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

June 18, 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 - Status

- Reviewed and analyzed issues with DNS Open Resolvers
- Identified the key findings
- Cross-mapped industry reports and recommendations to group's findings
- Identified initial list of recommendations
- Looked the various Internet community projects that measure Open Resolvers
- Starting to begin the internal review and critique process of the draft

DNS Next Steps

- Develop final report
- Merge with BGP sub-group’s report
- On-track for September

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.

Inter-Domain Routing Status

- Reviewed recent routing security incidents
- Developed routing security taxonomy
- Reviewed existing measurement projects
- Developing guide for RPKI population/use
- Editing and assembling for internal review