An Analysis of Selected IPv6 Network Attacks

**Attacks**

- **Rogue Router Advertisement MitM**
  - Default gateway: <Router’s IP>  
  - <Attacker’s IP>
  - **Victim**
  - **Attacker**
  - **Valid RA**
  - **Rogue RA**

- **Duplicate Address Detection DoS**
  - Neighbor Solicitation Target: <Victim’s tentative IP>
  - Neighbor Advertisement Target: <Victim’s tentative IP>

- **Neighbor Cache Poisoning MitM**
  - Alice’s Neighbor Cache
    - <Bob’s IP>  
    - <Attacker’s MAC>
  - Bob’s Neighbor Cache
    - <Alice’s IP>  
    - <Attacker’s MAC>

**Defense**

- **Neighbor Discovery Protocol Inspection**
  - Configured on a switch
  - Only trusted ports are allowed to forward Router Advertisements
  - Forwarding of Neighbor Advertisements based on a binding table containing valid IPv6-to-MAC mappings.

**Bypassing NDP Inspection**

An attacker is able to bypass NDP inspection by splitting an original RA message into more IPv6 fragments. A switch processes them individually, but is unable to determine the first octet of RA in the last fragment. Since NDP inspection is usually implemented in hardware, an attacker can use many extension headers in order to exhaust all the allocated resources, thus preventing the switch from recognizing malicious NDP message.

**Packet fragmentation**

1. Fragment
   - IPv6 HEADER
   - FRAGMENT HEADER
   - DESTINATION OPTIONS HEADER
2. Fragment
   - IPv6 HEADER
   - FRAGMENT HEADER
   - DESTINATION OPTIONS HEADER
   - ROUTER ADVERTISEMENT

**Extension Headers**

- IPv6 HEADER
- DESTINATION OPTIONS HEADER
- DESTINATION OPTIONS HEADER
- ... ROUTER ADVERTISEMENT

**Summary**

- Tested on Cisco and H3C devices
- Created tool to attack presented vulnerabilities of Neighbor Discovery Protocol
- All of the tested devices are vulnerable – it is possible for an attacker to easily cause a DoS in a local network
- Administrators are currently unable to prevent from these attacks

**Author:** Jozef Pivarník  
**Supervisor:** Ing. Matěj Grégr

---

BUT FIT 2013