BGP Security: 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 updates are technical, economic and political.
  - Effectively enables the business models of BGP interconnection.

- BGP Robustness Concerns
  - No-secure 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: 129.0.6.6 / 129.0.0.0 - 129.255.0.0
Autonomous System 44 (AS44)

BGP Routes 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?

Unauthenticated announcement
Unauthenticated announcement

BGP Threats / Risks

What Can Happen?
- Redirecting Data Traffic
  - Leverages conflicting policies in existing, non-mutually adversarial, but in the same administrative domain's BGP sessions.
  - Requires sink to have the same policies.
  - Injection of false routes to lead to desirable traffic.

What Does Happen?
- 2002-03 DCFCC Demonstration of stealthy BGP hijacking for purposes of worms.
  - 2005-06 - Facebook/AT&T routing hijacking.

RPKI – The Corner Stone of BGP Security

- Resource Public Key Infrastructure
  - Global PKI of limited scope/purpose.
  - RPKI Components
    - Resource Object
    - Resource Key
    - Path Certification
    - Path Validation
  - Possession of certificate indicates ownership of resource (address block, or AS number).
  - Non-identity certificate does not identify the name of the owner, only that the holder of the path is a trusted one.
  - Validation of RPKI components follows the trust path from one or more trusted anchors.
  - RPKI Uses to Secure Routing.
    - RGAs - can be used to validate the right of an AS to announce a given address block, thus preventing fake origin.
    - CE Certificates for AS ownership can be used to digitally sign the PATH in BGP announcements, thus preventing misrouting.

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.

Data Driven BGP Robustness

What are the Data Sources?
- Addressing Registries
  - global databases of address block and autonomous system number assignments
- Routing Registries
  - loosely managed 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?
- Registration
  - 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 policy decisions from highly imported data.
  - Needle in a Haystack
  - 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.
  - Unifies 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 RPKI Registry Data.
  - Analysis of data driven BGP robustness systems.