Alerting prefix owners of hijacks in near-real time

Mohit Lad
UCLA

Joint work with:

Dan Massey, Colorado State University
Yiguo Wu, and Lixia Zhang; UCLA
Beichuan Zhang; U. Arizona
Dan Pei, AT&T Research

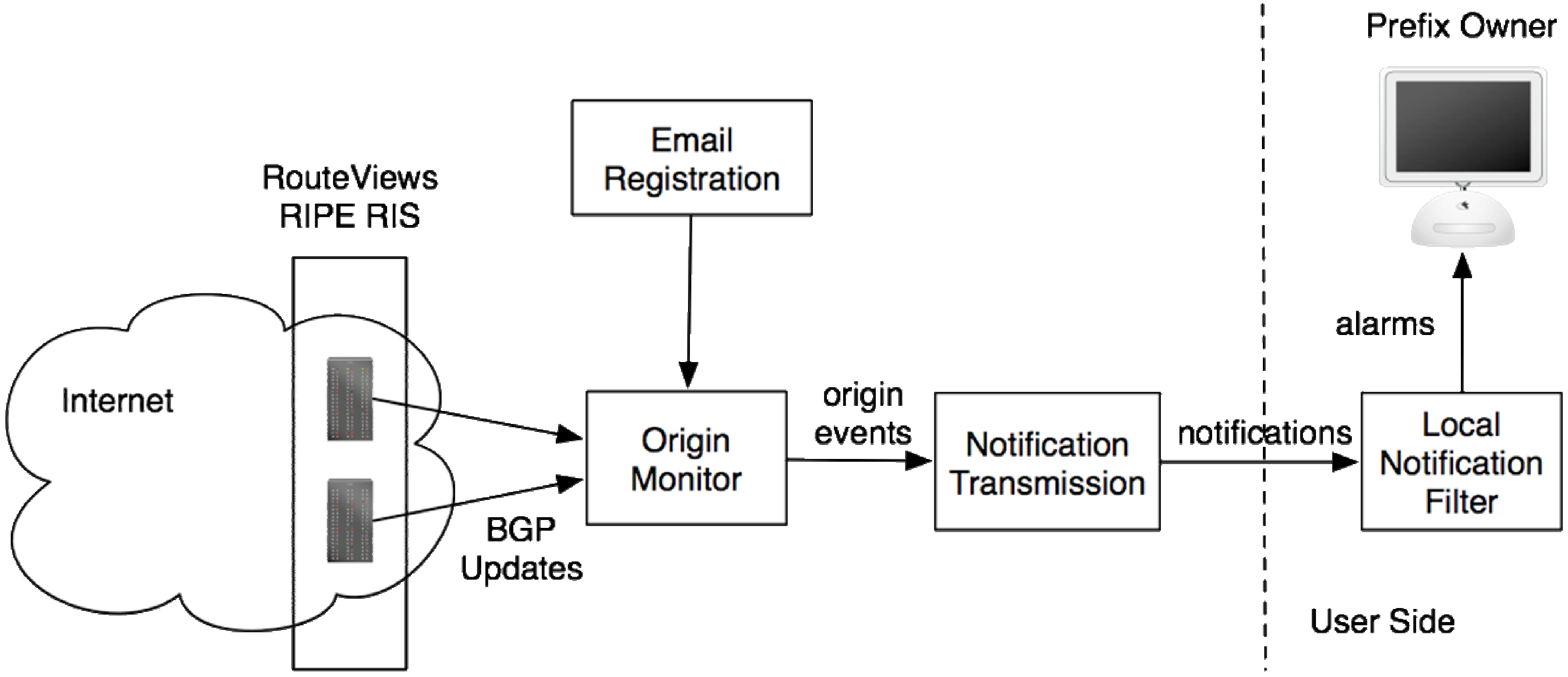
Prefix Hijack

- Three properties of a security solution
  1. Ability to see “bad” information
  2. Ability to distinguish between “good” and “bad” information
  3. Incentive to fix the problem
- Data collectors (RouteViews and RIPE)
  - Possess property 1.
- Prefix owners
  - Possess property 2 and 3 for their prefixes.
- Key is to combine all three

The PHAS (Prefix Hijack Alert System) Approach

- Use updates from existing BGP Monitors (RouteViews and RIPE RIS)
  - If a false origin is announced, high probability some monitor will see it
- Record any change in origins for a Prefix
  - Appearance of a new origin prefix (report immediately)
  - Disappearance of an existing origin (slight delay fine)
- Send Report To Prefix Owner
  - Very difficult for remote observer to determine which origins valid
  - Trivial for prefix owner to determine which origin is valid.

