Autonomous Security for Autonomous Systems

Josh Karlin - University of New Mexico
Stephanie Forrest - University of New Mexico and Santa Fe Institute
Jennifer Rexford - Princeton University
Interesting questions

• How much security can an individual AS achieve without relying on other networks to participate?

• How much global security could an oracle provide if only some networks listened?

• How effective are the known exploits?
Outline

- Related work
- Pretty Good BGP
- Results
- The Internet Alert Registry
- Sample attacks
- Conclusions
Vulnerabilities of BGP

• BGP does not verify information within route updates

• Allows ASes to draw traffic that belongs to other networks
  
  • Africa Online Kenya hijacked on March 15th 2008
  
  • YouTube hijacked on February 24th 2008
  
  • eBay hijacked on November 30th 2007
Exploit 1: Prefix hijack

- What if an AS announces a prefix it does not own?
Exploit 2: Sub-prefix hijack

What if an AS announces a sub-prefix it does not own?
Exploit 3: Spoofed edge

- What if an AS propagates a path with an edge that does not exist?
Exploit 4: Policy violation

- What if an AS propagates a route which violates contractual policy?
Exploit classification

- Invalid origin AS
  - Prefix and sub-prefix hijacks

- Invalid paths
  - Spoofed edge
  - Policy violation
  - Shortest valid path
  - Spoofed ASN
Related work

Public Key Infrastructure

- Each AS has a private/public key pair
  - SBGP, soBGP, psBGP

- Each prefix has a certificate naming its owner
  - SBGP, soBGP, psBGP

- Each AS has a certificate declaring its policies
  - soBGP
Related work
PKI continued

• SBGP & psBGP
  • Each AS signs the update as it is propagated
  • Each AS verifies the signatures along the path

• soBGP
  • Each recipient ensures that the origin AS number is correct
  • Each recipient ensures that the path is feasible (obeys published policy)
Related work

Anomaly detection

- Kruegel et al.: Use out-of-band WHOIS data to infer likelihood of network links

- Zhao et al.: Attach a list of trusted origins to each update, new origins are considered suspicious

- Wang et al.: Filter out all but stable routes for popular DNS destinations
Related work
Anomaly response

• Flag the route as suspicious, alert the local router’s operator

  • Route is still used until operator intervention

  • Local operator may not be able to verify the route

  • Can burden the local operator
## Related work

### Deployment difficulties

**PKI**

- Requires top-down key assignment
- Hard to verify paths with partial deployment
- Little incentive for early adoption
- Requires public policy disclosure

**Anomaly detection and response**

- Existing algorithms are not general enough
- Ineffective response
- Too much operator involvement
Ideal distributed security

- Autonomous security
- No PKI
- No sensitive network information revealed
- Immediate protection for early adopters
Threat model

- Detect and stop the propagation of routes with:
  - false origins
  - spoofed edges
  - policy violations
Pretty Good BGP

- Anomaly detector
  - Use a database of normal “trusted” routes instead of a PKI
  - Compare incoming routes to the database as in soBGP
- Response
  - Punish anomalous routes by lowering their chance of being propagated
  - Alert the pertinent operators, let them resolve the problem
PGBGP - Detection

- Monitor which origin ASes announce each prefix
- Monitor consecutive ASes in paths (directed edges)
- Label paths with new origins or edges as anomalous

Origin Verification
prefix: 12/8

History:
A → B → C → D

New path:
A → B → C → Z

Edge Verification

A → B → C → D

A → B → Z → D
Special case: anomalous sub-prefixes

- Problem: A new sub-prefix cannot be avoided as there are no alternative routes.

- Solution: For 24 hours, ignore the route and continue routing to the less specific through routers that have not propagated the sub-prefix.

