BGP protection without global cooperation

Josh Karlin\textsuperscript{1} \hspace{1cm} Stephanie Forrest\textsuperscript{1,2} \hspace{1cm} Jennifer Rexford\textsuperscript{3}

\textsuperscript{1}University of New Mexico

\textsuperscript{2}Santa Fe Institute

\textsuperscript{3}Princeton University

NANOG 41
October 16th 2007
Last time... Pretty Good BGP (PGBGP)

- Autonomous security for autonomous systems
  - No PKI
  - No sensitive network information revealed
  - Immediate protection for early adopters
Last time... Pretty Good BGP (PGBGP)

• Hijack detection
  • Routes with new origin ASes for a prefix are suspicious

• Notification
  • Internet Alert Registry
  • Notifies affected operators of suspicious routes
  • http://iar.cs.unm.edu

• Router alteration
  • Temporarily depreferences suspicious routes
  • Prevents the propagation of hijacks while notified operators intervene
PGBGP was vulnerable to malicious adversaries

- Adversary could use spoofed edges (e.g. prepend legitimate origin to path)

- Adversary could announce a path which violates contractual policy
Impact of exploits and misconfigurations

- Sub-prefix hijack
- Prefix hijack
- Spoofed prepend
- Policy violations

Fraction of ASes routed to attacker:
- 100%
- 80%
- 60%
- 40%
- 20%
- 0%
Pretty Good BGP today

- Detection
  - Hijacks, spoofed edges, and policy violations

- Internet Alert Registry
  - True positive only notification

- Router alteration
  - Implementation in the works, for Quagga/Zebra
Enhancements to detection algorithm

- Detecting spoofed edges is easy
  - Monitor edges in use, flag new edges as suspicious

- In response, lower the local preference for 24 hours
Enhancements to detection algorithm

- Detecting spoofed edges is easy
  - Monitor edges in use, flag new edges as suspicious

- In response, lower the local preference for 24 hours
- This can also detect policy violations!
Policy violations produce new edges

• 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)
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
  - RSS feed of alerts
IAR Tracker

• We have created a program (the IAR Tracker) that will regularly scan the IAR RSS feed and compare it to your network’s topology database
  • Programatically check for new alerts that pertain to your network
  • Filter out all but true positive alerts
  • Without revealing any network information!
Evaluation

- Is it effective?
- Are there a lot of false positives?
- How will false positives affect my network?
Would a partial deployment be effective?
Are there a lot of false positives?

- Yes
- The IAR discovers ~200 anomalies per day, some could be false
How will false positives affect my network?

- **Reachability is not lost!**
  - Suspicious routes are depreferenced, not discarded
- Many false positives are brief (e.g. due to flaps)

![Graph showing fraction of New Origin ASes, New Sub-Prefixes, and New Edges over time.](image)
Conclusions

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

• The IAR is ready for testing now

• Prototype router implementation available soon
  • The University of New Mexico ITS is helping to test the routing implementation
  • Additional help would be appreciated
Thank you!

http://iar.cs.unm.edu/