



Working Group #4: Network Security Best Practices

September 12, 2012

Presenter:

Rod Rasmussen, Internet Identity

WG #4 Co-Chair

Working Group #4: Network Security

- ❑ Description: This Working Group will examine and make recommendations to the Council regarding best practices to secure the Domain Name System (DNS) and routing system of the Internet during the period leading up to the successful global implementation of the Domain Name System Security Extensions (DNSSEC) and Secure BGP (Border Gateway Protocol) extensions.
- ❑ Duration: Sept. 2011 – Mar. 2013

Working Group #4 – Participants

- Co-Chairs
 - Rod Rasmussen – Internet Identity
 - Rodney Joffe – Neustar
- Participants
 - 30 Organizations represented
 - Service Providers
 - Network Operators
 - Academia
 - Government
 - IT Consultants

Working Group #4 – Deliverables

- Domain Name Service (DNS) Security Issues
 - Report and vote today
- BGP and Inter-Domain Routing Security Issues
 - Report in March 2013

Working Group 4 – Work Completed/Next Steps/Timeline

- Report out DNS paper today
- Draft issues and recommendations for Routing – Fall
- Routing draft report iterations Winter
- Report out Routing paper March 2013 CSRIC
- Teleconferences bi-weekly – Fridays 1330 Eastern
- Sub-team work parties meet in off-weeks



Working Group #4: Network Security Best Practices

FINAL Report – DNS Best Practices

DNS Key Points

- ❑ DNS is a cornerstone service provided by ISPs
 - ❑ Necessary for customers to use the Internet
 - ❑ Essential to allow customers to create and maintain their own Internet presences
 - ❑ Also important for Telco operations and enterprises/gov't/etc.
- ❑ A critical service that ISPs must ensure is resilient to operational challenges and protect from abuse by miscreants
- ❑ As a distributed infrastructure requiring several actors to both enable and protect it, ISPs face challenges outside of their direct control in tackling many of the issues identified

Report Scope

- Not commenting on DNSSEC work covered by WG 5 – recommend that ISPs refer to that report on this topic as appropriate (cache poisoning etc.)
- Recursive DNS infrastructure
- Authoritative DNS infrastructure (ISP and for ISP customers)
- Domain registration of ISP and ISP customer domains
- DNS operations in general that could impact ISPs and their customers
- Security of DNS infrastructure

DNS Issues Considered

- Publication of falsified malicious information
- Use of falsified malicious information published by authoritative nameservers
- Use/dissemination of falsified malicious information introduced in transit
- Insecure zone transfers (TSIG usage)
- DDoS including reflective DNS amplification DDoS attacks
- Filtering/synthesized responses
- NX rewriting on resolvers
- Open resolvers
- Ghost domains
- Customers infected with DNS manipulating virus (e.g. DNSChanger)
- Customers using routers with alternative DNS servers as default
- Resiliency of DNS infrastructure

ISP Roles in DNS Issues

- ❑ Attacks against & issues with ISP Recursive Infrastructure
- ❑ Attacks against & issues with Authoritative DNS of ISPs themselves
- ❑ Attacks against DNS Infrastructure that ISPs provide to their customers
- ❑ Abuse of an ISP's infrastructure to attack others
- ❑ Subscribers of ISPs having issues with DNS
- ❑ Hygiene and "other" issues touching on DNS security

Recommendation Process

- ❑ Numerous best practices based on existing documents
- ❑ Analyze issue and point to existing documentation as the source of practices to use
- ❑ Prior CSRIC Reports, IETF RFCs and BCPs, ICANN SSAC Papers, NIST Special Reports, ISOC papers, SANS Reports
- ❑ 24 separate documents referenced

Recommendation Highlights

- ❑ Protect recursive and authoritative DNS infrastructures from hacking/insiders/account takeovers
- ❑ Protect domain names from hijacking/misconfiguration
- ❑ Ensure resiliency of all DNS infrastructures
- ❑ Implement BCP38 and related measures – ingress filtering to combat reflective DDOS

Working Group #4 – Participant List

Name	Company
Rodney Joffe – Co-Chair	Neustar, Inc.
Rod Rasmussen – Co-Chair	Internet Identity
Mark Adams	ATIS (Works for Cox Communications)
Steve Bellovin	Columbia University
Donna Bethea-Murphy	Iridium
Rodney Buie	TeleCommunication Systems, Inc.
Kevin Cox	Cassidian Communications, an EADS NA Comp
John Crain	ICANN
Michael Currie	Intrado, Inc.
Dale Drew	Level 3 Communications
Chris Garner	CenturyLink
Igor Gashinsky	Yahoo, Inc.
Joseph Gersch	Secure64 Software Corporation
Jose A. Gonzalez	Sprint Nextel Corporation
Kevin Graves	TeleCommunication Systems (TCS)
Barry Greene	GETIT
Tom Haynes	Verizon
Chris Joul	T-Mobile
Mazen Khaddam	Cox
Kathryn Martin	Access Partnership
Ron Mathis	Intrado, Inc.
Danny McPherson	Verisign
Doug Montgomery	NIST
Chris Oberg	ATIS (Works for Verizon Wireless)
Victor Oppleman	Packet Forensics
Alan Paller	SANS Institute
Elman Reyes	Internet Identity
Ron Roman	Applied Communication Sciences
Heather Schiller	Verizon
Jason Schiller	Google
Marvin Simpson	Southern Company Services, Inc.
Tony Tauber	Comcast
Paul Vixie	Internet Systems Consortium
Russ White	Verisign
Bob Wright	AT&T



Working Group #4: Network Security Best Practices

September 12, 2012

Questions/Comments

Presenter:

Rod Rasmussen, Internet Identity

WG #4 Co-Chair