



CSRIC IV

Working Group 6

Long-Term Core Internet Protocol Improvements

September 24, 2014

William Check, CTO, NCTA
Working Group 6 Chair

Tony Tauber, Comcast
Sub-Group Chair

Matt Tooley, NCTA
Sub-Group 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.

Route Hijacking

INTER-DOMAIN ROUTING SUB- GROUP

Routing Security Approach

- Taxonomy
 - Need clear and agreed upon terms to discuss a subtle and complex topic
- Recent Events
 - Much motivation and interest comes from recent events that appear related to routing security
- Tools and Measurement
 - Measuring the global routing system is not simple given it's size and characteristics

Taxonomy - 1

- Overload
 - Possible result of traffic misdirection
 - Network Links or Processors
- Black-hole
 - Used as a verb more often than a noun
 - Discarding of traffic by an intermediate node between source and destination

Taxonomy - 2

- Mis-Origination
 - A BGP routing announcement with an Origin AS (Autonomous System) which is unauthorized
- Hijack
 - Mis-origination or other malicious act intended to disrupt reachability of the legitimate destination
 - Could also enable traffic disruption, injection, eavesdropping, censorship, or analysis

Taxonomy - 3

- Leak
 - Propagation of routing announcements beyond the intended scope – usually accidental
 - Traffic follows an unintended path
 - Could enable eavesdropping or traffic analysis
 - May or may not lead to black-hole or overload

Recent Internet Routing Incidents

- Belarus and Iceland Hijack Report
 - Mis-origination with possible ISP cooperation
 - Perhaps motivated by eavesdropping/injection
- Chinese Traffic Incident
 - Overload negatively affected a US operator
 - Caused by DNS, not Routing
- Indosat (Thailand) Incident
 - Vanilla leak, apparently unintentional

Tools and Measurements -1

- Purpose
- Coverage
- Enterprise Type
- Data Sources/Components
- Operational Status

Tools and Measurements - 2

- Tools vary in their intended goal
- Measurements vary in their coverage
- Many academic, fewer commercial
- Most depend on a small set of collection projects (Routeviews, RIPE RIS)
- Many measurements are done in an academic context
 - Availability and long-term support varies greatly

Routing Security Recommendations

- Best Practices a la CSRIC III Working Group 4
 - Route filtering, source address validation
- Monitor protocol development/enhancement in IETF SIDR Working Group
 - RPKI Origin Auth, BGP Path Security
- Continue involvement with RPKI
 - Register Objects
 - Experiment with data and relying-party software

