CPS 590.5 Computer Security
Lecture 14: Other Network Security Problems

Xiaowei Yang
xwy@cs.duke.edu
Roadmap

• Previous lecture
  – Proof of Work
    • Bandwidth
    • Computation

• Security problems we have discussed
  – Worms, Malware
  – Source address spoofing
  – DDoS

• Today
  – Other network security problems
TCP Sequence Number Prediction

Client

SYN C

SYN S, ACK C

ACK S

DATA

Server
Attack

SYN X, T

ACK S

Bad-DATA

Server

SYN S, ACK X

T

Attacker
Vulnerabilities

- Sequence numbers predictable
- R* services use IP addresses to authenticate hosts
Fixes?
Routing attacks

• Source routing
  – T, X, S

• Prefix hijacking attacks
Routing Background

- Routing is about finding a path.

To reach 20.0.0.2:
- forward to RB

To reach 20.0.0.2:
- forward to RD

• Routing is about finding a path.
Border Gateway Protocol

- A domain is a network under a single administration.
- Vulnerabilities
  - Lack of integrity: no mechanism to verify the integrity of route announcement
  - Global contamination: lies propagate globally
Type of attacks

- Blackholing
  - Hijacking

- Redirection
  - Interception

- Instability
Attack mechanisms

• False UPDATEs and prefix hijacking
  – Most serious attack
  – We’ll deal with this today

• De-Aggregation
• Contradictory advertisements
  – Is it really an attack?
• Update modifications
• Link flapping
• Instability
• Congest-induced BGP session failures
How prefix hijacking attacks are launched?

Internet

Victim

I own prefix 4/8 and use me to reach it

Polluted

Valid route

Bogus route

Attacker

I own prefix 4/8 and use me to reach it
Past Prefix Hijacking Incidents

- **Apr 1997**: AS7007 subprefix hijacked most of the Internet for 2 hours;

- **Dec 2004**: AS 9121 incorrectly originated routes to 106,089 prefixes, almost 70% of all the prefixes;

- **Jan 2006**: Panix’s /16 stolen by Con Edison;

- **Feb 2006**: Sprint and Verio briefly announced TTNET as the origin AS for 4/8, 8/8, and 12/8;

- **Feb 2008**: YouTube's prefix hijacked by Pakistan Telecom for 2 hours.

- And more ...
Defenses

• Prevention
  – Router filters to filter bogus announcements
  – Cryptographic enhancement to BGP
    • SBGP, SoBGP etc.

• Detection
  – Hijacking
  – Interception

• Mitigation

• Impact analysis
Cryptographic enhancement to BGP
SBGP

- PKIs that authorize prefix ownership and validate routes
- Signed BGP updates
- IPsec for routing message exchanges
sBGP’s PKIs

- Two hierarchical PKIs.
  - address allocation: binds addresses to org names
  - AS number and router association: bind org names to ASes and routers

- BGP announcements have AS numbers, not org names
sBGP’s attestations

• Address attestation (AA):
  – Which AS can originate which address prefix
  – Requires address allocation certificate

• Route attestation (RA):
  – Each transit AS signs the AS path from the next AS to the originator AS
Validate an sBGP announcement

1. A generates RA for P, including B as the next hop.
2. A sends RA and prefix update to B
3. B validates RA and verifies AA (fetched offline)
4. B generates new RAs for its peers C and D, and forwards the updates to C and D.
Disadvantages of sBGP

• Two hierarchical PKIs: address allocation, and AS number and router association
• Heavy weight
SoBGP

• Replace a hierarchical PKI with a web of trust PKI
• Goals:
  – Validate an AS is authorized to originate a prefix.
  – Verify a peer which is advertising a prefix has at least one valid path to the destination.
• Requirements:
  – Take advantage of operational experience
  – Minimize changes
  – No central authority
  – Must not rely on routing to secure routing
  – Incrementally deployable
  – Easy to manage
Certificate structure

- **EntityCert: who are you?**
  - Web-of-trust, signed by 3rd party

- **AuthCert: Are you authorized?**
  - Bind an AS to the address prefix it advertises
  - Wrapped in PolicyCert
  - Q: how can authcert be verified?

- **PolicyCert: Do You Really Have a Path**
  - Build a topology map
Pros and Cons

• Pros:
  – Prebuild databases, so that no cryptographic operation on UPDATEs

• Cons
  – Difficult to verify AuthCert
  – Paths integrity is not guaranteed
Detection mechanisms

• iSPY: detecting IP prefix hijacking on my own

• A Study of Prefix Hijacking and Interception in the Internet
Key Idea of iSpy

• Hijack of a prefix X causes a significant fraction of Internet to be polluted

• A significant fraction of probes sent out from prefix X to the Internet will not come back
Design Challenge

• How to distinguish unreachability caused by hijacks from other events (e.g. link failure and congestion)?

1. Reachability view from the prefix owner
2. Definition of cut
3. Cut distinguishes hijacks from other events
Reachability View from Prefix Owner

Internet

Prefix owner

216.239.46.246

149.165.254.7

192.31.0.105

172.19.124.1

128.46.101.1
Reachability View from Prefix Owner
Reachability View from Prefix Owner
“Cut” on the Reachability View

Prefix owner

cut
|Cuts|: Distinguish Hijacks from Other Events

- Hijack causes many cuts

Prefix owner (victim)

Other event causes few cuts

Prefix owner

cut
Why Does Hijacking Causes Many Cuts?

