Secure Neighbor Discovery

By-
Pradeep Yalamanchili
Parag Walimbe
Overview

- Neighbor Discovery Protocol (NDP)
- Main Functions of NDP
- Secure Neighbor Discovery (SEND) Overview
- Types of attacks.
NDP

- Nodes on the same link use NDP to discover each other presence and link-layer addresses, to find routers.
- It is used by both hosts and the routers.
Main Functions of NDP

- Router Discovery (RD).
- Redirect Function.
- Address Auto configuration.
- Duplicate Address Detection (DAD).
- Address Resolution Function.
- Neighbor Unreachability (NUD).
NDP-message

- It includes an NDP message header, consisting of an ICMPV6 header and ND message specific data and zero or more NDP-Options.

<table>
<thead>
<tr>
<th>IPV6 Header</th>
<th>ICMPV6 Header</th>
<th>ND message specific data</th>
<th>ND message (options)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Header (=58) (ICMPV6)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Secure Neighbor Discovery Overview

- A set of new NDP options is introduced to secure various functions of NDP.
- This specification introduces:
  - new options.
  - Authorization Discovery Process (ADD).
  - Address ownership proof mechanism.
Secure Neighbor Discovery Overview (cntd..)

- The main components involved are as follows...
  - certification paths, anchored on trusted parties are expected to certify the authority of routers.
  - Host must be configured to a trust anchor.
  - No need to go for RD messages.
Secure Neighbor Discovery Overview (cntd..)

- Cryptographically Generated Addresses are used to make sure the sender of a ND message is the owner of the claimed address.
- It also allows a node to use non-CGAs with certificates that authorize their use.
- RSA signature Option allows the Public-key based signatures to be attached to NDP messages.
- the RSA signature option, is used to protect all messages relating to ND and RD.
Secure Neighbor Discovery Overview (cntd..)

- To Prevent replay attacks, two ND options Timestamp and nonce are introduced.
- Timestamp is to make sure that unsolicited advertisements and redirects have not been replayed.
- Nonce is to make sure that an advertisement is fresh response to a solicitation sent earlier by the node.
Types of attacks.

- Neighbor Solicitation / Advertisement spoofing.
- Neighbor unreachability detection failure.
- Duplicate address detection DoS attacks.
- Router solicitation and advertisement attacks.
- Replay Attacks.
- Neighbor discovery Dos Attack.
- Attacks against SEND itself.
Neighbor Solicitation / Advertisement spoofing.

- Attacker approaches router with router solicitation, router inserts a entry in the neighbor cache.

- Now a node performing DAD for that address stops it because it gets a neighbor solicitation for same address and feels that it is a conflict.
Neighbor Solicitation / Advertisement spoofing.

**Solution**
SEND requires nodes to send solicitation messages with RSA signature CGA options, CGA source address which the router can verify and so the neighbor cache binding is correct.
Neighbor Unreachability Detection Failure.

- An attacker can send a neighbor unreachability detection failure message. SEND counters it by requiring that a node responding to neighbor solicitations sent as a neighbor unreachability detection probes include an RSA signature option and a proof of authorization to use the interface identifier in the address being probed. If these prerequisites are not met the node performing Neighbor unreachability discards the responses.
Duplicate address detection DoS Attacks

- If a node is performing Duplicate Address Detection then an attacker may send a message to node stating that it has the address. This is countered by SEND in the following way. Neighbor advertisements that are sent as responses to DAD include an RSA signature option and proof of authorization to use the interface identifier. If this is not found then node discards the messages.
Router solicitation and advertisement attacks

- An attacker may send router advertisement to a node and thus cause harm to node to avoid this. SEND requires router advertisement to have a RSA signature that is calculated using the node's public key. Thus only node can access it and use it. The router proves its authorization by showing a certificate containing the specific prefix that it is allowed or permitted to route.
Replay Attacks

- Replay attacks are averted using SEND. SEND uses a nonce and timestamp to implement a challenge response mechanism.
- But a window of vulnerability exists till time stamp expires.
- Time synchronization can be tampered with thus extending the life of timestamps.
- So proper security measures must be taken against tampering of time synchronization.
Neighbor discovery DoS attacks.

- An attacker may bombard the router with packets for fictitious address on the link, causing the router to busy itself by performing neighbor solicitation for addresses that do not exist.

- SEND does not address this problem as it can be handled by intelligent router management.
Attacks against SEND itself

- Flooding not prevented.

- Authorization delegation discovery may be vulnerable to DoS. Attacker may send large number of certification path to be discovered to the router.

- Attacker may also send large number of certification paths to the node forcing node to spend much time on processing them.
CONCLUSION.

- Thus we have seen that SEND protocol is used to Secure NDP off flaws and we have also seen the Security threats that SEND deals with
References

- RFC – 3971
Contact

- ypradeep4u@yahoo.com
- Paragwalimbe@yahoo.com