huawei.com