NIST
National Institute of Standards and Technology
U.S. Department of Commerce

BGP Security:

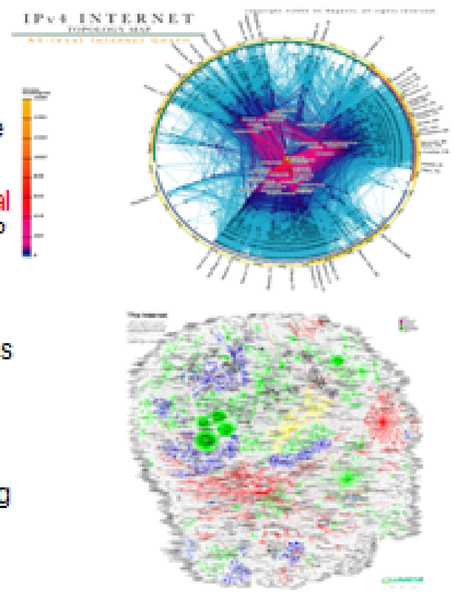
INFORMATION TECHNOLOGY LABORATORY

Securing the Internet's Global Routing Infrastructure

http://www.antd.nist.gov/bgp_security/

Border Gateway Protocol (BGP)

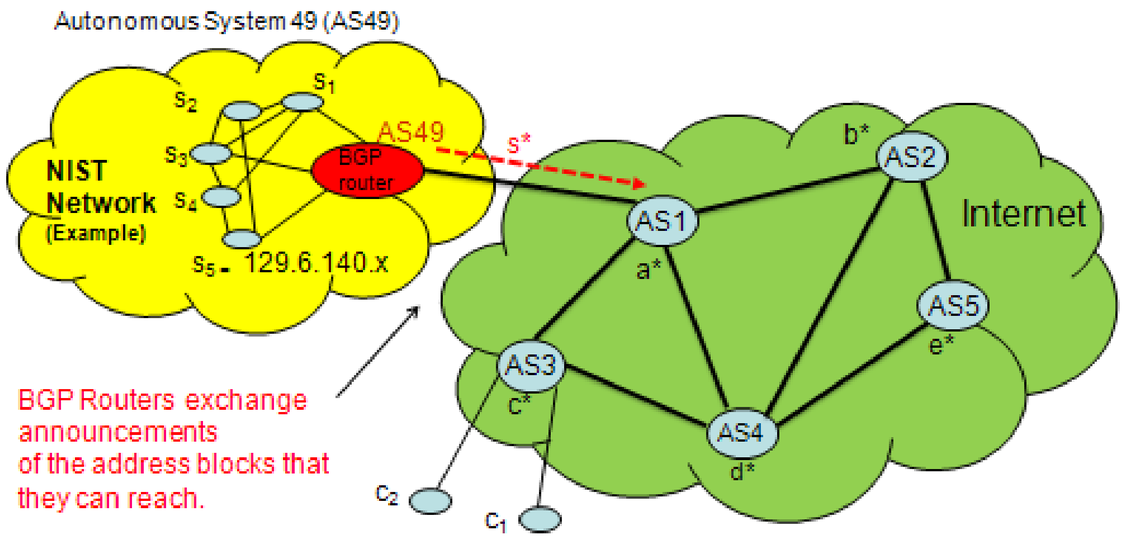
- Glue that enables the Internet
  - BGP is a live distributed system spanning the globe; comprised of ~30K distinct administrative domains and millions of routers.
  - BGP issues are technical, economic and political Effectively enables the business model(s) of ISP interconnection.
- BGP Robustness Concerns
  - No security model - subject to malicious attacks and large scale misconfigurations.
  - Emergent Behaviors - behavior of global BGP system poorly understood.
  - Scaling concerns – system dynamics operating at the edge of the envelope.



