Autonomous security for autonomous systems

Josh Karlin, Stephanie Forrest, Jennifer Rexford

Presented By: Virajith Jalaparti

(Some figures borrowed from author’s slides)
How secure is BGP?

- Open trust Model
- Completely Insecure
- ASes can
  - pretend to own any prefix
  - pretend to be neighbors with an other AS
  - pretend to have any arbitrary path to a destination
  - lie about their identity
Examples of Hijacks

- Africa Online Kenya hijacked on March 15, 2008
- Pakistan Telecom hijack of YouTube on Feb 24, 2008
- eBay hijacked on Nov 30, 2007
- Con Edison hijacked routes to Panix (ISP NY) on Jan 22, 2006.
- TTNet’s Christmas Eve Gift on Dec 24, 2005
- MAI Net (AS 7007) in 1997

Probably would not have been detected if they were intercepted
Prefix Hijack
Attack 2

- Sub-prefix hijack
Attack 3

- Shortest Spoofed Path
Policy Violation

• Is this really an attack?
• An AS can follow any policies it likes
• Probably useful for Mis-configurations
Other attacks

- Shortest Path
- Spoofed ASN

Other attacks?

An AS can spoof an intermediate ASN in the path, still having valid edges
Fixes to BGP

- S-BGP
  - PKI to ensure ownership of prefixes
  - Each AS signs the advertisement it sends
- so-BGP
  - Distributed PKI containing prefix ownership information and policy objects
  - Policy objects – used to define neighbor relationships and policies between them
A Pretty Good Hueristic

- Adopt *anomalous* paths only if they *turn out* to be *good*
- Works only because
  - Hijacks are typically short lived
  - Network Operators are on a constant vigil looking out for anomalies
  - Network Operators communicate with each other
- PGBGP relies on human intervention
Maintain a history of the normal network
- (prefix, origin AS) *prefix pairs*
- AS-level internet graph with directed edges inferred from paths advertised

First $h$ days – learning phase

Anomalous advertisement if
- new prefix advertised
  - with new origin AS
- More specific prefix of a prefix in history announced

- Edges stay in history for $h$ days after it becomes stale
- Opportunity for attackers to spoof paths
- More specific prefixes used for traffic engineering – How would this effect this goal?
Response to anomalies

- Defer adopting anomalous paths for some time (24hrs)
  - Reduce their preference
  - When will this work?
  - Depends on availability of other paths
  - Withdrawal messages can probably be spoofed also
    - Would force advertisements for more specific prefixes to be used
  - Does changing preferences arbitrarily affect stability for these 24hrs?

- Use IAR to alert operators to anomalies?
  - Why should be it be trusted?
  - Send spurious advertisements to IAR
  - Impersonate IAR – if not properly authenticated
Incremental adoption of PGBGP

- These experiments do not consider false positives
Of the remaining ones, how many are actual anomalies?
**PGBGP vs S–BGP vs so–BGP**

- **When fully deployed**
  
<table>
<thead>
<tr>
<th></th>
<th>SBGP</th>
<th>soBGP</th>
<th>PGBGP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid origin AS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy violations</td>
<td>No</td>
<td>Yes</td>
<td>Partial</td>
</tr>
<tr>
<td>Spoofed AS numbers</td>
<td>Yes</td>
<td>Partial</td>
<td>Partial</td>
</tr>
<tr>
<td>Spoofed edges</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- **When partially deployed**
  
<table>
<thead>
<tr>
<th></th>
<th>SBGP</th>
<th>soBGP</th>
<th>PGBGP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid origin AS</td>
<td>Partial</td>
<td>Partial</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy violations</td>
<td>No</td>
<td>Partial</td>
<td>Partial</td>
</tr>
<tr>
<td>Spoofed AS numbers</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
</tr>
<tr>
<td>Spoofed edges</td>
<td>Partial</td>
<td>Partial</td>
<td>Yes</td>
</tr>
</tbody>
</table>
What PGBGP does not handle

- Data Plane anomalies
- Does not entirely stop anomalies from propagating
- Mixed Relationships
- Potential DOS – as routers store history