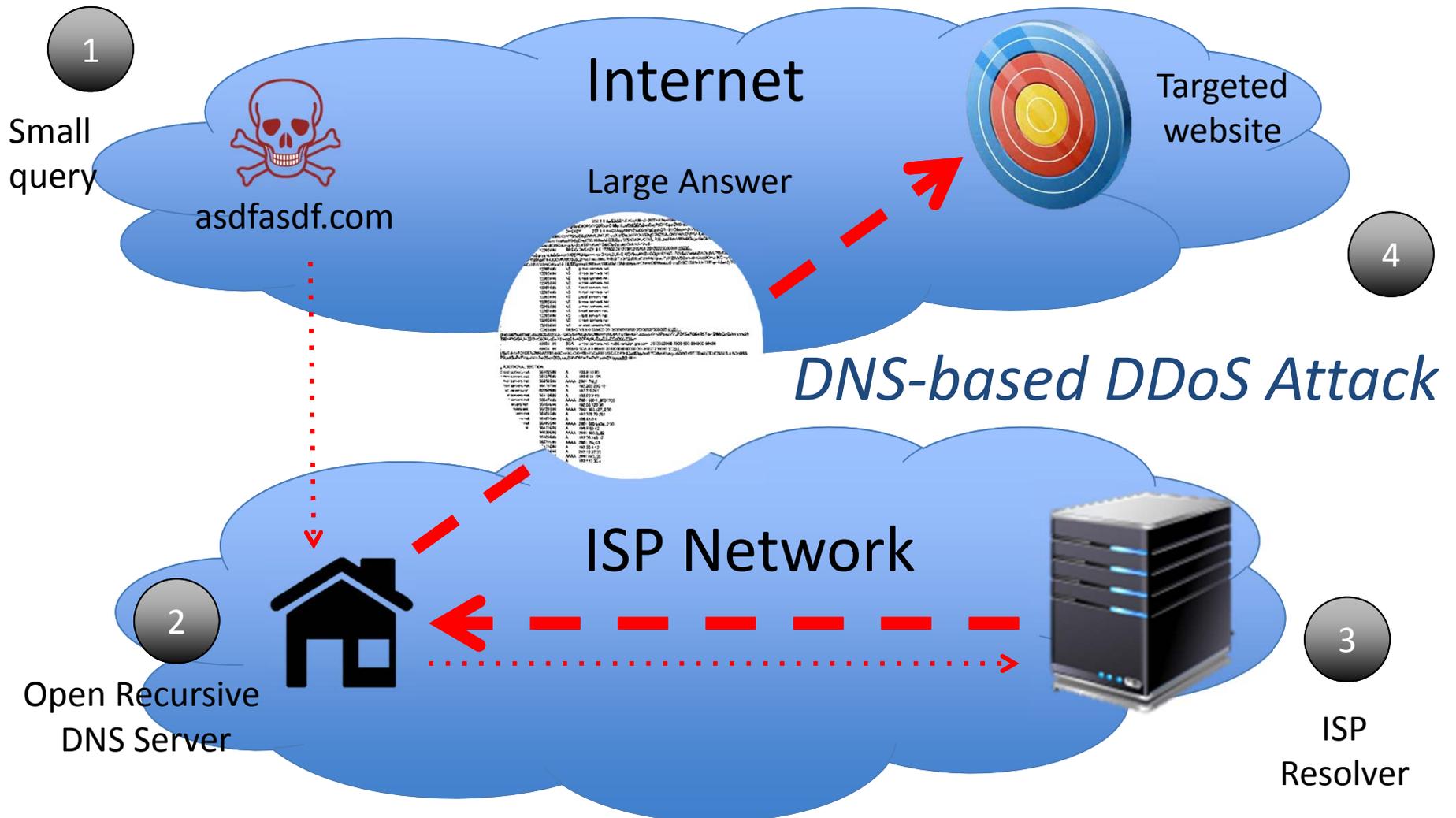
RPKI Getting Started Guide

- Intended to be a plain-language guide
- Separate from technical specifications such as IETF RFCs
- Separate from involved parties such as Regional Internet Registries (RIRs)

Open Recursive DNS Servers

DNS SUB-GROUP

Scope: Open Recursive DNS Servers



Methodology



Findings

- Issue of open recursive DNS servers is not a new problem
- DNS by itself is not the problem, the problem lies with the underlying protocol – UDP
- Attacks using the DNS attack surface have continued and increased since CSRIC III
- Numerous other groups including ICANN & US-CERT issued various reports

Findings

- IP address spoofing continues to be one of the primary threat vectors for DDoS attacks leveraging Open recursive DNS servers
- Misconfigured DNS servers continue to lead to DNS resolvers being configured as “open”
- Some low-cost network-connected devices expose DNS and other services to the Internet but have no fundamental reason to do so.
- DNS software updates are not consistently available nor applied
- Internet-wide community efforts to comprehensively and consistently measure the prevalence of open recursive DNS servers lacks scientific due-diligence

Recommendations

- 7 Recommendations specific to open recursive DNS servers
- 1 recommendation in common with BGP sub-group
 - The Internet community should continue measurements of open recursive DNS servers and of the global routing system

Open Recursive DNS Server Recommendations

- Network Operators and Service Providers should...
 - follow the recommendations published in SAC065 as applicable
 - segregate authoritative and recursive DNS servers
 - configure the DNS servers to limit the amount of information returned in queries
 - manage detected end-users of open recursive DNS servers
 - disable recursion on authoritative servers
 - should investigate encouraging the use of the TCP protocol for DNS on Internet facing interfaces
- Equipment suppliers that include DNS resolvers in their equipment should make sure they do not default to being an open recursive DNS server and should make it easy to verify its proper configuration