Vulnerabilities in IPv6
Project ID: 6778
Project's Summary

Supervisor: Mordechai Hagiz

Students: Jamal Tannous
Salah Kadry

The project's goal was to find/ research vulnerabilities in IPv6 and simulate them while suggesting mitigation techniques.

While working on the project we have researched and learned a lot of "fascinating" studies and material regarding IPv6.

We also reviewed some interesting platforms/ websites/libraries that deal with this topic , eg. shodan.io, THC, Linux Mint Forum, Imperva, Black Hat Conference...

Finally we simulated three attack scenarios:

1) Man in the middle with spoofed ICMPv6 router advertisement - an attack that exploits the Neighbor discovery protocol in IPv6 based networks as the attacking node announces itself as the router with the highest priority in the network, which causes all data traffic to pass through it.

We simulated the attack using two virtual machines, as one Kali Linux based machine used Scapy to perform the attack, and the other Ubuntu based machine was the victim.

2) TCP (over IPv6) Syn Flood - an attack that exploits the three way handshake in the TCP protocol.
The attacker keeps the connection "half open" as it sends every fixed interval a TCP-SYN to the server on a specific port but does not reply to the server's SYN-ACK.
As a mitigation technique we used SYN-Cookies.
This can be used as a DoS or DDoS attack.
We chose to simulate the attack because of a certain thread in the Linux Mint forum which mentioned that SYN-Cookies failed to be effective in a certain scenario on IPv6 based networks, while operating without a problem on IPv4 based networks.

3) Copycat Attack on Low Power and Lossy Networks - this is an attack that exploits a weakness in the RPL protocol for IoT devices on Low Power and Lossy Networks.
Mainly the attacker exploits a control message called DIO and sends it multiple times upon capturing it from a legitimate neighbor.
This kind of attack Leads in decrease in Packet Delivery Ratio (PDR) and increases Average End-to-End Delay (AE2ED) of the underlying network.

We simulated the attack using a C++ simulation that we programmed from scratch, while building a simulation of the network and simulating legitimate messages and the attack itself, finally we proposed a mitigation technique and tested it.

Notable:

IPvSeeYou - We found this attack, which targets household CPE routers, which use a form of legacy IPv6 address assignment called EUI-64.

This attack exploits a certain relation between the router's EUI-64 address and the WiFi's BSSID to try and geo locate the network.