BGP HIJACKING

OS3: Bram ter Borch & Jeroen Schutrup
National Cyber Security Center
BORDER GATEWAY PROTOCOL (BGP)

- Internets main routing protocol
- RFC 4271 - original from 1989
- Connects Autonomous Systems (AS)
- BGP hijack
WHAT IS A BGP HIJACK

- Prefix hijack
- Subnet hijack
- AS and prefix hijack
- AS and subnet hijack
- Supernet hijack (introduced in our paper)

1) http://www.bgpmon.net/chinese-isp-hijacked-10-of-the-internet/
## EXISTING SOLUTIONS

<table>
<thead>
<tr>
<th>Web based</th>
<th>Tooling</th>
<th>Theoretical</th>
</tr>
</thead>
<tbody>
<tr>
<td>• BGPMON</td>
<td>• PHAS</td>
<td>• Hu et al. (fingerprinting and traceroute)</td>
</tr>
<tr>
<td>• DYN.com</td>
<td>• iSPY</td>
<td>• Zheng et al. (traceroute to monitored networks from reference point)</td>
</tr>
</tbody>
</table>
LIMITATIONS & CHALLENGES

- Limited to online prefixes
- Noise generation
- Lacking Multiple Origin AS (MOAS) Support
- Information disclosure
RESEARCH QUESTION

How to create an early detection system for BGP hijacks for a fixed number of IP ranges and AS numbers using public resources?
PROPOSED MODEL (BHAS)

- Requires full BGP feed
- Supports IPv4 and IPv6
- Support MOAS
- Support Multi-homing
INITIALIZATION

BGP update

Subnet check: Is the prefix within the update a subnet, equal to, or supernet of monitored prefix?

Discard

Pass subnet check

No

Yes

Announcement or Withdrawal

Monitored prefixes Asnumber, AS path, AS path -1, country code AS

Announcement

Withdrawal

No

Yes
AS HIJACK DETECTION

Get AS-path -1

Different

Compare AS-path -1

Different

Get GEOLOCATION AS-path -1

Compare GEO with announcing AS

OK

OK

In hijack database?

Yes

No

Discard

Hijack registration and alert

Clear hijack

Hijacked Networks

Monitored prefixes Asnumber, AS path, AS path - 1, country code AS
WITHDRAWAL

Monitored prefixes
Asnumber, AS path, AS path - 1, country code AS

Update DB

Hijacked Networks

Hijack registration and alert

Clear hijack

In Hijacked Database?

No

Yes
PROOF OF CONCEPT

Build within 2 days
ExaBGP
Python application
Multithreaded
Postgres database
Peewee ORM

1) https://prince2pm.files.wordpress.com/
TEST CASES

- All five types of hijacks
- Virtualized environment
- IRR records
RESULTS - ANALYSIS - CONCLUSION
RESULTS TEST ENVIRONMENT

• All types of BGP hijacks are reported

• Prevents data disclosure to third parties
IRR RECORDS

“As it turns out 46% of all the prefixes in the routing table today have a valid route object.”

BGPmon.net (2009)

“Russia is way ahead of the others with 88.4% coverage”

research.dyn.com (2009)
RESULTS - IRR RECORDS

% of Dutch prefixes

# of IRR records

IPv4
IPv6
RESULTS - UPDATES

Amount of Updates per hour

Amount of Updates

Runtime in hours

Updates
IPv4 announcements
IPv6 announcements
RESULTS - WITHDRAWALS

- # of withdrawals:
  - IPv4 withdrawals
  - IPv6 withdrawals

- Runtime in hours:
  - 1 to 24 hours
RESULTS - INTERESTING WITHDRAWALS

Interesting IPv4 withdrawals
interesting IPv6 withdrawals

Runtime in hours

# of withdrawals

Interesting IPv4 withdrawals
interesting IPv6 withdrawals
RESULTS - HIJACKS

- **Type 1**
  - Total hijacks: 600
  - Withdrawn hijacks: 0

- **Type 2**
  - Total hijacks: 150
  - Withdrawn hijacks: 0

- **Type 3**
  - Total hijacks: 300
  - Withdrawn hijacks: 150

- **Type 4**
  - Total hijacks: 450
  - Withdrawn hijacks: 0

- **Type 5**
  - Total hijacks: 0
  - Withdrawn hijacks: 600
ANALYSIS

Dutch IRR registration coverage better than expected
Algorithm works
Architecture scales
More IPv6 withdrawals
9 hijacks every hour
LIMITATIONS

Model limitations

• Number of BGP feeds
• IRR registration
• Upstream AS geolocation

Future work

• Connect to live BGP feed for further analysis
• Correlate to real BGP hijacks
• Compare to other solutions
CONCLUSIONS

• The proposed model is tested successfully
CONCLUSIONS

- The proposed model is tested successfully
- IPv4 IRR registration coverage is 98% for Dutch ASes
- IPv6 IRR registration coverage is 96% for Dutch ASes
CONCLUSIONS

• The proposed model is tested successfully

• IPv4 IRR registration coverage is 98% for Dutch ASes

• IPv6 IRR registration coverage is 96% for Dutch ASes

• Lower number of MOAS networks for IPv6
CONCLUSIONS

• The proposed model is tested successfully

• IPv4 IRR registration coverage is 98% for Dutch ASes

• IPv6 IRR registration coverage is 96% for Dutch ASes

• Lower number of MOAS networks for IPv6

• Reported hijacks: 1460 out of 10.5 million updates
QUESTIONS