SMF & OLSRv2 Sec Threats
draft-yi-manet-smf-sec-threats
draft-clausen-manet-olsrv2-sec-threats

Jiazi Yi

Ulrich Herberg

Thomas Clausen

Motivation

- In the IESG Evaluation of RFC7186 (NHDP Sec Threats), our local-friendly SEC AD said:

2013-06-11	05	Stephen Farrell	[Ballot comment] I like that you've done this and have just a few comments and some nits:

- But, more to the point, as part of the process of RFC6130, RFC6622, RFC7181, RFC7882, RFC7183, etc., we went through the process of understanding what threats there were against the protocols (and their constituent parts) so as to try to guard against them.

- In the vein of RFC7185, offer these internal working notes up for the community, as **INFORMATIONAL** documents.

- Perhaps even more fundamental: our belief that security is not just an afterthought to tack on in a MANET environment, but a core design requirement given the potential deployment space.

The Meat Of The Matters

- OLSRv2 [RFC7181] and SMF [RFC6621] both use NHDP [RFC6130] -- therefore, RFC7186 (NHDP Sec Threats) remains relevant to also these documents.

- SMF [RFC6621] introduces new bits and pieces, notably Relay Set Selection, and Duplicate-Packet-Detection -- which, in turn, introduce attack vectors of their own:
  - draft-yi-manet-smf-sec-threats is about those, as well as how the threats identified in RFC7186 affect SMF.

- OLSRv2 [RFC7181] introduces TC messages, MPRs, -- which, in turn, introduce attack vectors of their own:
  - draft-clausen-manet-olsrv2-sec-threats is about those, as well how the threats identified in RFC7186 affect OLSRv2.

draft-yi-manet-smf-sec-threats (I)

- Impact of threats on RFC6130 - in part, see RFC7186.
- Duplicate Packet Detection:
  - Pre-activation attack (I-DPD)
    - Generate IP datagrams that will cause future legitimate IP datagrams to be rejected.
    - "Pre-play" future sequence numbers.
  - De-activation attack (I-DPD):
    - Modify packets so as to cause already seen/forwarded IP datagrams to be retransmitted.
    - Modify sequence number in forwarded packets to make them look new.
  - Hash Assist Value (H-DPD):
    - Actually, a "hint" to a malicious router that a hash value collision is not just possible, but the source has identified that it is highly likely.
    - Attacker simply "strip out the HAV from a forwarded IP datagram.

draft-yi-manet-smf-sec-threats (II)

- Relay Set Selection Threats:
  - Obviously, dependent on the relay set selection algorithm in use, but some generalities can be stated.
  - Essentially Priority, link-spoofing, identity-spoofing attacks.
  - Link-spoofing: declare a high connectivity to 2-hop neighbors, thereby preventing legitimate relays from being selected.
  - Identity-spoofing + Priority/willingness: force relay selection.
- Do look at the document for specifics.

Next Steps

draft-yi-manet-smf-sec-threats-00

- Submitted before the deadline.
- Therefore, we expect that you all have read, memorized it, and (if you have kids) recited it nightly, as their bed-time story.
- Goal of rapid process towards INFORMATIONAL.
- Of course, we'd like even more to get your constructive feedback on the document.
- **We hereby ask the WG chairs to call for WG adoption of this document.**

draft-clausen-manet-olsrv2-sec-threats-00

- Did not submit, before the deadline
- **Therefore we did not ask for a slot to present it, and we won't present it** - but, it's now out there (since Monday) and this just is an announcement of its existence.
- Similar in spirit and structure to draft-yi-manet-smf-sec-threats and RFC7186.
- Would like to ask you to read it, and give constructive feedback.
- Will ask the WG chairs to **call for WG adoption in a month or so**, once y'all have had time to read it.