

Autonomous Security for Autonomous Networks

Stephanie Forrest, Josh Karlin, and Jennifer Rexford

<http://cs.unm.edu/~karlinjf/pgbqp/>

NSF Grant: CCR-0331580



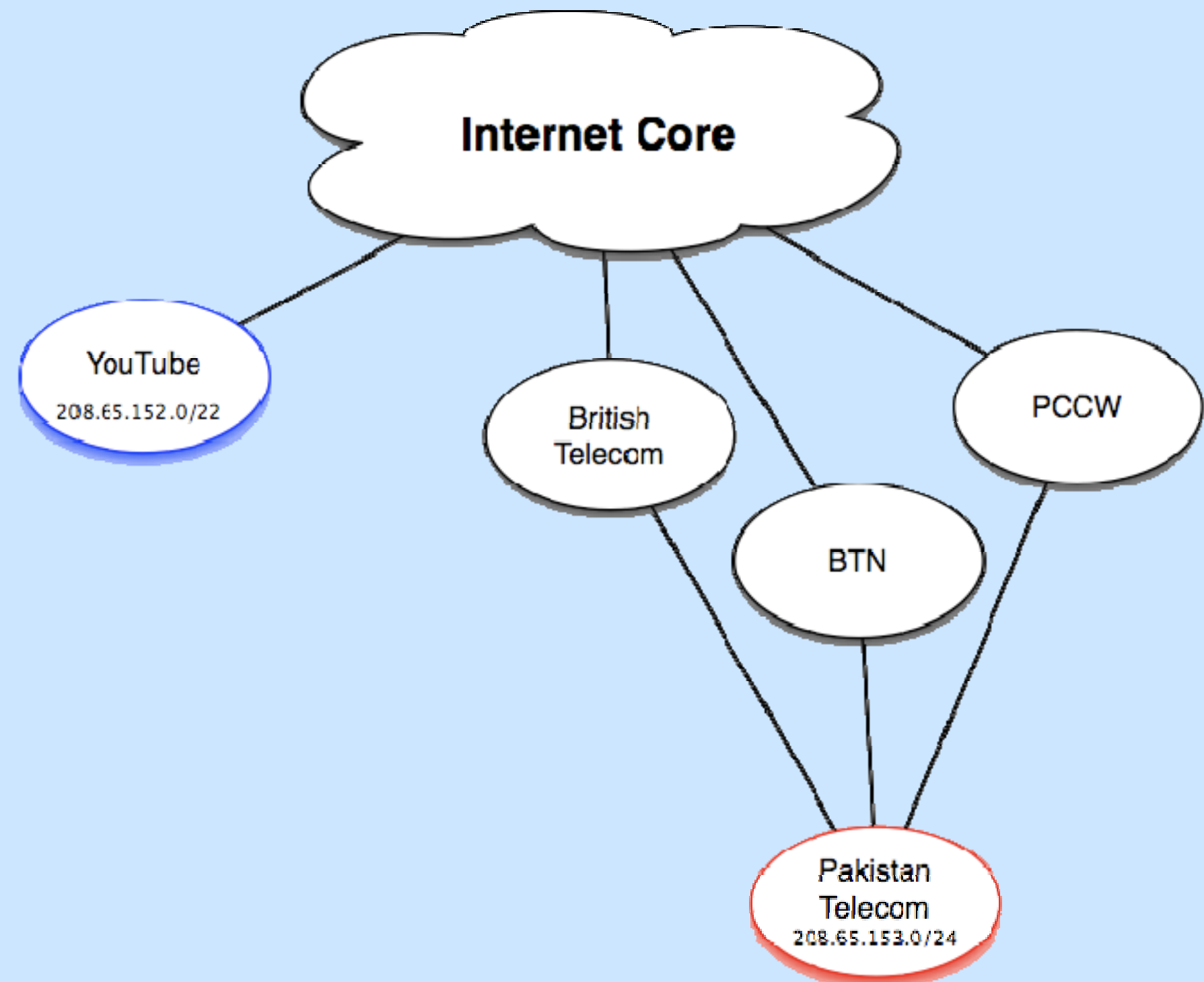
Problem

BGP routing messages are not verified. Any BGP router can announce IP address space owned by another network.

