How Secure are Secure Interdomain Routing Protocols?

S. Goldberg
M. Schapira
P. Hummon
J. Rexford

Vitali Bashko
NDS Seminar 2011
Outline

- Motivation
- Model and Methodology
- Attraction Attacks
- Interception Attacks
- Optimal Attacks
- Conclusion
Motivation

- Attracting extra traffic enables the AS to:
  - increase revenue from customers
  - drop or snoop packets
- It is difficult to deploy a new secure routing protocol to Internet
- Evaluate four major extensions to BGP: Origin Authentication, soBGP, S-BGP, data-plane verification
Modeling Interdomain Routing

- AS-graph topology is static
- Routing policies
  - ranking on outgoing paths
  - applying export policies
- Business relationships
  - custom-provider
  - peer-to-peer
Modeling Interdomain Routing

- Routes selection model
  - Local preferences
  - Shortest Path
  - Tie Break
- Export Policies model (Gao-Rexford condition)
  - AS \( b \) will only announce a path via AS \( c \) to AS \( a \) if at least one of \( a \) and \( c \) are customers of \( b \).
Threat model

- Normal ASes vs. Manipulator
- Manipulator can perform two types of attack
  - Attraction attacks
  - Interception attacks
- Attack strategy may include
  - Announcing an available or non-existent path
  - Announcing a path that is different from the normal
  - Ignoring normal exporting policies
- Experiments on ~ 60,000 randomly-chosen manipulator-victim pair
Fooling BGP Security Protocols

BGP

- Manipulator can announce any path that he wants
- By claiming that he is owner of the victims IP prefix, he can attract traffic from ~75% ASes
Fooling BGP Security Protocols

Origin Authentication

- Manipulator can announce a path that ends at the AS that owns victims IP prefix
- Announcing \((m, v, \text{Prefix})\) path 25% of traffic is attracted
Fooling BGP Security Protocols

soBGP

- Manipulator can announce exist but unavailable path
- Announcing (m, p, v, Prefix) path traffic from 10% of ASes is attracted
Fooling BGP Security Protocols

S-BGP

- Manipulator can announce shorter, but more expensive path
- Announcing \((m, T1, a1, v, \text{Prefix})\) path traffic from 1.7% of ASes is attracted
Attraction Attacks

“Shortest-Path Export-All” strategy
Attraction Attacks

“Shortest-Path Export-All” strategy
Attraction Attacks

- soBGP and S-BGP protocols provides similar performance
Attraction Attacks

- S-BGP is limiting the set of paths to announce
- However, path lengths in Internet, are short in general
Attraction Attacks

- Export policy is also important in attraction attacks
- Announcing a shortest path is less important than announcing a path to more neighbors
Intersection Attacks

- The interception attack strategy is used to prevent creating blackholes.
- Blackholes are guaranteed to not occur in following situations.

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>Customer</th>
<th>Peer</th>
<th>Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Peer</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Provider</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Intersection Attacks

- Manipulators with most customers are least likely to create blackholes
- Attacks on S-BGP never produces blackholes
Intersection Attacks

- “Shortest-Available-Path Export-All” strategy
  - Manipulator should announce his shortest available path from the normal outcome to his neighbors

- “Hybrid Interception” attack strategy
  - First run “Shortest-Path Export All” strategy. If no available paths found then announce the shortest available path from normal outcome to all neighbors
Intersection Attacks

- Hybrid strategy intercepts traffic from at least 10% of ASes with probability 50%
Optimal Attack Strategies

Attract more by announcing longer paths

(m, a1, v, Prefix) ~16%
Optimal Attack Strategies

Attract more by announcing longer paths

(m, a1, v, Prefix) $\sim$ 16%

(m, a2, a3, v, Prefix) $\sim$ 56%
Optimal Attack Strategies

Attract more by exporting less

(T1a, T2, m, v, Prefix)

~40%
Optimal Attack Strategies

Attract more by exporting less

(T1a, T2, m, v, Prefix) ~40%

(T1a, m, v, Prefix) ~50%
Conclusions

- Secure routing protocols should be deployed in combination with Defensive Filtering
- S-BGP do not significantly outperform soBGP for kind of attacks we evaluated
- Interception attacks are easy to perform on large ASes with many customers
- Very efficient attack strategy could exist for given AS graph, however finding the optimal one is NP hard
References
