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

IETF 110, IPPM, March 2021

Amplification Threat

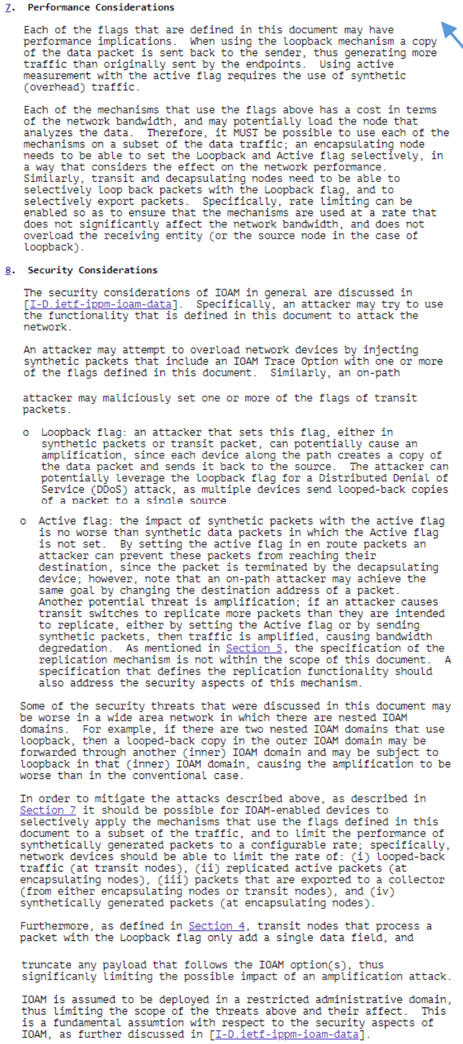
- Loopback flag:
  Looped back packet is sent by every IOAM transit node, thus potentially amplifying maliciously injected packets.

- 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



7. Performance Considerations

Each of the flags that are defined in this document may have performance implications. When using the loopback mechanism a copy of the data packet is sent back to the sender, thus generating more traffic than originally sent by the endpoints. Using active measurement with the active flag requires the use of synthetic (overhead) traffic.

Each of the mechanisms that use the flags above has a cost in terms of the network bandwidth, and may potentially load the node that analyzes the data. Therefore, it MUST be possible to use each of the mechanisms on a subset of the data traffic; an encapsulating node needs to be able to set the Loopback and Active flag selectively, in a way that considers the effect on the network performance. Similarly, transit and decapsulating nodes need to be able to selectively loop back packets with the Loopback flag, and to selectively export packets. Specifically, rate limiting can be enabled so as to ensure that the mechanisms are used at a rate that does not significantly affect the network bandwidth, and does not overload the receiving entity (or the source node in the case of loopback).

8. Security Considerations

The security considerations of IOAM in general are discussed in [I-D.ietf-ippm-ioam-data]. Specifically, an attacker may try to use the functionality that is defined in this document to attack the network.

An attacker may attempt to overload network devices by injecting synthetic packets that include an IOAM Trace Option with one or more of the flags defined in this document. Similarly, an on-path

attacker may maliciously set one or more of the flags of transit packets.

- Loopback flag: an attacker that sets this flag, either in synthetic packets or transit packet, can potentially cause an amplification, since each device along the path creates a copy of the data packet and sends it back to the source. The attacker can potentially leverage the loopback flag for a Distributed Denial of Service (DDoS) attack, as multiple devices send looped-back copies of a packet to a single source.

- Active flag: the impact of synthetic packets with the active flag is no worse than synthetic data packets in which the Active flag is not set. By setting the active flag in en route packets an attacker can prevent these packets from reaching their destination, since the packet is terminated by the decapsulating device; however, note that an on-path attacker may achieve the same goal by changing the destination address of a packet. Another potential threat is amplification; if an attacker causes transit switches to replicate more packets than they are intended to replicate, either by setting the Active flag or by sending synthetic packets, then traffic is amplified, causing bandwidth degredation. As mentioned in Section 5, the specification of the replication mechanism is not within the scope of this document. A specification that defines the replication functionality should also address the security aspects of this mechanism.

Some of the security threats that were discussed in this document may be worse in a wide area network in which there are nested IOAM domains. For example, if there are two nested IOAM domains that use loopback, then a looped-back copy in the outer IOAM domain may be forwarded through another (inner) IOAM domain and may be subject to loopback in that (inner) IOAM domain, causing the amplification to be worse than in the conventional case.

