Inter-domain Routing (BGP) Security
[IP Prefix Hijacking]

Akmal Khan
[raoakhan@mmlab.snu.ac.kr]
4-15-2010
Outline

• Introduction
• Types of IP Prefix Hijacking
• Internet Routing Data Sources
• Tools of the Trade
• Past Research on BGP Sec
• Conclusion
Internet Abstractions

- Collection of Hosts, Routers, Point of Presence (PoP’s) or
- Autonomous System (AS)
  - An AS is a connected group of one or more IP prefixes run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy (RFC 1930)
Internet Number Resources

- IPv4/IPv6 addresses
- Autonomous System Numbers (ASn)
  - 16 bit
    - SNU has AS9488
  - 32 bit
    - Asx.y
Border Gateway Protocol (BGP)

- Inter-domain routing protocol (Inter AS)
  - Critical Communications and Business Infrastructure!
- Vulnerable to different threats
  - Configuration/Human Errors
    - “Patches” applied as threats are exploded
    - E2E solutions require collaboration
Outline

• Introduction
• Types of IP Prefix Hijacking
• Internet Routing Data Sources
• Tools of the Trade
• Past Research on BGP Sec
• Conclusion
Types of Prefix hijacking (PH)

[Type1] Prefix hijacking / Duplicate PH
- AS1 owns 1.2.0.0/16 but advertised by AS2

[Type2] Sub prefix hijacking
- AS2 advertises 1.2.3.0/24

[Type3] AS Path Spoofing
- AS5 announce [5 1] without having peering with AS1

[Type4] Independent PH
- AS2 use Bogons (unused address space)

[Type5] Man in the middle (MITM) Attacks
Prefix announcements

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.0.0/16</td>
<td>4, 2, 1</td>
</tr>
</tbody>
</table>

AS 1

Advertise 1.2.0.0/16

Path: 1

AS 2

AS 3

Prefix 1.2.0.0/16 Path: 3, 2, 1

AS 4

Prefix 1.2.0.0/16 Path: 4, 2, 1

AS 5

Prefix 1.2.0.0/16 Path: 2, 1

Prefix 1.2.0.0/16 Path: 2, 1

Prefix 1.2.0.0/16 Path: 2, 1
Type 1: Hijack a prefix

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.0.0/16</td>
<td>1</td>
</tr>
<tr>
<td>1.2.0.0/16</td>
<td>4, 5</td>
</tr>
<tr>
<td>1.2.0.0/16</td>
<td>5</td>
</tr>
</tbody>
</table>

AS 1 — AS 2 — AS 3 — AS 4 — AS 5

MOAS (Multiple Origin AS)

Advertise 1.2.0.0/16
Type 2: Hijack a prefix and its AS number

Advertise a path to 1.2.0.0/16

NO MOAS!

Prefix | Path
-------|------
1.2.0.0/16 | 5, 1

Prefix | Path
-------|------
1.2.0.0/16 | 2, 1

Prefix | Path
-------|------
1.2.0.0/16 | 1

Prefix | Path
-------|------
1.2.0.0/16 | 5, 1
Type 3: Hijack a subnet of a prefix

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.0/24</td>
<td>5</td>
</tr>
<tr>
<td>1.2.0.0/16</td>
<td>2, 1</td>
</tr>
</tbody>
</table>

Advertise 1.2.3.0/24
SubMOAS!

Advertise 1.2.0.0/16
Longest prefix matching

Attacker is able to attract all traffic

Advertise 1.2.3.0/24

Send packet to 1.2.3.4 in AS 1

Advertise 1.2.0.0/16

Prefix | Path
--- | ---
1.2.3.0/24 | 5
1.2.0.0/16 | 2, 1

Prefix | Path
--- | ---
1.2.3.0/24 | 4,5
1.2.0.0/16 | 2, 1

Prefix | Path
--- | ---
1.2.3.0/24 | 4.5
1.2.0.0/16 | 1
Type 4: Hijack a subnet of a prefix and AS number

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.0.0/16</td>
<td>2, 1</td>
</tr>
<tr>
<td>1.2.3.0/24</td>
<td>5, 1</td>
</tr>
</tbody>
</table>

Neither MOAS Nor SubMOAS!