Example: YouTube hijack

- Pakistan announced IP block (prefix) 208.65.153.0/24 on Jan. 24th 2008
- Which is a sub-prefix of YouTube's 208.65.152.0/22
- PT's provider, PCCW, forwarded the route. The other providers filtered it out.
- Longer prefixes are preferred at forwarding time

Result: YouTube traffic was sent to Pakistan Telecom for two hours.



Pretty Good BGP: Anomaly Detection and Response

Detection

- Routes that contain new data (prefix origins and edges) are considered anomalous
- Anomalous routes distributed to appropriate network operators via opt-in service "Internet Alert Registry"

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

Response

- Anomalous routes are depreferenced by BGP routers for 24 hours
- When possible, choose trusted routes
- Propagation of new information is slowed to the human time scale, giving operators a change to fix routes before they become a problem

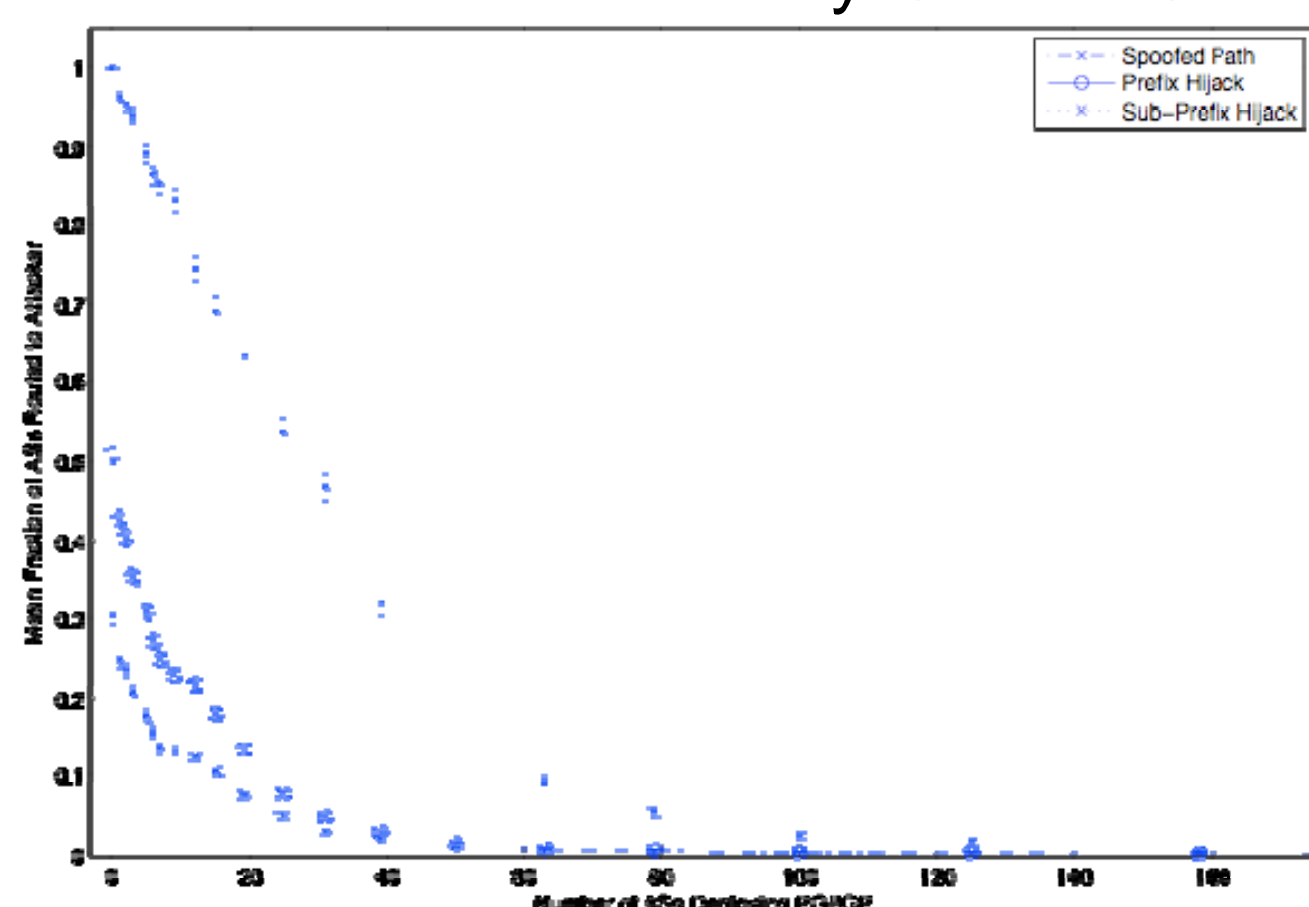
Why not use an authenticated registry?