- Reachability issues: It is possible (though unlikely) that the origin AS of the less specific will be unable to properly route to the destination.
Intuition behind the detector

• Assume that the normal database $N$ is clean (contains only valid routing information)

  • The database should gradually become more reliable as anomalous routes are detected and fixed

• Origins: New origins for prefixes will not be in $N$ since $N$ is clean

• Spoofed edges: A new edge will also not be in $N$ since $N$ is clean

• Policy violations: This is trickier..
Inferring policy violations

- Provider edges should only be seen by customers
  - Only customers of B should see *directed* edge (B,C)

- Peer edges should only be seen by customers
  - Only customers of B should see *directed* edge (B,C)
Policy violations produce new edges

- Assumption: Single policy of (peer/customer/provider) between each pair of ASes

- Proven that any policy violating path includes an edge not in $N$ unless the policy violator is one of the recipient’s transient providers
PGBGP - Response

• Try not to select suspicious routes for 24 hours

• This prevents the use and propagation of potentially harmful routes
  • Without affecting reachability! (with one unlikely exception)

• Use distributed route monitoring systems to alert operators to suspicious routes (e.g. Internet Alert Registry)
Simulations

- Given an inferred BGP network (with inferred relationships)
- Some percentage of the routers have PGBGP enabled
- Select an attacker and victim AS from the graph at random
- Time 0: Victim announces trusted route (normal database is updated)
- Time 1: Attacker announces a bogus route
- After the network converges, count up the ASes that routed to the attacker
Vulnerability of unprotected networks

- Sub-prefix hijack
- Prefix hijack
- Spoofed prepend
- Policy violations
Global (simulated) impact of deployment

Mean Fraction Routed Through Attacker vs. Number of ASes Deploying Enhanced PGBGP

- Sub-prefix hijack
- Prefix hijack
- Spoofed path
- Policy violation
Measurements on RouteViews data

- Ran the PGBGP algorithm on 4 months of RouteViews2 updates
- Selected the top 10 most active streams in the data
- Measured the number of alerts vs. number of streams and history time $h$ (how recently an origin or edge must have been seen to be in $N$)
Number of prefix-hijack anomalies per day

![3D graph showing the number of prefix-hijack anomalies per day against days in history window and number of streams. The graph is color-coded with a gradient scale from 0 to 130, indicating the number of new prefix origins per day.]
Many anomalies are brief

```
<table>
<thead>
<tr>
<th>Duration of anomaly in routing table (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>20</td>
</tr>
<tr>
<td>25</td>
</tr>
</tbody>
</table>

PMF

New Origin ASes
New Sub-Prefixes
New Edges
```
The Internet Alert Registry

- [http://iar.cs.unm.edu/](http://iar.cs.unm.edu/)

- Runs the PGBGP algorithm on public BGP feeds

- Two methods of receiving alerts
  - Email alerts for AS numbers of your interest
    - .02 alerts / day / AS (std .18) -- 4.24 alerts per day per Tier 1 ISP
  - IAR Tracker compares RSS feed of alerts to local configuration, eliminating false positives
IAR Tracker example configuration

BEGIN_ASN: 65002
Prefix: 10.0.0.0/8
Prefix: 192.168.1.0/24 :65041,65009

BEGIN_GROUP: PEERS
    Neighbor: 65042
END_GROUP: PEERS

BEGIN_GROUP: PROVIDERS
    Neighbor: 65001
    Neighbor: 65022
END_GROUP: PROVIDERS

BEGIN_GROUP: CUSTOMERS
    Neighbor: 65041
END_GROUP: CUSTOMERS

# Standard export rules
EXPORT: CUSTOMERS :PEERS,PROVIDERS,CUSTOMERS
EXPORT: PEERS :CUSTOMERS
EXPORT: PROVIDERS :CUSTOMERS