Inter-Network of Autonomous Systems

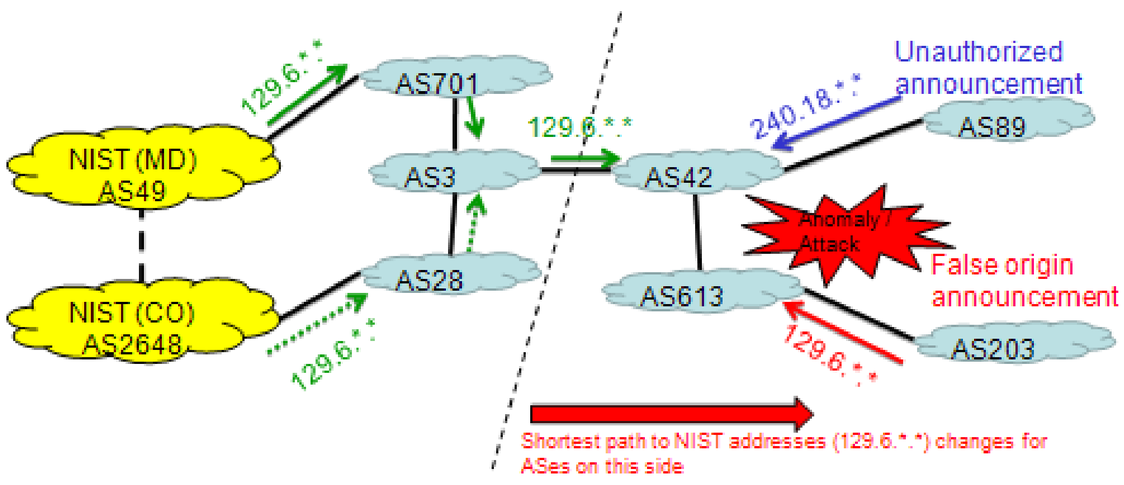
NIST owns IP address block: s* = 129.6.x.x = 129.6/16 = 129.6.0.0 → 129.6.255.255

Autonomous System 49 (AS49)



BGP Routers exchange announcements of the address blocks that they can reach.

BGP Robustness Problem Space



- Misrouting of traffic
- Unauthorized routing
- Denial of Service

How can we validate ownership of address blocks and the advertised paths used to reach them?

BGP Threats / Risks

What Can Happen?

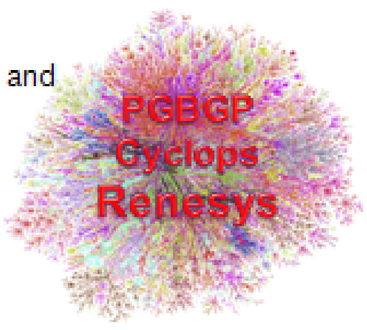
- Redirecting Data Traffic
  - Detour data traffic to eavesdrop, man-in-the-middle security mechanisms, cause delay and/or disrupt traffic. Traffic eventually makes it to real destination, but not over the path you thought.
  - Misdeliver data traffic to malicious endpoints.
  - Hijack address space (both unallocated and allocated) to use as a launching pad for spam, attacks, etc.
  - Deny service – "black hole" entire networks so that others can not reach them.
- Attacking the BGP System.
  - Cause Routing Instability - by injecting bogus advertisements into the system that effect global BGP stability/control algorithms.
  - Overload Routing System – by injecting a volume of updates that exhausts the processing power of router's control plane.

What Does Happen?

- 2008-08 DEFCON Demonstration of stealthy BGP misrouting for purposes of eavesdropping.
  - http://www.wired.com/threatlevel/2008/08/revealed-the-in/
- 2008-02 - Pakistan Telecom purposeful hijack/backhole of YouTube.
  - http://www.dpe.net/news/study-youtube-hijacking.html
- 2006-01 – Con-Edison hijacks majority of Internet
  - http://www.dpe.net/news/study-youtube-hijacking.html
- 2004-12 TTNet in Turkey hijacks the Internet
  - http://www.renesys.com/blog/2009/12/internet-wide-near-catastrophe-in-turk.shtml
- 2004-05 Malaysian ISP blackholes Yahoo.com
- 2003-05 Spammers hijack Northrop Grumman address space.
- ..... These are examples that made the news. It happens every day.