- Companies consider the requisite information to be proprietary
- Little incentive for early adopters
- Would force centralization on a decentralized system
- For example, a PKI

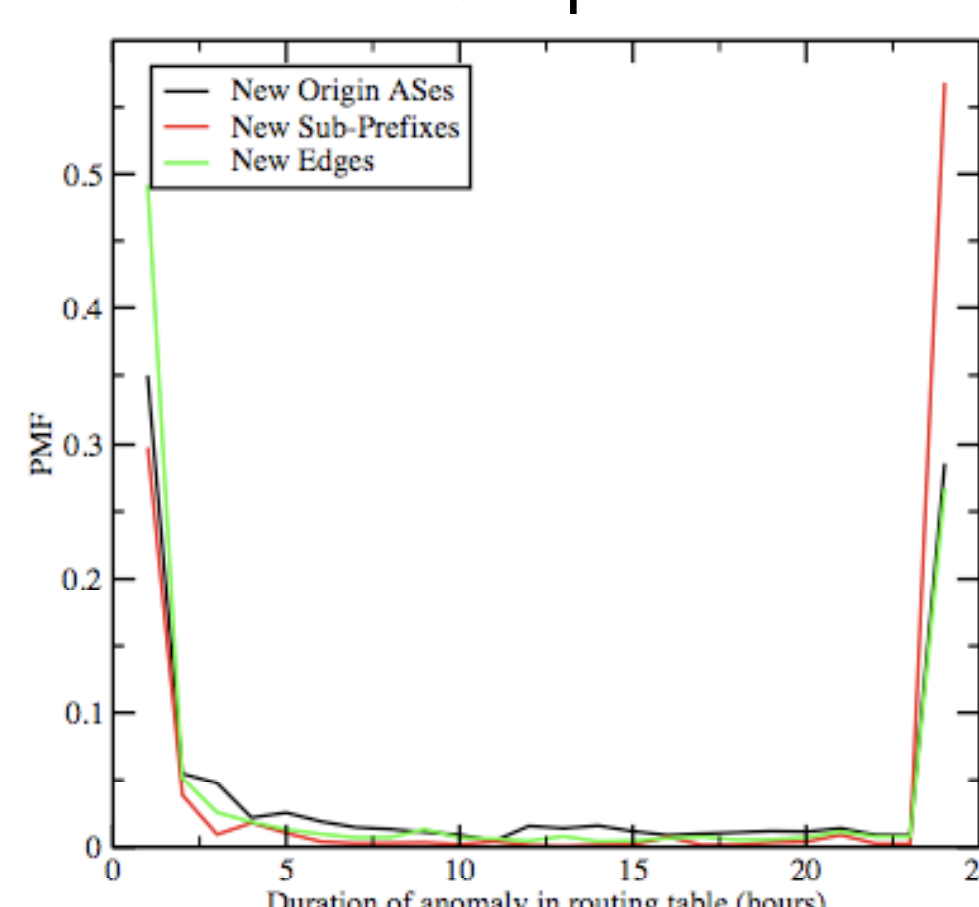
PGBGP Strengths

- Incentive for early adopters (see figure 1)
- Plausible deployment path
- Blocks short-lived anomalies (misconfigurations)
- And allows legitimate new routes to propagate
- See figure 2
- Comparable in strength to SBGP, soBGP, psBGP
- For example, a PKI

Effectiveness of Pretty Good BGP



Behavior of Suspicious Routes



References:

Josh Karlin, Stephanie Forrest, and Jennifer Rexford, "Pretty Good BGP: Improving BGP by Cautiously Adopting Routes", 14th IEEE International Conference on Network Protocols, November 2006.

Josh Karlin, Stephanie Forrest, and Jennifer Rexford, "Autonomous Security for Autonomous Systems, Journal of Computer Networks, In Press.

P. Holme, J. Karlin, and S. Forrest "Radial structure of the Internet." *Proc. Royal Academy A* 463:1231-1246 (2007).

P. Holme, J. Karlin, and S. Forrest "An integrated model of traffic, geography and economy in the Internet." *ACM SIGCOMM Computer Communication Review* (submitted) <http://arxiv.org/abs/0802.3283v1>