Security in IPv6 enabled home networks: Are we ready yet?

Nikhitha Kishore, McAfee
PNSQC 2021
Agenda

• IPv6 Overview
• IPv6 Features
• Security attacks in IPv6 networks
• Smart home eco systems and IPv6
• IPv6 best practices for smart home network
IPv6 overview

- IPv6 is the most recent version of the Internet protocol.
- IPv6 uses a 128-bit address, theoretically allowing $2^{128}$, or approximately $3.4 \times 10^{38}$ addresses.
- Why IPv6?
  - IPv4 is only 32 bits long and offers around $4,294,967,296$ ($2^{32}$) addresses. The address space offered by IPv4 is saturating.
  - IPv4 on its own does not provide any security feature.
  - IPv4 enabled clients can be configured manually or they need some address configuration mechanism. It does not have a mechanism to configure a device to have globally unique IP address.
IPv6 Features

- Larger Address Space
- Simplified Header
- End-to-end Connectivity
- Auto-configuration
- Faster Forwarding/Routing
- IPSec
- Extensibility
Security attacks in IPv6

- Reconnaissance attacks
  - DNS reverse zone scanning
  - DNSSEC Zone Reconnaissance
- Extension Header (EH) attacks
- Neighbor Discovery Protocol (NDP) attacks
- DHCPv6 attacks
- Security attacks due to the IPv6 Transition mechanisms
Smart Home Networks

- The Internet of Things/IoT have created new opportunities for cybercriminal to infiltrate into home networks. Consider a few scenarios:
  - An attacker gaining access to the baby monitor for spying.
  - An attacker gaining access through an IoT device for a ransomware attack thereby demanding a ransom to get the user’s systems working again.
  - An attacker altering the firmware update URL of a smart thermostat to his system’s web address to understand when the home user is away from home.
IPv6 best practices for smart home network

- Virtual Private Network
- Host based firewalls
- Network based firewalls
- Next Generation Firewall (NGFW)
- Separate network for IoT devices
<table>
<thead>
<tr>
<th>IOT Devices</th>
<th>VPN</th>
<th>Host based firewalls</th>
<th>Network-based firewalls</th>
<th>NGFW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thermostat/Baby monitor/Alexa/Google Home</td>
<td>Cannot be installed</td>
<td>Most IoT devices don't have the support</td>
<td>Must for all IoT devices since endpoint protection is rare.</td>
<td>Enable IPv6 blacklist for botnet</td>
</tr>
<tr>
<td></td>
<td>Can connect to VPN enabled gateways with IPv6 support</td>
<td>Need to add IPv6 firewall rules if the device supports</td>
<td>Clone IPv6 rules for the existing IPv4 rules</td>
<td>Enable IPv6 SSL interception</td>
</tr>
</tbody>
</table>

| Office Devices - Laptop/Desktop/Macbooks | Must be installed. Use IPv6 supported VPN software | Must be configured. Clone IPv6 rules for the existing IPv4 rules | Must for all office devices to disable port forwarding via SSH/Telnet. Clone IPv6 rules for the existing IPv4 rules | Enable IPv6 blacklist for botnet |

| Mobile Devices (connected to LTE) | Must be installed. Use IPv6 supported VPN software | Cannot configure host-based firewall rules. Can install endpoint security solutions like Web scanner, web protection, content filtering software etc. Need to install endpoint security apps with IPv6 support. | Must for all smartphones since smartphones could have been vulnerable since they move in-out of the network. Clone IPv6 rules for the existing IPv4 rules | Cannot apply rules if the device moves out of the network. Enable IPv6 blacklist for botnet while inside the network |

| | | | | Enable IPv6 SSL interception while inside the network |

| | | | | Enable content filtering while inside the network |
Thank You!