END_ASN: 65002
### Alexa top 500 websites

<table>
<thead>
<tr>
<th>Rank</th>
<th>Site</th>
<th>Time</th>
<th>Origin</th>
<th>Prefix</th>
<th>Why?</th>
<th>Super Prefix</th>
<th>Trusted Origins</th>
<th>AS Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><a href="http://www.youtube.com">www.youtube.com</a></td>
<td>2008-02-24 18:47:57</td>
<td>17557</td>
<td>208.65.153.0/24</td>
<td>1</td>
<td>208.65.152.0/22</td>
<td>36561</td>
<td>3333 12859 6461 3491 17557</td>
</tr>
<tr>
<td>3</td>
<td><a href="http://www.live.com">www.live.com</a></td>
<td>2007-11-30 16:06:51</td>
<td>10139</td>
<td>207.46.0.0/19</td>
<td>0</td>
<td></td>
<td>8075</td>
<td>4608 7474 7473 9299 10139</td>
</tr>
<tr>
<td>5</td>
<td><a href="http://www.myspace.com">www.myspace.com</a></td>
<td>2007-11-30 16:06:51</td>
<td>10139</td>
<td>216.176.0/20</td>
<td>0</td>
<td></td>
<td>33739</td>
<td>4608 7474 7473 9299 10139</td>
</tr>
<tr>
<td>6</td>
<td><a href="http://www.facebook.com">www.facebook.com</a></td>
<td>2007-05-08 13:12:38</td>
<td>21318</td>
<td>69.63.176.0/20</td>
<td>0</td>
<td></td>
<td>32934</td>
<td>16186 21318 21318</td>
</tr>
<tr>
<td>18</td>
<td><a href="http://www.microsoft.com">www.microsoft.com</a></td>
<td>2006-11-30 03:30:04</td>
<td>4761</td>
<td>207.46.192.0/18</td>
<td>0</td>
<td></td>
<td>8070</td>
<td>4608 1221 4637 4761</td>
</tr>
<tr>
<td>23</td>
<td><a href="http://www.ebay.com">www.ebay.com</a></td>
<td>2007-11-30 16:06:51</td>
<td>10139</td>
<td>66.135.192.0/19</td>
<td>0</td>
<td></td>
<td>11643</td>
<td>4608 7474 7473 9299 10139</td>
</tr>
<tr>
<td>23</td>
<td><a href="http://www.ebay.com">www.ebay.com</a></td>
<td>2006-11-30 03:28:16</td>
<td>4761</td>
<td>66.135.192.0/19</td>
<td>0</td>
<td></td>
<td>11643</td>
<td>4608 1221 4637 4761</td>
</tr>
<tr>
<td>31</td>
<td><a href="http://www.youporn.com">www.youporn.com</a></td>
<td>2007-10-12 00:40:26</td>
<td>35985</td>
<td>74.86.108.0/22</td>
<td>1</td>
<td>74.86.0.0/16</td>
<td>36351</td>
<td>3333 12859 6461 1299 35985</td>
</tr>
<tr>
<td>50</td>
<td><a href="http://www.redtube.com">www.redtube.com</a></td>
<td>2006-11-30 03:28:16</td>
<td>4761</td>
<td>66.55.128.0/19</td>
<td>0</td>
<td></td>
<td>20473</td>
<td>4608 1221 4637 4761</td>
</tr>
<tr>
<td>78</td>
<td><a href="http://www.veoh.com">www.veoh.com</a></td>
<td>2007-11-19 21:37:59</td>
<td>26608</td>
<td>8.3.211.0/24</td>
<td>0</td>
<td></td>
<td>40415</td>
<td>34225 41692 3491 26608</td>
</tr>
<tr>
<td>82</td>
<td><a href="http://www.ebay.fr">www.ebay.fr</a></td>
<td>2007-11-30 16:06:51</td>
<td>10139</td>
<td>66.135.192.0/19</td>
<td>0</td>
<td></td>
<td>11643</td>
<td>4608 7474 7473 9299 10139</td>
</tr>
<tr>
<td>82</td>
<td><a href="http://www.ebay.fr">www.ebay.fr</a></td>
<td>2006-11-30 03:28:16</td>
<td>4761</td>
<td>66.135.192.0/19</td>
<td>0</td>
