Security Threats of OLSRv2

draft-clausen-manet-olsrv2-sec-threats-01

T. Clausen, U. Herberg, J. Yi

IETF 91

Objective

- Identify vulnerabilities without minimum security mechanisms ([RFC 7183])

- Which vulnerabilities mitigated by [RFC 7183]?

Draft Structure

RFC 7186

Topology Map Acquisition

Effective Topology

Inconsistent Topology

Inherent OLSRv2 resilience

RFC 7183 resilience

Vulnerabilities

Mitigation of vulnerabilities

Vulnerabilities

- Topology map acquisition
  - Attack on jittering, hop-count and hop-limit attacks, etc..
- Effective Topology
  - In correct forwarding, wormholes, sequence number attacks, etc.
- Inconsistent Topology
  - Identity spoofing, link spoofing

Mitigation of vulnerabilities

- Inherent OLSRv2 resilience
  - Sequence number for freshness
  - Ignoring uni-directional links
  - Rejecting certain invalid control messages
- Resilience by using RFC 7183
  - Shared key between all routers
  - Reject messages not properly singed

What's Next

- Target:
  - Informational RFC
- Histories
  - -00 submitted July 22, 2014
  - Briefly introduced at IETF'90
  - -01 submitted August 12, 2014
- Ready for Working Group Adoption
  - Comments appreciated
  - Solicit call for adoption