1. A single cut if Internet topology were a tree

2. Actual Internet topology is different, and its implication

3. Simulation validation
Tree Topology Causes Single Cut

- Polluted region is a subtree
- A single cut at the subtree root
Mesh Topology Causes Multiple Cuts

Many peering links and multi-homing links → Mesh

- Polluted region consists of multiple subtrees
- Each subtree creates multiple cuts
Simulation: How Many Cuts?

Simulated 2450 hijacking instances on a realistic AS topology inferred by running Gao’s relationship inference algorithm.

CDF (% of hijackings) vs |cuts|
iSPY Design

- Continuous probing
- Threshold-based Detection

|Cuts|

Large

Small

Hijacking

Other disruption events, e.g. link failures, congestions

Detection threshold
iSPY’s Implementation Details

- Lightweight traceroute
  - How does traceroute work?
    - Sample one destination per transit AS (total ~4000 transit ASes) with no loss of accuracy
      - If hijacked, ICMP replies will not come back to prefix owner
    - One round of probing takes every 10~15 mins
## iSPY’s Accuracy

<table>
<thead>
<tr>
<th>Experiment</th>
<th>Purpose</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulating hijacks on an Internet AS topology</td>
<td>False negative</td>
<td>0.45%</td>
</tr>
<tr>
<td>Deploying iSPY on 108 Planetlab sites (over 25 days)</td>
<td>False positive</td>
<td>0.17%</td>
</tr>
</tbody>
</table>

Detection threshold = 10
Internet Hijacking Experiment

Performed 15 hijacks with different attacker and victim
iSPY is Real-time!

Transit ASes in Internet

31-53% polluted

Probed 1~3%

- iSPY detected all 15 hijacks in 1.4~3.1 mins
- All hijacks have over 200 cuts
Security Properties of iSPY

• Deal with regular prefix hijacking
  • Not subprefix hijacking
  • Not interception
    – Why?

• Evasion attacks on iSPY
  • Probe spoofing needs an interception attack
  • Pollution shaping is not easy
Conclusion

iSPY prefix-owner centric hijacking detection

√ Real-time (1.4-3.1 minutes)
√ Lightweight
√ Accurate (F.N.=0.45%, F.P.=0.17%)
√ Easy to deploy
√ Incentive to deploy
√ Robust in victim notification
A Study of Prefix Hijacking and Interception in the Internet

Ballani et al.
Who can hijack/intercept my prefix?

• Hijack
  – As long as I can announce a more preferable route
  – Which routes are more preferable?
    • Customers > peers > providers
    • AS path length to break ties
      – Announce a direct path: p X
      – Or a two-hop path: p XO
    » Why not direct path?
Interception

• Two conditions must be met
  – I can announce a more preferable path
  – My original path to hijacked prefix is not polluted

• Challenge: how to ensure both conditions are met?
Valley-free properties

- After traversing one provider-to-customer or peer-to-peer edge, no more such edges can be traversed
If (existing route to p is through a provider) then
   Advertise to all peers and customers a route for prefix p with AS-PATH [X];
else
   Advertise to all neighbors a route for prefix p with AS-PATH [X];
endif
If (the invalid advertisement causes the existing route for p to change) then
   Stop the advertisement to the anomaly-causing neighbor;
endif
Evaluation

Generated traffic from 23,588 recursive nameservers
For each site as owner, hijacked and intercepted traffic using other sites
<table>
<thead>
<tr>
<th>Ber</th>
<th>Pit</th>
<th>Sea</th>
<th>Lth</th>
<th>Ote</th>
<th>% of traffic Hijacked</th>
<th>% of traffic Intercepted</th>
</tr>
</thead>
<tbody>
<tr>
<td>O</td>
<td>✗</td>
<td>✗</td>
<td>☑</td>
<td>☑</td>
<td>91.7</td>
<td>78.8</td>
</tr>
<tr>
<td>✗</td>
<td>0</td>
<td>✗</td>
<td>☑</td>
<td>☑</td>
<td>68.8</td>
<td>67.5</td>
</tr>
<tr>
<td>✗</td>
<td>✗</td>
<td>0</td>
<td>☑</td>
<td>☑</td>
<td>97.4</td>
<td>66.2</td>
</tr>
<tr>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>0</td>
<td>☑</td>
<td>66.0</td>
<td>47.3</td>
</tr>
<tr>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>✗</td>
<td>0</td>
<td>76.1</td>
<td>23.4</td>
</tr>
</tbody>
</table>

- O: Site owning the prefix
- ✗: Site not advertising an invalid route during interception
- ☑: Site advertising an invalid route during interception
Detection

- Compare traceroute from dataplane with AS path from BGP
Conclusion

• Tier-1 ASes can hijack and intercept significant fraction of traffic to any p
• Small ASes can hijack and intercept a non-negligible amount of traffic
• Verified using known prefix hijacking events
Summary

- TCP attacks and fixes
- BGP and prefix hijacking attacks
- sBGP and soBGP
- Detection of hijacking attacks
  - Traffic will not return to prefix owners