<td></td>
<td>11643</td>
<td>4608 1221 4637 4761</td>
</tr>
<tr>
<td>84</td>
<td><a href="http://www.terra.com.br">www.terra.com.br</a></td>
<td>2007-12-10 14:38:17</td>
<td>3549</td>
<td>200.176.3.0/24</td>
<td>1</td>
<td>200.176.0.0/16</td>
<td>11706</td>
<td>3333 12859 6461 3549</td>
</tr>
<tr>
<td>88</td>
<td><a href="http://www.apple.com">www.apple.com</a></td>
<td>2006-09-07 15:28:00</td>
<td>9121</td>
<td>17.251.0.0/16</td>
<td>0</td>
<td></td>
<td>714</td>
<td>286 1299 9121</td>
</tr>
<tr>
<td>90</td>
<td><a href="http://www.ebay.de">www.ebay.de</a></td>
<td>2007-11-30 16:06:51</td>
<td>10139</td>
<td>66.135.192.0/19</td>
<td>0</td>
<td></td>
<td>11643</td>
<td>4608 7474 7473 9299 10139</td>
</tr>
<tr>
<td>90</td>
<td><a href="http://www.ebay.de">www.ebay.de</a></td>
<td>2006-11-30 03:28:16</td>
<td>4761</td>
<td>66.135.192.0/19</td>
<td>0</td>
<td></td>
<td>11643</td>
<td>4608 1221 4637 4761</td>
</tr>
<tr>
<td>93</td>
<td><a href="http://www.ebay.co.uk">www.ebay.co.uk</a></td>
<td>2007-11-30 16:06:51</td>
<td>10139</td>
<td>66.135.192.0/19</td>
<td>0</td>
<td></td>
<td>11643</td>
<td>4608 7474 7473 9299 10139</td>
</tr>
<tr>
<td>93</td>
<td><a href="http://www.ebay.co.uk">www.ebay.co.uk</a></td>
<td>2006-11-30 03:28:16</td>
<td>4761</td>
<td>66.135.192.0/19</td>
<td>0</td>
<td></td>
<td>11643</td>
<td>4608 1221 4637 4761</td>
</tr>
<tr>
<td>96</td>
<td><a href="http://www.mediafire.com">www.mediafire.com</a></td>
<td>2006-11-09 09:58:40</td>
<td>29449</td>
<td>38.0.0.0/8</td>
<td>0</td>
<td></td>
<td>174</td>
<td>513 286 5602 29449</td>
</tr>
<tr>
<td>104</td>
<td><a href="http://www.sendspace.com">www.sendspace.com</a></td>
<td>2006-11-09 09:58:40</td>
<td>29449</td>
<td>38.0.0.0/8</td>
<td>0</td>
<td></td>
<td>174</td>
<td>513 286 5602 29449</td>
</tr>
<tr>
<td>108</td>
<td><a href="http://www.megaflirt.com">www.megaflirt.com</a></td>
<td>2007-11-30 16:06:51</td>
<td>10139</td>
<td>69.5.88.0/24</td>
<td>0</td>
<td></td>
<td>29748</td>
<td>4608 7474 7473 9299 10139</td>
</tr>
</tbody>
</table>
Interesting (previously unknown) hijacks

• 11/30/2007 - AS 10139 (Smart Broadband PH) announced 23 specific prefixes, including prefixes for 13 of the top 500 Alexa websites:
  - youtube.com, live.com, msn.com, myspace.com, ebay.com, friendster.com

• 5/8/2007 - AS 21318 (Norwegian Open Peering) hijacked facebook.com’s website prefix

• 11/30/2006 - AS 4761 (INDOSAT) announced 4,035 prefixes it did not own, including the prefixes owned by:
Conclusions

• It is possible to protect networks without global cooperation
  • Simple anomaly detector coupled with a soft, but effective, response mechanism

• Partial deployments may be preferable, and equally effective

• The IAR is ready for testing now

• PGBGP is implemented in Quagga, undergoing testing
Thank you!