IPv6 Security Activities in Japan

Tomohiro Fujisaki
NTT/IPv6 Promotion Council
27th February 2014
Outline

- Introduce activities related to IPv6 security in Japan
  - Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
  - IPv6 Technical Verification Consortium
  - JAPAN Network Security Association (JNSA)
  - IPv6 Security Working Group, IPv6 Promotion Council in Japan
ACTIVITIES OF JPCERT/CC
IPv6 related activities in JPCERT/CC 1/2

• In 2012, conducted survey about IPv6 security risks based on existing documents (RFCs, internet drafts and so on) and studied how to tackle with such risks
• Verified actual equipment (routers, firewalls and so on)
• Output:
  – Report of security risks related to IPv6 protocol specification
  – Testing results about IPv6 security risks
IPv6 related activities in JPCERT/CC 2/2

• In 2013, ‘Report of security risks related to IPv6 protocol specification’ was updated.

• Based on that updated report, continue conducting verification of actual equipment
  – Create VM images including various tools to check IPv6 security risks they choosed, and ask venders to check their products.
  – Plan to publish their check results.
Example of test items

<table>
<thead>
<tr>
<th>No</th>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2013-ipv6sec-0001</td>
<td>Type 0 Routing Header processing</td>
</tr>
<tr>
<td>2</td>
<td>2013-ipv6sec-0002</td>
<td>DoS Attack by Hop-by-hop option headers</td>
</tr>
<tr>
<td>3</td>
<td>2013-ipv6sec-0003</td>
<td>Implementation issues on jumbo payload option processing</td>
</tr>
<tr>
<td>4</td>
<td>2013-ipv6sec-0004</td>
<td>Overlapping fragments</td>
</tr>
<tr>
<td>8</td>
<td>2013-ipv6sec-0008</td>
<td>DoS attack by tiny fragment packets</td>
</tr>
<tr>
<td>10</td>
<td>2013-ipv6sec-0010</td>
<td>DoS attack by first fragment packet</td>
</tr>
<tr>
<td>11</td>
<td>2013-ipv6sec-0011</td>
<td>DoS attack by atomic fragment packets</td>
</tr>
<tr>
<td>13</td>
<td>2013-ipv6sec-0013</td>
<td>Attack by predicting fragment ID</td>
</tr>
<tr>
<td>14</td>
<td>2013-ipv6sec-0014</td>
<td>DoS attack by ND packets</td>
</tr>
</tbody>
</table>
IPv6 Technical Verification Consortium
IPv6 Technology Verification Consortium

IPv6 experiment working group

- IPv6 Testbed
  - In Microsoft Technology Center

- Attack Simulation

- IPv6 Appliance Vendor
  - IPv6 Appliance Vendor
  - IPv6 Appliance Vendor

- NICT IPv6 Security Test tool

- Extraction and experimentation of known / unknown security issues
- Consideration of countermeasures

Industry / Standards body

Members / Other Organizations
Attack Scenario 1

- DoS attack against Router by sending enormous number of packets with RH0 (Routing Header type 0) option

**Possible Result**
- The packets lead congestion between the nodes and consuming valuable router processing and forwarding resources, potentially lead to a DoS attack.

**Experimental Result**
- The attacks failed on all targeted devices.
- RFC5095 has been already standardized in IETF, which specifies for routers to ignore RH0 packets.
Packet amplification DoS attack by forged multicast packets

**Possible Result**
- ICMP error messages (ICMP Parameter Problem) from all nodes on the same network and potentially lead DoS attack against B.

**Experimental Result**
- Packet amplification (ICMP error messages) were observed.
- The behavior for processing multicast packet is defined by RFC and the nodes are just following the RFC. → problem of protocol

**Countermeasure**
- Apply rate limitation of number of ICMP messages on each node
Attack Scenario 3

- Data sniffing by forged RA (Router Advertisement)

Attack Scenario
- Attacker (Y) sends forged RA to B, which specifies Y as B’s default router

Possible Result
- All traffic from B to A are transmitted through attacker (Y) so that Y can sniff the data.

Experimental Result
- The attack was succeeded.
- It is difficult to detect this attack because B and A can keep their communication under the attack situation.

Countermeasure
- SeND (Secure Neighbor Discovery: RFC3971), RA Guard (RFC6105) is proposed, which authenticate router so that only legitimate router can publish RA message in the network.
JAPAN Network Security Association (JNSA)
Activities of JNSA IPv6 Security WG

• Just re-established in end of 2012
• Has been conducting ‘observation’ based activities
  – Set up publicly accessible servers with same contents
    • IPv4 only, IPv4/IPv6 dual stack, IPv6 only
    • At first, target service (protocol) is http, however, plan to add other services such as ntp.
  – Set up IDS and WAF (monitoring nodes) and monitor access to those servers

Monitoring is ongoing, and results will be reported this year.
IPv6 Promotion Council in Japan (IPv6 PC)
Recent Activities of IPv6 Security WG in IPv6 PC

- Publish a report ‘IPv6 security guidelines for constructing public servers’
- Drafting ‘6SLoC’ (IPv6 Security List of Considerations)
  - Summarize IPv6 security considerations discussed in several organizations
  - Will publish soon.
Three NW models for IPv6 public servers

Parallel stack model

Dual stack model

Translator model
# 6SLoc (IPv6 Security List of Considerations)

<table>
<thead>
<tr>
<th>April-01</th>
<th>System</th>
<th>IPv4</th>
<th>IPv6</th>
<th>MAC</th>
<th>MACv4</th>
<th>MACv6</th>
<th>IPv4 MTU</th>
<th>IPv6 MTU</th>
<th>Port</th>
<th>LP</th>
<th>IPv4v6</th>
<th>IPv6v4</th>
</tr>
</thead>
<tbody>
<tr>
<td>April-02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-03</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-04</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-05</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-06</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-08</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-26</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>April-27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In Japan, several organizations have been discussing IPv6 security related issues.