In order to mitigate the attacks described above, as described in Section 7 it should be possible for IOAM-enabled devices to selectively apply the mechanisms that use the flags defined in this document to a subset of the traffic, and to limit the performance of synthetically generated packets to a configurable rate; specifically, network devices should be able to limit the rate of: (i) looped-back traffic (at transit nodes), (ii) replicated active packets (at encapsulating nodes), (iii) packets that are exported to a collector (from either encapsulating nodes or transit nodes), and (iv) synthetically generated packets (at encapsulating nodes).

Furthermore, as defined in Section 4, transit nodes that process a packet with the Loopback flag only add a single data field, and

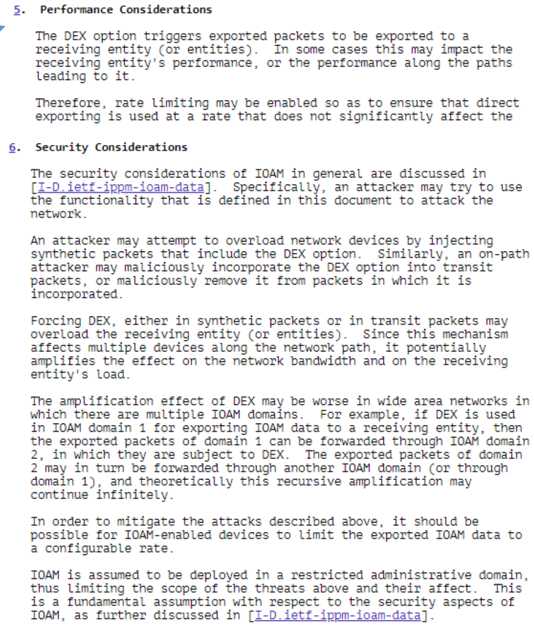
truncate any payload that follows the IOAM option(s), thus significanly limiting the possible impact of an amplification attack.

IOAM is assumed to be deployed in a restricted administrative domain, thus limiting the scope of the threats above and their affect. This is a fundamental assumtion with respect to the security aspects of IOAM, as further discussed in [I-D.ietf-ippm-ioam-data].

Performance considerations

Security considerations

DEX draft



5. Performance Considerations

The DEX option triggers exported packets to be exported to a receiving entity (or entities). In some cases this may impact 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 exporting is used at a rate that does not significantly affect the

6. Security Considerations

The security considerations of IOAM in general are discussed in [I-D.ietf-ippm-ioam-data]. Specifically, an attacker may try to use the functionality that is defined in this document to attack the network.

An attacker may attempt to overload network devices by injecting synthetic packets that include the DEX option. Similarly, an on-path attacker may maliciously incorporate the DEX option into transit packets, or maliciously remove it from packets in which it is incorporated.

Forcing DEX, either in synthetic packets or in transit packets may overload the receiving entity (or entities). Since this mechanism affects multiple devices along the network path, it potentially amplifies the effect on the network bandwidth and on the receiving entity's load.

The amplification effect of DEX may be worse in wide area networks in which there are multiple IOAM domains. For example, if DEX is used in IOAM domain 1 for exporting IOAM data to a receiving entity, then the exported packets of domain 1 can be forwarded through IOAM domain 2, in which they are subject to DEX. The exported packets of domain 2 may in turn be forwarded through another IOAM domain (or through domain 1), and theoretically this recursive amplification may continue infinitely.

In order to mitigate the attacks described above, it should be possible for IOAM-enabled devices to limit the exported IOAM data to a configurable rate.

IOAM is assumed to be deployed in a restricted administrative domain, thus limiting the scope of the threats above and their affect. This is a fundamental assumption with respect to the security aspects of IOAM, as further discussed in [I-D.ietf-ippm-ioam-data].

How Amplification is Addressed in the Drafts – Brief Summary

<table>
<tr><th></th><th>Flag Draft</th><th>DEX Draft</th></tr>
<tr><td rowspan="2">Description of the threat</td><td colspan="2">The amplification problem and its effects are described.</td></tr>
<tr><td colspan="2">Description of potentially worse threats in wide area networks.
More on this on the next slide.</td></tr>
<tr><td rowspan="5">Mitigations</td><td colspan="2">Confined administrative domain.</td></tr>
<tr><td colspan="2">Ability to limit the rate of looped back / exported traffic.</td></tr>
<tr><td>Ability to apply loopback to a subset of the traffic.</td><td></td></tr>
<tr><td>Looped back packets are truncated.</td><td></td></tr>
<tr><td>IOAM trace option is limited to a single data field when using loopback.</td><td></td></tr>
</table>

Pathological Amplification Cases

Thanks Martin Duke for raising these issues.
https://datatracker.ietf.org/meeting/110/materials/slides-110-ippm-sessb-ioam-loopback-direct-export-concerns-00

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.