draft-vyncke-pim-mld-security

Eric Vyncke

Enno Rey

Antonios Atlasis

Agenda

High Level Problem Statement

Main MLD Vulnerabilities

Mitigation approaches as proposed by I-D

High Level Problem Statement

RFC 4861, sect. 7.2.1, uses ambiguous wording to describe relationship between ND and MLD.

Common operating systems have (subsequently?) MLD enabled and active by default.

MLD is susceptible to a number of attacks.

Main MLD Vulnerabilities & Attacks

Downgrading to MLDv1 is possible.

MLD packets can be sent to unicast addresses.

Election (of querier) can easily be won.

Host enumeration & OS fingerprinting

Flooding of MLD messages / DoS of devices

Amplification attacks (link-local)

Mitigation Approaches

`MLD guard` feature (similar to RA guard).

Discard/don't process MLD packets sent to unicast addresses (=> updating RFCs 2710/3810).

Set hop-limit of MLD packets to 255 and discard packets with hop-limit less than 255.

The above will not only mitigate MLD based attacks but also contribute to overall stability & performance.