Goal
Check if ISPs in the world follow the egress filtering practice without the need to deploy agents within the ISP network.

In practice...
Use IPv4-IPv6 transition mechanisms in order to IPv4 source spoof.

Agent-less IPv4 Spoofing Final Presentation
Daniel Galante
Agent-less IPv4 Spoofing Final Presentation
Daniel Galante
Goal

Check if ISPs in the world follow the egress filtering practice without the need to deploy agents within the ISP network

In practice...

Use IPv4-IPv6 transition mechanisms in order to IPv4 source spoof
A unique string of numbers separated by periods that identifies each computer attached to the Internet

IPv4
- Most common version today
- Designed in 1981 by the IETF
- Consists of 32-bit addresses
  Example: 192.0.233

IPv6
- Next IP generation
- Consists of 128-bit addresses
  Example: 2001:0db8:0000:0000:0000:0000:0000:0000

Address Space Exhaustion
- Some issues:
  - Limited address pool
  -难于分配IPv4 addresses
  - Each one is less than 64 device
    solutions: NAT, private network addressing, etc.

Long-term Solution
To Address Space Exhaustion
- Some ideas:
  - Approaches to IPv4 addressing
  - More than 4294967296 addresses
  - Almost 32 billion addresses for each of
    the 32 billion people of the

More improvements of IPv6
- Large management of networks should
  to access via an aggregation
- End-to-end communication support of host
  addresses
- Support for more than a half trillion
  people
IPv4

- Most common version today
- Designed in 1981 by the IETF
- Consists of 32-bit addresses
  Example: 192.0.3.23
### IPv4 Packet

<table>
<thead>
<tr>
<th>4 Bits</th>
<th>8 Bits</th>
<th>16 Bits</th>
<th>24 Bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>IHL</td>
<td>Type of Service</td>
<td>Total Length</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identification</td>
<td>Flags</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Time to Live</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source IP Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination IP Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP Options</td>
<td>Padding</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>

---
Address Space Exhaustion

Some numbers...
- Poorly allocated: Only 14% are utilized
- Provides approx. 4.3 billion addresses
- Each one of us has more than one device

Solutions: NAT, private network addressing, etc.
IPv6

- Next IP generation.
- Consists of 128-bit addresses.
  Example:
  2001:0db8::0042:1000:8a2e:0370:7334
Long-Term Solution
To Address Space Exhaustion

Some more numbers:
  • Approximately $3.4 \times 10^{38}$ addresses.
  • More than $7.9 \times 10^{28}$ times as many as IPv4
  • About $4.8 \times 10^{28}$ addresses for each of the 7.1 billion people alive
More improvements of IPv6

- Easier management of networks thanks to autoconfiguration capabilities
- End-to-end connective integrity (direct addressing)
- Improved security: IPsec is built into the IPv6d principle
IPv6 Packet
Problem: IPv4 and IPv6 are not interoperable.
Solution: Transition mechanisms

We will focus on 4in6 and NAT64.
Tunneling

4in6 Tunneling

IPv6 packet:
Header:
SRC: Tunnel entry point address
DST: Tunnel exit point address
Payload:
The latter IPv4 packet:
SRC: 192.0.2.35
DST: 192.0.100.5

IPv4 packet:
SRC: 192.0.2.35
DST: 192.0.100.5

IPv4 packet:
SRC: 192.0.2.35
DST: 192.0.100.5

IPv4 packet:
SRC: 192.0.2.35
DST: 192.0.100.5

Source IPv4: 192.0.2.35
IPv4-only network

Destination IPv4: 192.0.100.5
IPv4-only network

IPv4-only network

4in6 Tunnel

Tunnel Entry Point

Tunnel Exit Point
Translation

Used for communicating between IPv4-only and IPv6-only networks.
Stateless NAT64

- The IPv4 is directly embedded in the IPv6 address.
- Network prefix destination routed to the NAT64.
- Usually deployed in conjunction with a DNS64.
Stateless NAT64

IPv6-only network
Network Prefix: 64:ff9b::/56

Query: www.destination.com
Answer: 64:ff9b::192.0.100.5

Source IPv6: 64:ff9b::192.0.2.33
(corresponds to IPv4: 192.0.2.33)
IPv6 packet:
SRC: 64:ff9b::192.0.2.3
DST: 64:ff9b::192.0.100.5