IPv6 Security WG in IPv6 PC will publish a list of security issues which has discussed in those organizations.
Questions?
Overview of JPCERT/CC

- Japan Computer Emergency Response Team Coordination Center
  - Founded in 1996
  - An independent, non-profit organization
  - National CSIRT (Computer Security Incident Response Team)
  - Coordination center

- JPCERT/CC, as a national CSIRT, monitors computer security incidents at a national level, identifies and handles incidents that could affect the economy and critical infrastructures, and warns critical stakeholders and the nation about computer security threats.

- JPCERT/CC, as a coordination center, provides technical support in response to computer security incidents through coordination with other local and overseas CSIRTs.
Overview of JPCERT/CC
- 3 pillars and 4 foundations -

**Prevent**
- Vulnerability Information Handling
  - Coordinate with developers on unknown vulnerability information
  - Secure Coding

**Monitor**
- Information gathering / analysis / sharing
- Internet Traffic Monitoring
  - Alerts / Advisories

**Respond**
- Incident Handling
  - Mitigating the damage through efficient incident handling
  - Information sharing to prevent similar incidents

---

**Early Warning Information**
Information sharing with critical infrastructure enterprises, etc.

**CSIRT Establishment Support**
Capacity building for internal CSIRTs in enterprises / overseas national CSIRTs

**Artifact Analysis**
Analysis on attack methods / behavior of malware (unauthorized program)

**International Collaboration**
Collaboration with overseas organizations for smoother handling of incidents and vulnerabilities
IPv6 Technology Verification Consortium

- IPv6 Technical Verification Consortium (http://ipv6tvc.jp/)
- Objectives
  - July 28th, 2010 - National Institute of Information and Communications Technology (NICT), Microsoft Japan and other 8 companies have established an "IPv6 Technical Verification Council" for verifying the security and interoperability of IPv6 technology. This consortium is organized to test and come up with solutions against over 40 security (threats and vulnerabilities) and interoperability issues identified through the NICT research activities. Microsoft Innovation Center Japan will take key position to host all testing and organize activities, and outcome will be shared to communities broadly to improve security and interoperability of IPv6.

- Activities of the Consortium
  - Consortium members inspect vulnerabilities of their IPv6-enabled products and solutions such as network devices (e.g., router, switch, NAT, load balancer), security appliances (e.g., IDS, IPS, Firewall) and network service equipment (e.g., proxy server, DHCP server, Web server, DNS server) with respect to the IPv6 security issues that have been studied in NICT (National Institute of Information and Communications Technology). Consortium members also share all of the discovered vulnerabilities from the inspection with each other and devise countermeasures against them, so that the consortium can contribute to make more secure and stable IPv6-based networks. The direction of the activity will be decided under consensus of all consortium members and its main goal is to make the future IPv6-based Internet more secure and stable.
IPv6 Technology Verification Consortium
Participating Organizations
## Japan Network Security Association (JNSA) - Overview -

- **Name**: Specified Non-profit Organization (NPO) Japan Network Security Association (JNSA)
- **Established**: April, 2000 (Established as a voluntary association, and later granted the status as a specified non-profit organization (NPO) in 2001.)
- **Membership**: 140 member companies (as of April 2013), mostly information security vendors
- **Address**: Headquarters: Nishi-shinbashi, Minato-ku, Tokyo
  Western Japan Branch: Nishi-Nakashima, Yodogawa-ku, Osaka
- **Email**: sec@jnsa.org

### Directors

- **President**: Hidehiko Tanaka (President/Professor, Graduate School of Information Security, Institute of Information Security)
- **Vice Presidents**: Koji Nakao (KDDI CORPORATION)
  Masakazu Takahashi (Microsoft Japan Co., Ltd.)
- **General Secretary**: Masahiro Shimomura (dit Co., Ltd.)
Aim of JNSA

Rapid Diffusion of Networks
Expansion of the Internet (anyone, anywhere)
User base expanded to include general public
(beginners to professionals)
Everything is on the network (internal data, confidential data, etc.)

Secure Networked Society

Users

Vendors

Awareness promotion, Information provision

Technology advancement, Information exchange, Problem-solving

Copyright (C) 2000-2013 NPO Japan Network Security Association
IPv6 Promotion Council in Japan

- IPv6 Promotion Council (IPv6 PC)
  - Aims
    1. Pursue an international leadership role for Japan in the Internet field
    2. Develop rich human resources for continuous development of a new infrastructure for a high information society
    3. Promote new business and vitalize existing business in hardware, software and service of networks and devices

Working Groups in IPv6 PC

Basic Strategy Steering Group

Certification WG
- Core SWG
- IPsec SWG
- MIPv6 SWG
- MLDv2 SWG
- SIP SWG
- DHCPv6 SWG

IPv4/IPv6 Coexistence WG
- Service Transition SWG
- IPv6 Home Router SWG
- v6fix SWG
- IPv6 Application SWG
- IPv6 Deploy SWG

FMC v6 Platform WG

Business Testbed WG

Digital Information Appliance v6 Platform WG

Business Learning WG

Security WG

Business Exchange WG

New Internet Technology & IPv4 address shortage WG