
# CSRIC IV
# Working Group 6
# Long-Term Core Internet Protocol Improvements

March 20, 2014

William Check, CTO, NCTA
Working Group 6 Chair

# WG6 Members

- Alliance for Telecommunications Industry Solutions
- AT&T
- Bank of America
- CableLabs
- Center for Democracy & Technology
- CenturyLink
- Cisco
- Comcast
- Cox
- CTIA
- Farsight Security
- Goldman Sachs
- Google
- Internet Identity
- NCTA
- NIST
- Nsight
- Princeton University
- Renesys
- Shadowserver
- Sprint
- Time Warner Cable
- University of Oregon
- Verizon
- Verisign
- Xerocole

# WG6 – Subgroup Descriptions

**DNS**

- Matt Tooley (NCTA), subgroup chair
- The protocols used to govern the operation of the Internet Domain Name System (DNS) are vulnerable to spoofing attacks.

**Inter-Domain Routing**

- Tony Tauber (Comcast), subgroup chair
- The protocols used to govern the operation of the Internet's crucial inter-domain routing system are vulnerable to route hijacking attacks.

# DNS Subgroup Mission

- DNS Open Resolvers
  - A DNS open resolver will resolve queries from any external location even if they are not part of its administrative domain
  - Open DNS resolvers are frequently the source of DDoS attacks

- WG6 Mission/Scope for DNS Sub-team
  - The DNS sub-team will identify and recommend best practices for use by the Internet ecosystem (ISPs, ASPs, and CPE vendors) for mitigating issues related to DNS Open Resolvers

# DNS Subgroup

- Reviewing and analyzing the issue with DNS Open Resolvers
- Identified the initial key findings
- Cross-mapping industry reports and recommendations to group's initial findings
- Identified an initial list of recommendations
- Began discussions on tracking progress on the issue
- Draft of interim report ready for review by subgroup

# DNS Next Steps

- Survey past and present projects and activities
  - Coverage and Goals
  - Methodology
  - Operational status
- Attempt to identify recommended methods for tracking progress
- Finalize interim  and final report

# Inter-Domain Routing Subgroup

- Review of recent Internet route hijacking incidents and review of CSRIC III recommendations to determine if updates are needed.
- Analyze methods and procedures to quantify routing anomalies and attacks.
- Describe practical steps for deployment of protocol extensions (e.g., RPKI) and possible benefits for incremental deployment.
- Develop methods to detect reachability issues related to deployment of RPKI or other protocol extensions.

# Routing Security Next Steps

- Characterize and analyze recent events
- Survey past/present projects and activities categorizing their:
  - Coverage and Goals
  - Methodology
  - Operational status
- Develop taxonomy of routing measurements

# Routing Security Events and Terms

- Characterize and analyze recent events
  - Renesys report of traffic "hijack" via routing
    - Best practices may or may not help
    - Protocol extensions may or may not help
  - Chinese traffic event
    - Not routing related
    - Included to provide clarification
- Develop taxonomy
  - What exactly are we talking about?

# Routing Measurement Survey

- Examine past and current projects
  - Coverage and Goals
    - Break them down using the taxonomy
    - What do they try and do?
  - Methodology
    - What data sources do they rely on?
    - What logic do they apply?
  - Operational status
    - Can we rely on it sticking around?
    - Is it under a grad students desk?

# RPKI Deployment Aids

- What are possible playbooks for deploying?
  - Many operators currently lack expertise to know how to approach and break down the problem
- How would you know if you broke anything?
  - RPKI relies on views from (many) other (far flung) vantage points on the Internet
  - What could I measure to know if I caused a problem?