Buddyguard: A Buddy System for Fast and Reliable Detection of IP Prefix Anomalies

Jun Li
Toby Ehrenkranz
Paul Elliott

at: ICNP
October 31, 2012
Routing Anomalies with an IP Prefix

- An IP Prefix (i.e. a block of IP addresses) can undergo many types of routing anomalies
  - The most well-known is probably prefix hijacking
  - Others include being unreachable, poorly reachable, or pathological routing dynamics
- Often not noticeable
- Consequences: loss of business, identity theft, or many other devastating effects
Problem Statement

- How can we monitor IP prefix anomalies reliably, even with the countermeasures from attackers?
Our Research

- **Research Goal**: investigate, design, and evaluate a new approach to reliable monitoring of IP prefixes.

- **Our Idea**: Surround a prefix with a buddy system, and monitor the behavior of the prefix against that of its buddies.
Outline of This Talk

- State of the art and limitations
- Overview of Buddyguard
- Design of Buddyguard
- Evaluation
- Discussions and conclusions
State of the Art and Limitations
State of the Art

- Mostly on prefix hijacking
- With limitations
  - Not comprehensive: Sub-prefix hijacking, prefix interception, etc. can go undetected
  - Not robust: Intelligent attackers can circumvent them
  - Largely due to inadequate estimation on what prefix hijackers can do
Overview of Buddyguard
Main Idea

- Surround a prefix with a buddy system composed of buddy prefixes, or buddies
- Monitors the behavior of the prefix against that of its buddies
The Internet
The Internet

monitor

p
The Internet

monitor

p
Define (Ab)normality via Buddies

- Key to monitoring an IP prefix is to know what is normal and what is not

- When inspecting a prefix in isolation, it is difficult to know what behaviors are abnormal
  - Use historical behavior? But some new behavior can be normal too
  - Specify what is normal or abnormal? But hard to specify all cases

- A buddy system, however, allows a prefix to be compared with its buddies to determine its normality on the fly
  - Similar to (most) buddies? Normal. Otherwise, Abnormal!
Advantages of Buddyguard

- **Resilient**
  - A prefix is allowed to have hundreds or even thousands of buddies from different ASes

- **Deployable**
  - Only passive measurement using existing BGP monitoring systems is required

- **Extensible**
  - One always can first determine the type of the behavior and how to measure it, and then select its buddies in terms of that behavior
Design of Buddyguard
Buddy Discovery, Selection, and Maintenance

- What prefixes can be buddy candidates?
- Which candidates to select as buddies?
- How to maintain a good buddy system after initial selection?
- prefix/buddy candidate  

  AS  

  → AS path from m to p
- prefix/buddy candidate
- AS
- AS path from m to p
- prefix/buddy candidate
- AS
- AS path from m to p
- prefix/buddy candidate
- AS
- AS path from m to p
- prefix/buddy candidate
- AS
- AS path from m to p
- prefix/buddy candidate
- AS
- AS path from m to p
Buddy Selection

- Which buddy candidates to select as buddies?
- We observe buddy candidates during a training period
- And apply the skewer mechanism
Skewer Mechanism
Skewer Mechanism

- Choose those that
  - most frequently show path similarity,
  - ensure enough buddies exist for every path switch, and
  - ensure topological diversity (i.e. from multiple different ASes).
Evaluation
Tested Prefix Hijacking Events

- May 7, 2005—Cogent hijacked one of Google’s prefixes
- January 22, 2006—Con Edison hijacked 30+ prefixes, including some belonging to their customers
- February 24, 2008—Pakistan Telecom hijacked a sub-prefix of YouTube’s prefix
Tested Route Leak Events

- April 4, 2010—China Telecom leaked many IP prefixes from roughly 15:54 UTC to about 16:10 UTC
Cogent Hijacking Google

![Graph showing the percentage of monitors raising warning signals over time.]

- **Origin Buddies**
- **Parent Buddies**
- **Sibling Buddies**

**Y-axis:** Percentage of monitors raising warning signals

**X-axis:** Time (hours)
Hijacked prefix is the only prefix at the origin AS, so there is no origin buddies.
Pakistan Hijacking YouTube

![Graph showing percentage of monitors raising warning signals over time](image)

- **Origin Buddies**
- **Parent Buddies**
- **Sibling Buddies**

Time (hours)

0 1 2 3 4 5 6 7 8

Percentage of monitors raising warning signals

0 20 40 60 80 100
China Telecom Route Leaks

![Diagram showing the percentage of monitors raising warning signals over time for Origin Buddies, Parent Buddies, and Sibling Buddies. The x-axis represents time, ranging from 0 to 1, and the y-axis represents the percentage of monitors raising warning signals, ranging from 0 to 100. The Origin Buddies line is in red, the Parent Buddies line is in magenta, and the Sibling Buddies line is in cyan. The graph shows peaks in warning signals at certain times for all three types of buddies.]
False Alerts

CDF

Percentage of monitors raising warning signals

warnings / decision windows

Time

Jun Li
Discussions & Conclusions
Deploying Buddyguard

- RouteViews/RIPE BGP collectors
- BGP speakers
- Anywhere in the Internet
  - need to access BGP data in real time, such as through BGPMon
Attacking Buddyguard

- Can an attacker hijack all the buddies of a prefix to stay undetected?
- Can an attacker announce an illegitimate path that is not visible to monitors?
Conclusions

- Every IP prefix on the Internet may experience certain anomalies without being detected. And attackers are smart!
- Buddyguard monitors a prefix’s behavior on the fly via a buddy system
- Results are promising
- More details in the paper
Buddyguard: A Buddy System for Fast and Reliable Detection of IP Prefix Anomalies

Jun Li
Network Security Research Laboratory
University of Oregon
Email: lijun@cs.uoregon.edu
http://www.cs.uoregon.edu/~lijun

This research is supported by the USA National Science Foundation under Award No. CNS-1118101. Any opinions, findings, and conclusions or recommendations expressed in this research are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.