IPv4 packet:
SRC: 192.0.2.33
DST: 192.0.100.5

Destination IPv4: 192.0.100.5
(corresponds to IPv6: 64:ff9b::192.0.100.5)
IPv4 packet:
www.destination.com
IPv4-only network
Spoofing via 4in6

IPv6 packet:
Header:
SRC: Tunnel entry point address
DST: Tunnel exit point address
Payload:
The latter IPv4 packet:
SRC: 192.0.4.10
DST: 192.0.100.5

4in6 Tunnel

IPv4 packet:
SRC: 192.0.4.10
DST: 192.0.100.5

IPv4-only network

Tunnel Entry Point

Tunnel Exit Point

IPv4-only network

Source
IPv4: 192.0.2.35

Destination
IPv4: 192.0.100.5
Spoofing via NAT64

IPv6 packet (specially crafted):
SRC: 64::ff9b::192.0.4.10
DST: 64::ff9b::192.0.100.5

IPv6-only network
Network Prefix: 64::ff9b::/96

Source
IPv6: 64::ff9b::192.0.2.33
(corresponds to IPv4: 192.0.2.33)

NAT64

IPv4 packet:
SRC: 192.0.4.10 (spoofed)
DST: 192.0.100.5

IPv4-only network

Destination
IPv4: 192.0.100.5
(corresponds to IPv6: 64::ff9b::192.0.100.5)
Research of Services

4in6 Tunnel Brokers
- gogonet
- 6fei

NAT64
- Andrews & Arnold Ltd (U.S)
- TUXIS (England)
- Go6Lab (Netherlands)

6in4 Tunnel Brokers
- gogonet
- Hurricane Electric
4in6 Tunneling

First Try

Second Try

Last Try
Preps

- Crafting tool: Scapy \ Ostinato
- OS: Linux \ Windows
- Working Zone: Home \ Technion
- Port Forwarding \ Disable NAT \ DMZ
The Packet

IPv6 SRC: remote IPv6 of the 6in4
IPv6 DST: IPv6 of the 4in6 server

IPv4 SRC: legit source address
IPv4 DST: legit destination address

UDP header
Conclusions

- The servers aren’t part of the packet’s course

- The server supplies the tunnel and its endpoint addresses
Preps

- Contact with gogonet and supply of tunnels
- Move from to Windows and Scapy
- Create a gogonet 4in6 tunnel

Conclusions

- Exception thrown
- 6in4 tunnel missing
Preps

- Contact with gogonet and supply of tunnels
- Move from to Windows and Scapy
- Set a gogonet 4in6 tunnel
The Packet

IPv6 SRC: local IPv6 endpoint address of the 4in6 tunnel

IPv6 DST: remote IPv6 endpoint address of the 4in6 tunnel

IPv4 SRC: legit source address

IPv4 DST: legit destination address

UDP header
Conclusions

- Exception thrown

- 6in4 tunnel missing
Last Try

Preps
- Set a gogonet 4in6 tunnel
- Set a Hurricane Electric 6in4 tunnel

The Packet
- IPv4 SRC: my public IPv4 address
- IPv4 DST: remote IPv4 endpoint address of 6in4 tunnel
- IPv6 SRC: local IPv6 endpoint address of the 6in4 tunnel
- IPv6 DST: remote IPv6 endpoint address of the 4in6 tunnel
- IPv4 SRC: legit source address
Preps

- Set a gogonet 4in6 tunnel
- Set a Hurricane Electric 6in4 tunnel
The Packet

IPv4 SRC: my public IPv4 address

IPv4 DST: remote IPv4 endpoint address of 6in4 tunnel

IPv6 SRC: local IPv6 endpoint address of the 6in4 tunnel

IPv6 DST: remote IPv6 endpoint address of the 4in6 tunnel

IPv4 SRC: legit source address

IPv4 DST: legit destination address

UDP header
NAT64

Preps
- Get network prefix
- Set a gogonet 6in4 tunnel
- Set DNS of the system to be the provided DNS64

The Packet
IPv6 SRC: local IPv6 endpoint address of the 6in4 tunnel
IPv6 DST: synthesized IPv6 address of (IPv4) destination
UDP header
Preps

- Get network prefix

- Set a gogonet 6in4 tunnel

- Set DNS of the system to be the provided DNS64
The Packet

IPv6 SRC: local IPv6 endpoint address of the 6in4 tunnel

IPv6 DST: synthesized IPv6 address of (IPv4) destination

UDP header
Thoughts

- MAC address issue
- DNS64 issue
Summary
Agent-less IPv4 Spoofing Final Presentation
Daniel Galante