Advertise a path to 1.2.3.0/24

1.2.3.0/24 path 5, 1

Advertise 1.2.0.0/16

Longest Prefix Matching
BGP Prefix hijacking Incidents

• Did AS13214 really hijack the Internet?
  • http://bgpmon.net/blog/?p=80
• Cyclops detects global routing leak by AS13214
• Don’t be afraid of AS3130..April 2009
  • http://cyclops.cs.ucla.edu/
• WorldofWarcraft.com and WoWarmory.com sub-prefix hijacked (July 2008)
• YouTube’s prefix hijacked by Pakistan Telecom February 2008
  • Search NANOG/NSP-Sec mailing archives for more
Outline

• Introduction
• Types of IP Prefix Hijacking
• Internet Routing Data Sources
• Tools of the Trade
• Past Research on BGP Sec
• Conclusion
Data Sources

- **RIR/Internet Route Registry (IRR)**
  - Registration information/Policy Information
    - RADB, RIPE, ARIN, APNIC

- **BGP Data Collectors**
  - RouteViews, RIPE-RIS
    - No. of BGP collector deployed around the world

- Trace route Datasets [Skitter/Ark, DIMES]

- P2P Ono, multicast data (mrinfo), Router logs, ACLs
  - Collect traces from Route Servers, Looking Glass servers etc.
Route Views (SNU AS)

RIPE-RIS (SNU AS)

http://bgplay.routeviews.org/bgplay/
http://www.ris.ripe.net/bgplay/
Outline

• Introduction
• Types of IP Prefix Hijacking
• Data Sources to start research
• Tools of the Trade
• Past Research on BGP Sec
• Conclusion
Cyclops..AS-Centric Visualization tool

• Data sources
  ▫ BGP routing tables + updates: Route Views, RIPE, Abilene, CERNET BGP View
  ▫ Route Servers: Packet Clearing House, UCR, traceroute.org, Route Server Wiki
  ▫ Looking Glasses: traceroute.org, NANOG, Looking Glass Wiki

• Others
  ▫ Mapnet, Otter, HERMES, VAST, FixedOrbit

http://cyclops.cs.ucla.edu/
Tools to get started

- Software based Router
  - Quagga 0.99.14/vyata/GateD etc.
- RIR-Internet Routing Registry
  - IRRd - 2.3.9
  - RIPE WHOIS 3.6
  - Irrtoolset 4.8.5
  - IrrPowerTools
- MRT dump file manipulation toolkit(MDFMT) version 0.2
  - BGP4MP
  - TableDump V2

- BGP trace Analyzers
  - PCH-Prefix Sanity Checker
  - RIPE-MyASN Service
  - BGPPlay
  - BGPmon.net
  - StraighRV
  - Prefixanalyzer
  - Pybgpdump
  - LinkRank Beta 02
Outline

• Introduction
• Types of IP Prefix Hijacking
• Data Sources to start research
• Tools of the Trade
• Past Research on BGP Sec
• Conclusion
BGP Solutions Categories

- **Prevention**
  - S-BGP, SO-BGP, SPV
- **Mitigation**
  - Wang et al., PG-BGP, Zhang et al., Anycast Routing
- **Detect & Alert**
  - myASN, IAR, Phas->Cyclops, BGPmon.net
- **Detect & Recover**
  - Probabilistic IP Prefix Hijacking (PIPA)
<table>
<thead>
<tr>
<th></th>
<th>Detection System</th>
<th>Alarm Type</th>
<th>Prefix/Duplicate PH</th>
<th>Subprefix PH</th>
<th>Super/Independent PH</th>
<th>Path Spoofing</th>
<th>MITM</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHAS [mohit et al]</td>
<td>H</td>
<td>Origin, Last Hop, Sub Allocation</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>limited</td>
<td>N</td>
</tr>
<tr>
<td>PG-BGP [J.Karlin et al]</td>
<td>H</td>
<td>Prefix, Sub Prefix</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>limited</td>
</tr>
<tr>
<td>K.Sriram et al. [ ]</td>
<td>H+R</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Nemecis</td>
<td>R</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Hu et al.</td>
<td>H</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

Table 1: Taxonomy of Prefix Hijacking Solutions (PH: Prefix Hijacking, Y: yes, N: No, H: History, R: Registry, Un: Unreachability, MITM: Man In The Middle)
Major Research Groups

- University of California Los Angeles (Lixia Zhang)
  - Internet Research Lab (irl)
- CAIDA
- Colorodo State University (Dan Massey)
  - Network Security Research Group
- University of Princeton (Jennifer Rexford)
  - Incrementally Deployable Secure Interdomain Routing
- University of Michigan (Z. Morley Mao)
  - RobustNet Group
Major Research Groups

• National Institute of Standards and Technology (Advanced Network Technologies Division)
  ▫ Trustworthy Networking
  ▫ BGP Security and Routing Robustness
  ▫ http://w3.antd.nist.gov/

• University of Swinburne (Geoff Huston)
  ▫ CAIA

• UCL, Louvain-la-Neuve, Belgium (Olivier Bonaventure)

INLAB Networking Lab
Conclusion

• None of the solution has been deployed? Why?
  ▫ Incentive to deployment, cost, politics, what not 😊

• Quite difficult to differentiate between hijack or router misconfiguration

• Working on the full level implementation and experimental results of BGP security Solution for IP prefix Hijacking
  ▫ Probabilistic IP Prefix Hijacking
References

  - Internet Alert Registry[http://iar.cs.unm.edu]
Thank You

Questions