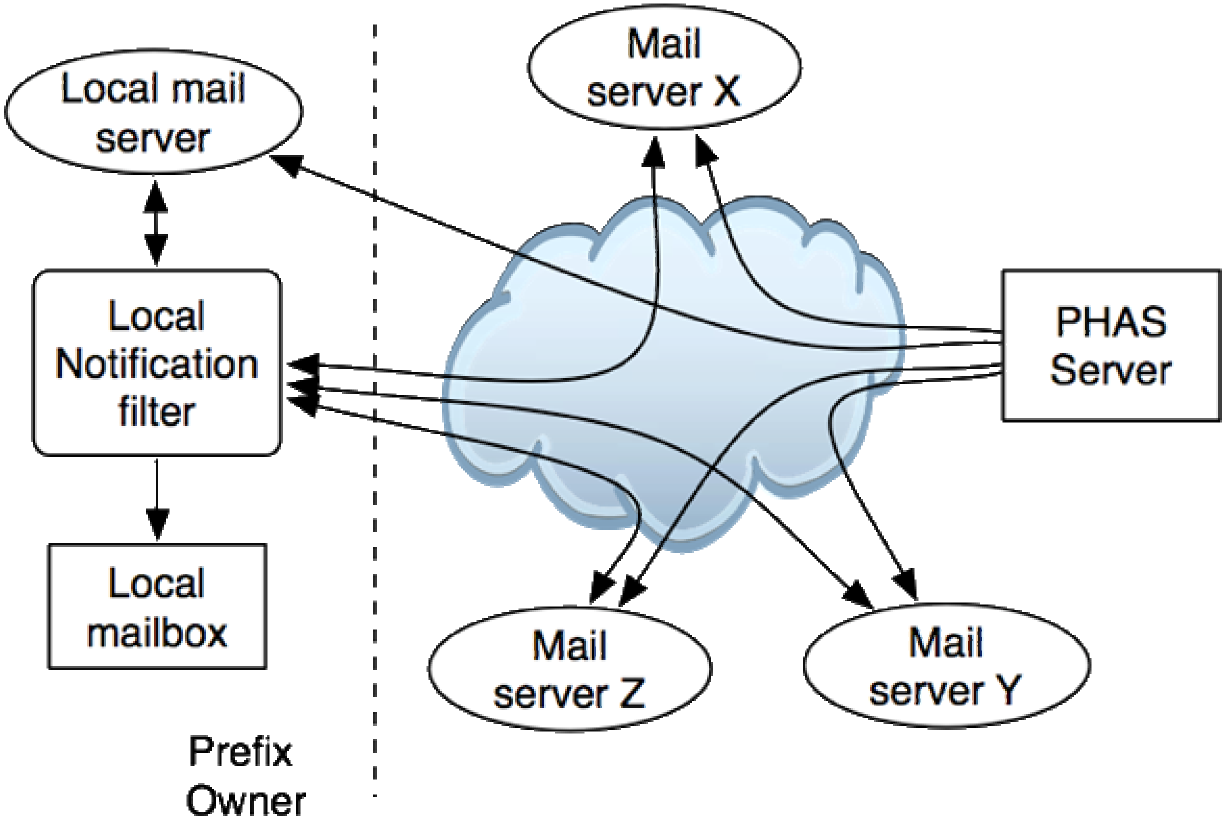
Components of PHAS



Push Complexity of detection to user

Message Delivery

Apply local rules before generating alarms

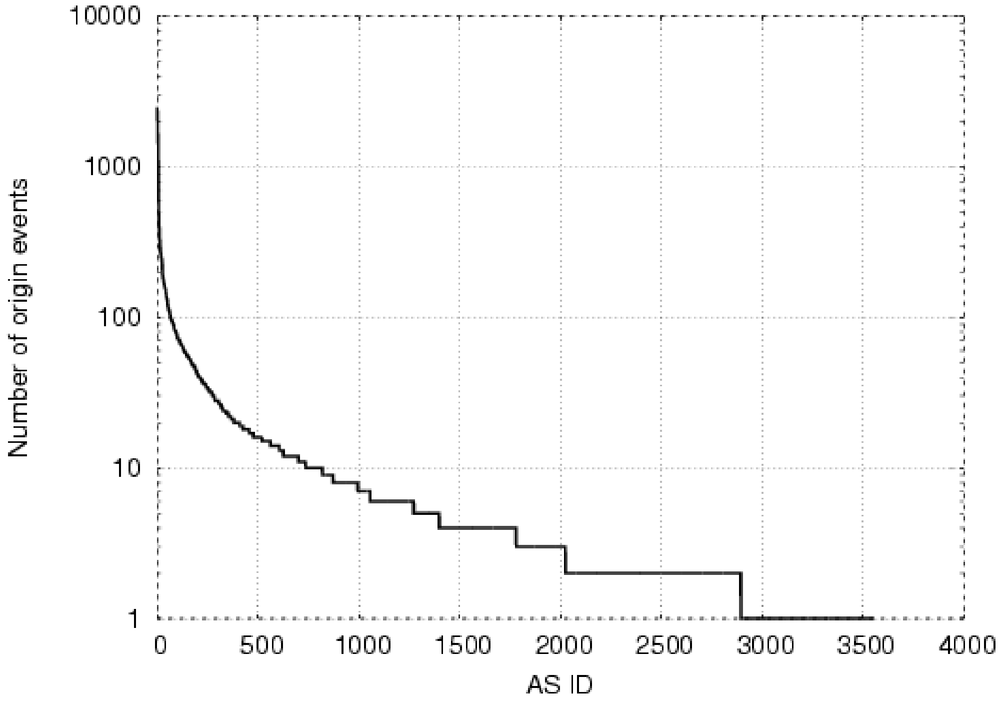


All messages are authenticated by PHAS server

Key: Due to topological mesh-ness, its difficult for a hijacker to receive all notifications

Evaluation: Messages per AS

- Period December 2005
- Map prefixes to origin AS using Routing table
- Most AS receive less than 100 messages per month.
  - Local Filters can remove valid origin changes



Advantages

- Readily deployable
  - RouteViews and RIPE RIS already collect data
- Alarm generation not dependent on
  - co-operation from other networks
  - Monitor knowing correct origins
- Alarm authentication: single source
- Low overhead

Summary

- Comprehensive study using archived data
- Developing near real-time system
- Interested in receiving notifications
  - Send email to
    - mohit@cs.ucla.edu
    - massey@cs.colostate.edu
- Ongoing efforts
  - Covered prefix hijack
  - False last hop
- Reference:
  - "PHAS: A prefix hijack alert system", to appear in USENIX Security 2006