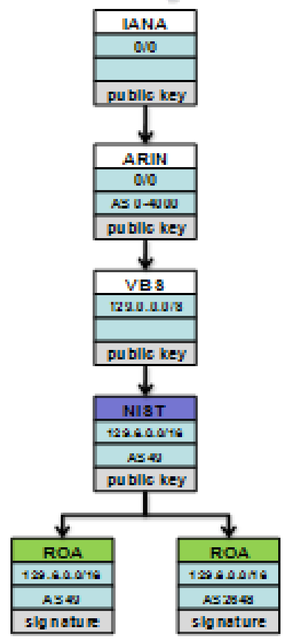
Remedies for the BGP Vulnerabilities

- Cryptographic Security Mechanisms
  - Deploy global Resource PKI (RPKI) to validate address ownership and routing relationships.
  - Develop tools to automate route origin validation based upon RPKI data.
  - Develop security extensions to BGP to further use RPKI to validate the full AS Path.
- Data Driven Robustness Mechanisms
  - Exploit existing global registries of addressing and routing arrangements (Registry data)
  - Exploit BGP monitoring and measurement infrastructures (History Data)
  - Develop automated route filtering capabilities, anomaly detection systems.



RPKI – The Corner Stone of BGP Security

- Resource Public Key Infrastructure
  - Global PKI of limited scope/purpose.
  - RPKI Components
    - Certificate Authorities
    - End Entity Certificates
    - Route Origin Attestations
  - Possession of certificate indicates ownership of resource (address block, or AS number).
    - Not identity certificates. Doesn't identify the name of the owner, only that the holder of the Cert is the owner. Much like the key to your office.
  - Validation of RPKI components follows chain of trust up towards one or more trust anchors.
- RPKI Uses to Secure Routing.
  - ROAs – can be used to validate the right of an AS to announce a given address block, thus preventing false origination.
  - EE Certificates for AS ownership can be used to digitally sign the PATH that BGP announcements follow, thus preventing misrouting.



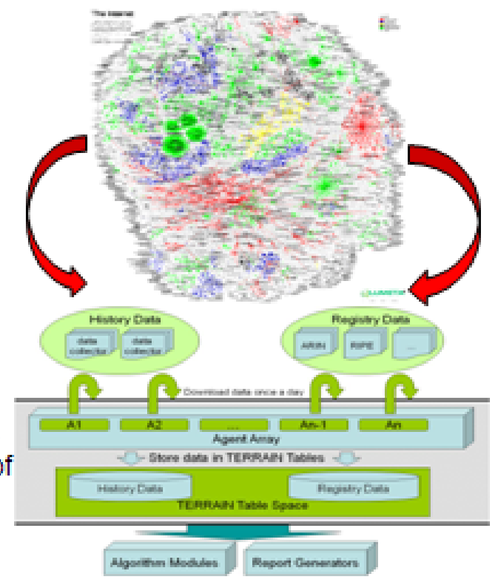
Data Driven BGP Robustness

What are the Data Sources?

- Addressing Registries
  - global databases of address block and autonomous system number assignments.
- Routing Registries
  - loosely maintained global databases of contractual relationships for routing services.
- Monitoring Data
  - public BGP monitoring and measurement projects that collect BGP protocol exchanges at various spots around the Internet.

Why is this hard?

- Registries
  - known to be incomplete and inaccurate, and are maintained in differing formats, by differing processes in different regions of the world.
- Robustness Algorithms
  - to be effective, must make precise policy decisions from highly imperfect data.
- Needle in a Hay Stack
  - millions of BGP update messages per day, millions of registry entries, rare but potent threats.

Test and Measurement of BGP Robustness Mechanisms

- TERRAIN
  - NIST Evaluation Framework
  - Continuously extracts Internet's registry and BGP monitoring data.
  - Unified data model for storing disparate data sources.
  - Research platform for the design and analysis of robustness mechanisms.
  - Information quality measurements of registry data.
- Results
  - TERRAIN system developed and operational.
  - Comprehensive analysis of quality and utility of RIR/IRR Registry Data.
  - Analysis of data driven BGP robustness systems.