In-situ OAM Flags
In-situ OAM Direct Exporting

draft-ietf-ippm-ioam-flags-04
draft-ietf-ippm-ioam-direct-export-03

IETF 110, IPPM
March 2021
Open issue regarding amplification threat in

In-situ OAM Flags
In-situ OAM Direct Exporting
Amplification Threat

• Loopback flag:
  Looped back packet is sent by every IOAM transit node, thus potentially amplifying maliciously injected packets.

• Direct exporting:
  DEX causes every transit node to export IOAM data, similarly amplifying malicious packets.

• Amplification is both a performance issue and a security issue.
Flag draft / DEX draft – How Amplification is Addressed

Flag draft

2. Performance Considerations

Each of the IETF that are defined in this document may have implications on the performance of the data path in one or more of the entities that are provided with the DEX draft. This is generally non-trivial that is critical to the implementation. A key aspect of the implementation is the actual performance of the data path, which is often impacted by the performance of the network. In this case, an attacker may try to use the functionality that is included in this document to attack the network.

An attacker may attempt to configure network devices by injecting synthetic packets that include the attack option. Similarly, an attacker may try to use the functionality that is included in this document to attack the network.

a. Loopback flag: An attacker may try to use the loopback flag to flood the network with packets that advertise that the packets are intended for the attacker.

b. Security considerations:

Security considerations may be used to affect the performance of the network. For example, if a loopback flag is used to flood the network, the attacker may try to use the functionality that is included in this document to attack the network.

Performance considerations may be used to affect the performance of the network. For example, if a loopback flag is used to flood the network, the attacker may try to use the functionality that is included in this document to attack the network.

DEX draft

3. Performance Considerations

The DEX option triggers exported packets to be expected at a receiving entity (RSEE). It may also help in reducing the receiving entity’s performance, or the performance along the paths leading to it.

Therefore, rate limiting may be enabled so as to ensure that direct injection is used at a rate that does not significantly affect the performance of the network.

Performance considerations may be used to affect the performance of the network. For example, if a loopback flag is used to flood the network, the attacker may try to use the functionality that is included in this document to attack the network.

Security Considerations:

Security considerations may be used to affect the performance of the network. For example, if a loopback flag is used to flood the network, the attacker may try to use the functionality that is included in this document to attack the network.
# How Amplification is Addressed in the Drafts – Brief Summary

<table>
<thead>
<tr>
<th>Description of the threat</th>
<th>Flag Draft</th>
<th>DEX Draft</th>
</tr>
</thead>
<tbody>
<tr>
<td>The amplification problem and its effects are described.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description of potentially worse threats in wide area networks.</td>
<td></td>
<td>More on this on the next slide.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mitigations</th>
<th>Flag Draft</th>
<th>DEX Draft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confined administrative domain.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ability to limit the rate of looped back / exported traffic.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ability to apply loopback to a subset of the traffic.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Looped back packets are truncated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IOAM trace option is limited to a single data field when using loopback.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Pathological Amplification Cases

Thanks Martin Duke for raising these issues.

Suggested mitigation methods (beyond previous slide):
• Probability bounds – IOAM encapsulating node: limit the DEX probability / loopback probability for transit data packets.
  1 of n packets for a sufficiently large n.
• Stronger restriction to a domain.
Amplification Threat – Next Steps

• The authors will update the security considerations in the two drafts based on the previous slide.

• Any further feedback and text suggestions would be welcome.
In-situ OAM Flags

draft-ietf-ippm-ioam-flags-04

Tal Mizrahi, Frank Brockners, Shwetha Bhandari, Ramesh Sivakolundu,
Carlos Pignataro, Aviv Kfir, Barak Gafni, Mickey Spiegel, Jennifer Lemon

IETF 110, IPPM
March 2021
Status of this Draft

- Version 04 addresses a security-related comment from Martin Duke. Another update is expected soon (see previous slides).

- Once the security issue is resolved, the authors will suggest WG last call.
In-situ OAM Direct Exporting

draft-ietf-ippm-ioam-direct-export-03

Haoyu Song, Barak Gafni, Tianran Zhou, Zhenbin Li, Frank Brockners, Shwetha Bhandari, Ramesh Sivakolundu, Tal Mizrahi

IETF 110, IPPM,
March 2021
Status of this Draft

• This draft is the product of a design team that worked on combining two documents (PBT-I and immediate exporting).

• Open issues:
  • Hop Count field.
  • Direct Exporting option length.

• Changes in version 03:
  • Minor changes related to security.
  • More on security in the previous slides.
Open Issue – Hop Count

• Question: should the DEX option include an explicit Hop Count field, or is the Hop_Lim/Node_ID data field sufficient?

• No Hop Count:
  • Using existing functionality: Hop_Lim/Node_ID data field can be used, copied from the TTL/Hop Limit from the lower layer, and included in the exported packet.
  • The DEX option does not need to be modified by transit switches.

• Explicit Hop Count:
  • The lower layer TTL may not be accurate, e.g., L2 or hierarchical VPN.
  • Allows to detect IOAM-capable node that fails to export packets.

• Version 02:
  • The DEX option does not include a Hop Count field.
  • Discussion in an appendix.
Open Issue – DEX Option Length

• The DEX option has two optional fields: Sequence Number, Flow ID. Two possible lengths: 8 octets / 16 octets. The length is known from lower layer header.

• What happens if we want to add another field in the future?

• **Solution 1:**
  • Use reserved flags for indicating whether the Sequence Number and Flow ID are present.
  • No need to rely on length from lower layer header.

• **Solution 2:**
  • Define a constant DEX option length (8 octets) without optional fields.