Development of a suite of IPv6 vulnerability scanning testes using TTCN-3 language

Igor Cunha Teixeira
Adriano Leal
Development of a suite of IPv6 vulnerability scanning tests using TTCN-3 language

Igor Cunha Teixeira
Adriano Leal

IPT – Institute for Technological Research of the State of São Paulo
CIAM – Center for Information Technology Automation and Mobility
Introduction

- Internet of Things Age
- IPv6 protocol running on the Internet.
  - It takes much more than the few 4.3 billion IPv4 addresses available to connect 50 billions devices, besides other requirements such as security and mobility.
  - With the growing popularity of IPv6, new forms of attack will arise and new vulnerabilities.
  - Many research groups involved in discover vulnerabilities on IPv6.
Introduction

- Most of the existing tools use programming languages like C, Java and Python instead of a specific language to build tests, which reduces its extensibility and maintainability.

- Passive tests
  - Observe the system behavior

- Active tests
  - Stimulate the system to present symptomatic behavior

- Development of a prototype that simulates and detects Denial of Service attacks to ICMPv6 protocol
IPv6 protocol

IPv6 features:

• Provide billions of unique addresses to each person;
• Stateless IPv6 address configuration;
• Neighbor Discovery Protocol
• Multicast;
• IPSec;
• Extensibility (extension headers)
IPv6 security vulnerabilities

- National Vulnerability Database – NVD
  - In 2017, the most attacks are DoS and DDoS attacks
- Kaspersky Lab’s cyberthreat research and reports
  - DDoS attacks per day ranged from 296 (24 July) to 1508 (26 September) in 2017
    - The peak numbers were registered on 27 July (1399) and 24 September (1497)
Testing and Test Control Notation Version 3 (TTCN-3)

“There are no practical limits to the extent that tests or test systems can be adapted to users’ needs” — ETSI
TTCN-3 features

- Specially designed for many types of testing;
- Independent of technology, operation system and implementation domain;
- Extensible;
- Scalable;
- Allows reusability of a existing code structure;
- Dynamic test configuration;
- Rich typing system;
- Powerful matching mechanisms;
- Multiple test components;
Architecture of test suite

- **Attack Simulation Module**
  - Stimulate SUT
- **Vulnerability Detection Module**
  - Analyzing the behavior of the SUT
- **Report Generation Module**
  - Generate records of detected vulnerabilities and suggest improvements to mitigate
Proof of concept validation

• IPv6 vulnerability scanning tests:
  • Multicast traffic amplification attack (Smurf attack);
  • Denial of Service Attack in IPv6 Duplicate Address Detection (DoS SLAAC)
Proof of concept development

• Software
  o TTworkbench Professional version 18.

• Library
  o LibCommon v.1.4.0
    ➢ Type and Subtype definitions;
    ➢ Test component synchronization mechanisms;
    ➢ Timers.
  o LibIPv6 v.1.0
    ➢ RFC-based TTCN-3 definitions;
    ➢ Templates;
    ➢ Functionalities of Sending and Receiving.
• Test Environment Multicast Traffic Amplification Attack (Smurf)
Testbed

- Debian Linux running Router Advertisement Daemon (RADVD);
- Windows 7 running the tests;
- Ubuntu Linux running iftop and Nmap software;
- Implementation Under Test (IUT)
  - Windows 7
- 3 Attackers
  - 1 Ubuntu Linux
  - 2 Debian Linux
Smurf attack execution report
<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>Information about the devices</th>
<th>Echo Reply messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8::1dfe:e354:2710:77f7</td>
<td>Microsoft Windows XP SP3 32 bits</td>
<td>28</td>
</tr>
<tr>
<td>2001:db8::204:ff:ef5:11b4</td>
<td>Lexmark T640 printer</td>
<td>28</td>
</tr>
<tr>
<td>2001:db8::20c:29ff:fe3:949c</td>
<td>Linux 2.6.32 - 3.2</td>
<td>28</td>
</tr>
<tr>
<td>2001:db8::6ab5:99ff:fe56:41c1</td>
<td>HP LaserJet P4015 printer</td>
<td>28</td>
</tr>
<tr>
<td>2001:db8::a00:27ff:fe24:41d2</td>
<td>Linux Debian GNU/Linux 8 3.16.0-4-586</td>
<td>32</td>
</tr>
<tr>
<td>2001:db8::a00:27ff:fe98:1f17</td>
<td>Linux Ubuntu 16.04.2 LTS 4.4.0-62 32 bits</td>
<td>32</td>
</tr>
<tr>
<td>2001:db8::a00:27ff:fe4:ff37</td>
<td>Linux Debian GNU/Linux 8 3.16.0-4-586</td>
<td>32</td>
</tr>
<tr>
<td>2001:db8::d9d7:c01f:b28:982e</td>
<td>Host Linux 2.6.32 - 3.2</td>
<td>6</td>
</tr>
<tr>
<td>2001:db8::f8bc:2338:2d19:6730</td>
<td>Microsoft Windows XP SP3 32 bits</td>
<td>29</td>
</tr>
<tr>
<td>2001:db8::f5:bff:db31:cd84</td>
<td>Microsoft Windows XP SP3 32 bits</td>
<td>28</td>
</tr>
</tbody>
</table>

After analyzing the captured packets, it was seen that only the non-compliance devices to RFC 4443 responded to Echo Request messages with Echo Reply.

At least 3000 Echo Request messages and 430 Echo Reply messages were travelling through the network.
<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Test Case</th>
<th>Test Purpose</th>
<th>Verdict</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-02-11 17:57:49.628</td>
<td><strong>AtsIpv6_Icmpv6Functions_TestsCases.TC_VUL_SMURF6</strong></td>
<td>Detect multicast traffic amplification vulnerability or Smurf attack</td>
<td>pass</td>
</tr>
<tr>
<td>2018-02-11 17:58:56.581</td>
<td></td>
<td><strong>=&gt; Solutions:</strong> 1) All IPv6 Nodes MUST implement RFC 4443, Internet Control Message Protocol (ICMPv6); 2) Follow the recommendations defined by IETF for filtering ICMPv6 Messages (RFC 4890)</td>
<td></td>
</tr>
</tbody>
</table>

Report with the detected vulnerability and suggestions of improvement to mitigate such loophole.
Conclusion

- Primer advantage of using TTCN-3:
  - Look and feel of regular programming languages like Java, Python and C but without their complexity
  - Concentrates on what to test and not on how.
- The proof of concept showed that TTCN-3 could be used to detect vulnerabilities and penetration tests;
- The code in TTCN-3 is highly reusable, then a considerable number and types of vulnerabilities tests may be shared and deployed together.
## Conclusion

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Conformance RFC 4443</th>
<th>Non-Conformance RFC 443</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS Windows 7 Professional 64-bit (version 6.1.7601 with Service Pack 1)</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows XP SP3 32-bit</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Linux Debian GNU / Linux 8 3.16.0-4-586</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Linux Ubuntu 16.04.2 LTS 4.4.0-62-generic 64-bit</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Lexmark T640 LS Firmware printers STN234</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>HP LaserJet P4015 Firmware 04.270.2)</td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>
THANK YOU!!

igort@ipt.br
https://www.ipt.br/EN